aws

Guia do Desenvolvedor

AWS Key Management Service

AWS Key Management Service: Guia do Desenvolvedor

Table of Contents

AWS Key Management Service 1
Conceitos 4
AWS KMS keys 5
Chaves do cliente e chaves do AWS 6
Chaves do KMS de criptografia simétrica 10
Chaves do KMS assimétricas 10
Chaves do KMS de HMAC 11
Chaves de dados 11
Pares de chaves de dados 15
Aliases 20
Armazenamentos de chaves personalizados 21
Operações criptográficas 22
Identificadores-chave () KeyId 23
Material de chave 26
Origem do material de chave 27
Especificação da chave 28
Uso da chave 29
Criptografia de envelope 29
Contexto de criptografia 31
Política de chaves 35
Concessão 35
Auditar o uso de chaves do KMS 35
Infraestrutura de gerenciamento de chaves 36
Gerenciar chaves do 37
Criar chaves 37
Permissões para criar chaves do KMS 40
Criar chaves do KMS de criptografia simétrica 41
Usar aliases 46
Sobre aliases 48
Como gerenciar aliases 51
Usar aliases em suas aplicações 61
Controlar o acesso a aliases 63
Usar aliases para controlar o acesso a chaves do KMS 69
Localizar aliases em logs do AWS CloudTrail 73

Visualizar chaves 74
Visualizar chaves do KMS no console 75
Visualizar chaves do KMS com a API 90
Visualização da configuração criptográfica 98
Como encontrar o ID e o ARN da chave 100
Encontrar o nome e o ARN do alias 101
Editar chaves 104
Marcar chaves com tags 105
Sobre etiquetas no AWS KMS 106
Gerenciar etiqueta de chaves no console 107
Gerenciar etiquetas de chaves do KMS com operações de API 109
Controlar o acesso a etiquetas 112
Usar etiquetas para controlar o acesso a chaves do KMS 116
Habilitar e desabilitar chaves 120
Habilitar e desabilitar chaves do KMS (console) 121
Habilitar e desabilitar chaves do KMS (API do AWS KMS) 121
Alternar chaves do 122
Por que alternar as chaves do KMS? 125
Como funciona a rotação de chaves 126
Como habilitar e desabilitar a rotação de chaves automática 130
Como realizar a rotação de chaves sob demanda 132
Alterar chaves manualmente 135
Chaves de monitoramento 137
Ferramentas de monitoramento 138
Fazendo login com AWS CloudTrail 140
Monitoramento com CloudWatch 225
Monitoramento com a Amazon EventBridge 238
Usando CloudFormation modelos 240
AWS KMS recursos em AWS CloudFormation modelos 241
Saiba mais sobre AWS CloudFormation 242
Excluir chaves 243
Sobre o período de espera 244
Excluir chaves do KMS assimétricas 245
Excluir chaves de várias Regiões 246
Excluir chaves do KMS com material de chave importado 246
Controlar o acesso à exclusão de chaves 246

Programar e cancelar a exclusão de chaves 249
Criar um alarme 252
Determinar a utilização anterior de uma chave do KMS 255
Referência de estado de chave 259
Estados de chave e tipos de chaves do KMS 260
Tabela de estados de chave 261
Autenticação e controle de acesso 269
Conceitos 271
Autenticação 271
Autorização 271
Autenticando com identidades 271
Como gerenciar acesso usando políticas 275
Atributos AWS KMS 278
Políticas de chaves 279
Criação de uma política de chave 280
Política de chaves padrão 286
Visualizar uma política de chaves 301
Alterar uma política de chaves 304
Permissões para AWS serviços 307
Políticas do IAM 311
Visão geral de políticas do IAM 312
Práticas recomendadas para políticas do IAM 313
Especificando chaves do KMS em instruções de políticas do IAM 316
Permissões necessárias para usar o AWS KMS console 319
AWS política gerenciada para usuários avançados 320
Exemplos 322
Concessões 328
Sobre concessões 328
Conceitos sobre concessões 330
Práticas recomendadas 335
Criar concessões 336
Gerencias concessões 345
Endpoint da VPC 350
Considerações sobre endpoints da VPC do AWS KMS 351
Criar um endpoint da VPC para o AWS KMS 351
Conectar-se a um endpoint da VPC 352

Controlar o acesso a um endpoint da VPC ... 353
Usar um endpoint da VPC em uma declaração de política ... 357
Registrar o endpoint da VPC em log ... 360
Chaves de condição ... 361
AWS chaves de condição globais ... 362
AWS KMS chaves de condição ... 364
AWS KMS chaves de condição para AWS Nitro Enclaves ... 434
Controle de acesso baseado em atributos (ABAC) ... 438
Chaves de condição de ABAC para o AWS KMS ... 439
Etiquetas ou aliases? ... 442
Solução de problemas com o ABAC para o AWS KMS ... 444
Acesso entre contas ... 449
Etapa 1: Incluir uma declaração de política de chaves na conta local ... 451
Etapa 2: Adicionar políticas do IAM à conta externa ... 454
Criar chaves do KMS que podem ser usadas por outras contas ... 456
Permitir o uso de chaves do KMS externas com Serviços da AWS ... 458
Usar chaves do KMS em outras contas ... 458
Perfis vinculados ao serviço ... 459
Permissões da função vinculada ao serviço para armazenamento de chaves personalizado do AWS KMS ... 459
Permissões de função vinculada ao serviço para chaves de várias regiões do AWS KMS ... 460
Atualizações do AWS KMS para políticas gerenciadas pela AWS ... 461
TLS pós-quântico híbrido ... 461
Sobre o TLS pós-quântico ... 463
Como usar ... 464
Como configurá-lo ... 465
Como testá-lo ... 467
Saiba mais ... 467
Determinar o acesso ... 468
Examinar a política de chaves ... 468
Examinar políticas do IAM ... 472
Examinar concessões ... 474
Solucionar problemas de acesso à chave ... 475
Referência de permissões ... 482
Descrições das colunas ... 531
Testar suas permissões ... 533

O que é DryRun? ... 534
Especificando DryRun com a API ... 535
Chaves para fins especiais ... 536
Escolha de um tipo de chave do KMS ... 537
Selecionar o uso de chave ... 540
Selecionar a especificação de chave ... 542
Chaves assimétricas ... 543
Chaves do KMS assimétricas ... 545
Criar chaves do KMS assimétricas ... 546
Fazer download de chaves públicas ... 552
Identificar chaves do KMS assimétricas ... 555
Especificações de chave assimétrica ... 560
Chaves de HMAC ... 573
Especificações de chave para chaves do KMS de HMAC ... 576
Criar chaves de HMAC ... 576
Controlar o acesso a chaves de HMAC ... 582
Visualizar chaves de HMAC ... 583
Chaves de várias regiões ... 584
Considerações de segurança de chaves de várias Regiões ... 587
Como funcionam chaves de várias Regiões ... 588
Conceitos ... 592
Controlar o acesso ... 595
Criar chaves de várias regiões ... 604
Visualizar chaves de várias regiões ... 615
Como gerenciar chaves de várias regiões ... 619
Importar material de chave para chaves de várias regiões ... 625
Excluir chaves de várias regiões ... 629
Material de chave importado ... 642
Planejar para importar o material de chave ... 645
Gerenciar o material de chave importada ... 653
Etapa 1: criar uma chave do KMS sem material de chave ... 661
Etapa 2: Fazer download da chave pública de empacotamento e do token de importação ... 664
Etapa 3: Criptografar o material de chave ... 673
Etapa 4: Importar o material de chave ... 683
Armazenamentos de chaves personalizados ... 687
AWS CloudHSM lojas principais ... 689

Armazenamentos de chaves externas ... 761
Referência de tipos de chaves ... 903
Tabela de tipos de chave ... 903
Tabela de recursos especiais ... 909
Segurança ... 920
Proteção de dados ... 921
Proteger material de chave ... 921
Criptografia de dados ... 923
Privacidade entre redes ... 924
Gerenciamento de identidade e acesso ... 925
Registro em log e monitoramento ... 926
Validação de conformidade ... 927
Documentos de conformidade e segurança ... 928
Saiba mais ... 928
Resiliência ... 929
Isolamento regional ... 929
Design de vários locatários ... 930
Práticas recomendadas de resiliência no AWS KMS ... 930
Segurança da infraestrutura ... 931
Isolamento de hosts físicos ... 932
Práticas recomendadas de segurança ... 933
Cotas ... 934
Cotas de recurso ... 934
AWS KMS keys: 100,000 ... 935
Aliases por chave do KMS: 50 ... 936
Concessões por chave do KMS: 50.000 ... 936
Tamanho do documento da política de chaves: 32 KB ... 936
Cota de recursos de armazenamento de chaves personalizado: 10 ... 937
Rotação sob demanda: 10 ... 937
Cotas de solicitações ... 937
Solicite cotas para cada operação de AWS KMS API ... 938
Aplicar cotas de solicitações ... 945
Cotas compartilhadas para operações de criptografia ... 946
Solicitações de API dofeitas em seu nome ... 947
Solicitações entre contas ... 948
Cotas de solicitação de armazenamento de chaves personalizadas ... 948

Controle de utilização de solicitações do 950
Como os serviços da AWS, usam o AWS KMS 952
AWS CloudTrail 953
Entender quando sua chave do KMS é usada 953
Amazon DynamoDB 960
Amazon Elastic Block Store (Amazon EBS) 961
Criptografia de Amazon EBS 961
Usar chaves do KMS e chaves de dados 962
Contexto de criptografia do Amazon EBS 963
Detectar falhas do Amazon EBS 963
Como usar o AWS CloudFormation para criar volumes criptografados do Amazon EBS 964
Amazon Elastic Transcoder 964
Criptografia do arquivo de entrada 965
Descriptografia do arquivo de entrada 966
Criptografia do arquivo de saída 967
Proteção de conteúdo HLS 970
Contexto de criptografia do Elastic Transcoder 971
Amazon EMR 971
Criptografar dados no EMR File System (EMRFS) 972
Criptografar dados nos volumes de armazenamento dos nós de cluster 975
Contexto de criptografia 976
AWS Nitro Enclaves 977
Como chamar APIs do AWS KMS para um Nitro enclave 979
Chaves de condição do AWS KMS para o AWS Nitro Enclaves 980
Solicitações de monitoramento para Nitro enclaves 984
Amazon Redshift 989
Criptografia do Amazon Redshift 989
Contexto de criptografia 990
Amazon Relational Database Service (Amazon RDS) 990
AWS Secrets Manager 991
Amazon Simple Email Service (Amazon SES) 991
Visão geral da criptografia do Amazon SES usando o AWS KMS 992
Contexto de criptografia do Amazon SES 993
Conceder permissão ao Amazon SES para usar sua AWS KMS key 993
Obter e descriptografar mensagens de e-mail 995
Amazon Simple Storage Service (Amazon S3) 996

AWS Systems Manager Parameter Store 996
Proteger parâmetros de string segura padrão 997
Proteger parâmetros de string segura avançados 1000
Definir permissões para criptografar e descriptografar valores de parâmetro 1004
Contexto de criptografia do Parameter Store 1006
Solução de problemas com chaves do KMS no Parameter Store 1009
Amazon WorkMail 1009
WorkMail Visão geral da Amazon 1010
WorkMail Criptografia da Amazon 1010
Autorizar o uso da chave do KMS 1014
Contexto WorkMail de criptografia da Amazon 1017
Monitorando a WorkMail interação da Amazon com AWS KMS 1017
WorkSpaces 1020
Visão geral da WorkSpaces criptografia usando AWS KMS 1020
WorkSpaces contexto de criptografia 1022
Dar WorkSpaces permissão para usar uma chave KMS em seu nome 1022
Programação da API do AWS KMS 1025
Criar um cliente 1025
Trabalhar com chaves 1027
Criar uma chave do KMS 1027
Gerar uma chave de dados 1029
Como visualizar um AWS KMS key 1033
Obter IDs e ARNs de chave 1036
Habilitar o AWS KMS keys 1038
Desabilitar as AWS KMS key 1041
Trabalhar com aliases 1043
Criar um alias 1044
Listar aliases 1047
Atualizar um alias 1052
Excluir um alias 1055
Criptografar e descriptografar chaves de dados 1057
Criptografar uma chave de dados 1058
Descriptografia de uma chave de dados 1061
Criptografar novamente uma chave de dados em uma AWS KMS key 1065
Trabalhar com políticas de chaves 1070
Listar nomes de política de chaves 1070

Obter uma política de chaves 1073
Definir uma política de chaves 1076
Trabalhar com concessões 1082
Criar uma concessão 1083
Visualizar uma concessão 1086
Remover uma concessão 1092
Revogar uma concessão 1094
Como testar suas chamadas de API do AWS KMS 1098
O que é DryRun? 534
Especificando DryRun com a API 535
Consistência eventual do AWS KMS 1100
Referências 1102
Histórico do documento 1104
Atualizações recentes 1104
Atualizações anteriores 1109
..... mcxiv

AWS Key Management Service

O AWS Key Management Service (AWS KMS) é um serviço gerenciado que facilita a criação e o controle de chaves criptográficas usadas para proteger os dados. Para proteger e validar suas AWS KMS keys, o AWS KMS usa módulos de segurança de hardware (HSMs) de acordo com o Programa de validação de módulos criptográficos FIPS 140-2. As regiões China (Pequim) e China (Ningxia) não oferecem suporte ao Programa de validação de módulo criptográfico FIPS 140-2. O AWS KMS usa HSMs certificados pela OSCCA para proteger chaves do KMS nas regiões da China.

O AWS KMS é integrado à maioria dos serviços da AWS que criptografam seus dados. O AWS KMS também é integrado ao AWS CloudTrail para registrar em log o uso das suas chaves do KMS para necessidades de auditoria, regulamentação e conformidade.

Você pode usar a API AWS KMS para criar e gerenciar chaves KMS e recursos especiais, como armazenamentos de chaves personalizados e usar chaves do KMS em operações criptográficas. Para obter mais informações, consulte a Referência da API do AWS Key Management Service.

É possível criar e gerenciar as AWS KMS keys:

- Criar, editar e visualizar chaves do KMS simétricas e assimétricas, inclusive chaves de HMAC.
- Controle o acesso às suas chaves do KMS usando políticas de chaves, políticas do IAM e concessões. O AWS KMS oferece suporte ao controle de acesso baseado em atributos (ABAC). Você também pode refinar políticas usando chaves de condição.
- Criar, excluir, listar e atualizar aliases, que são nomes amigáveis para as suas chaves do KMS. Você também pode usar aliases para controlar o acesso às suas chaves do KMS.
- Marcar suas chaves do KMS para identificação, automação e rastreamento de custos. Você também pode usar etiquetas para controlar o acesso às suas chaves do KMS.
- Habilitar e desabilitar chaves do KMS.
- Habilitar e desabilitar a alternância automática do material criptográfico em uma chave do KMS.
- Excluir chaves do KMS para concluir o ciclo de vida das chaves.

Você pode usar suas chaves do KMS em operações de criptografia. Para ver exemplos, consulte Programação da API do AWS KMS.

- Criptografar, descriptografar e recriptografar dados com chaves do KMS simétricas ou assimétricas.

- Assinar e verificar mensagens com chaves do KMS assimétricas.
- Gerar chaves de dados simétricas e pares de chaves de dados assimétricas exportáveis.
- Gerar e verificar códigos de HMAC.
- Gerar números aleatórios adequados para aplicações criptográficas.

É possível usar os recursos avançados do AWS KMS.

- Crie chaves de várias regiões, que atuam como cópias da mesma chave do KMS em diferentes Regiões da AWS.
- Importe material criptográfico para uma chave do KMS.
- Criar chaves do KMS em seu próprio armazenamento de chaves do AWS CloudHSM com suporte de um cluster do AWS CloudHSM.
- Crie chaves do KMS em um armazenamento de chaves externas baseadas em suas chaves de criptografia fora da AWS.
- Conectar-se diretamente ao AWS KMS por meio de um endpoint privado em sua VPC.
- Usar o TLS pós-quântico híbrido para fornecer criptografia prospectiva em trânsito para os dados enviados ao AWS KMS.

Ao usar o AWS KMS, você ganha mais controle sobre o acesso aos dados que você criptografa. Você pode usar os recursos de criptografia e gerenciamento de chaves diretamente nas suas aplicações ou por meio dos serviços da AWS integrados ao AWS KMS. Seja escrevendo aplicações para a AWS ou usando serviços da AWS, com o AWS KMS, você pode manter o controle sobre quem pode usar suas AWS KMS keys e obter acesso aos seus dados criptografados.

O AWS KMS integra-se ao AWS CloudTrail, um serviço que fornece os arquivos de log para o bucket do Amazon S3 designado. Ao usar, CloudTrail você pode monitorar e investigar como e quando suas chaves KMS foram usadas e quem as usou.

AWS KMS em Regiões da AWS

As Regiões da AWS em que o AWS KMS é compatível estão listadas em AWS Key Management ServiceEndpoints e cotas do. Se um recurso do AWS KMS não for compatível com uma região da Região da AWS em que o AWS KMS tem suporte, a diferença regional estará descrita no tópico sobre o recurso.

AWS KMSDefinição de preço do

Assim como ocorre com outros produtos da AWS, não há contratos nem requisitos mínimos de compra para uso do AWS KMS. Para obter mais informações sobre os preços do AWS KMS, consulte Definição de preço do AWS Key Management Service.

Acordo de nível de serviço

O AWS Key Management Service tem o suporte por um contrato de nível de serviço que define nossa política de disponibilidade.

Saiba mais

- Para saber mais sobre os termos e os conceitos usados no AWS KMS, consulte Conceitos do AWS KMS.
- Para obter mais informações sobre a API do AWS KMS, consulte a Referência de APIs do AWS Key Management Service. Para obter exemplos em diferentes linguagens de programação, consulte Programação da API do AWS KMS.
- Para aprender a usar modelos AWS CloudFormation para criar e gerenciar chaves e aliases, consulte Criando AWS KMS recursos com AWS CloudFormation e Referência do tipo de recurso AWS Key Management Service no Guia do usuário do AWS CloudFormation.
- Para obter informações técnicas detalhadas sobre como o AWS KMS usa criptografia e protege chaves do KMS, consulte Detalhes criptográficos do AWS Key Management Service. A documentação de Detalhes criptográficos não descreve como o AWS KMS funciona nas regiões China (Pequim) e China (Ningxia).
- Para obter uma lista de endpoints do AWS KMS, incluindo endpoints FIPS, em cada Região da AWS, consulte Service endpoints (Endpoints de serviço) no tópico AWS Key Management Service da Referência geral da AWS.
- Para obter ajuda com perguntas sobre o AWS KMS, consulte o Fórum de discussão do AWS Key Management Service.

AWS KMS nos AWS SDKs

- 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

Conceitos do AWS KMS

Aprenda os termos e conceitos básicos usados no AWS Key Management Service (AWS KMS) e como eles trabalham juntos para ajudar a proteger seus dados.

Tópicos

- AWS KMS keys
- Chaves do cliente e chaves do AWS
- Chaves do KMS de criptografia simétrica
- Chaves do KMS assimétricas
- Chaves do KMS de HMAC
- Chaves de dados
- Pares de chaves de dados
- Aliases
- Armazenamentos de chaves personalizados
- Operações criptográficas
- Identificadores-chave () KeyId
- Material de chave
- Origem do material de chave
- Especificação da chave
- Uso da chave
- Criptografia de envelope
- Contexto de criptografia
- Política de chaves
- Concessão

- Auditar o uso de chaves do KMS
- Infraestrutura de gerenciamento de chaves

AWS KMS keys

AWS KMS keys (chaves do KMS) são o recurso principal no AWS KMS. É possível usar uma chave do KMS para criptografar, descriptografar e recriptografar dados. Ela também pode gerar chaves de dados que você pode usar fora do AWS KMS. Normalmente, você usará chaves do KMS de criptografia simétrica, mas pode criar e usar chaves do KMS assimétricas para criptografia ou assinatura, além de criar e usar chaves do KMS de Hash-based message authentication code (HMAC – Código de autenticação de mensagem por hash) para gerar e verificar tags de HMAC.

> **Note**
>
> AWS KMS está substituindo o termo chave mestre do cliente (CMK) por AWS KMS key e Chave KMS. O conceito não mudou. Para evitar alterações interrompidas, o AWS KMS está mantendo algumas variações deste termo.

Uma AWS KMS key é uma representação lógica de uma chave criptográfica. Uma chave do KMS contém metadados, como o ID da chave, especificação de chave, uso da chave, data de criação, descrição e estado da chave. O mais importante é que ela contém uma referência ao material de chave que é usado quando você realiza operações de criptografia com a chave do KMS.

Você pode criar uma chave do KMS com material de chave de criptografia gerado em módulos de segurança de hardware validados pelo FIPS do AWS KMS. O material de chave para chaves do KMS simétricas e as chaves privadas de chaves do KMS assimétricas nunca deixam o AWS KMS descriptografadas. Para usar ou gerenciar suas chaves do KMS, você deve usar o AWS KMS. Para obter mais informações sobre como criar e gerenciar chaves do KMS, consulte Gerenciar chaves do . Para obter mais informações sobre como usar chaves do KMS, consulte a Referência de APIs do AWS Key Management Service.

Por padrão, o AWS KMS cria o material de chaves para uma chave do KMS. Você não pode extrair, exportar, visualizar ou gerenciar esse material de chaves. A única exceção é a chave pública de um par de chaves assimétricas, que você pode exportar para uso fora da AWS. Além disso, não é possível excluir esse material de chave. Você deve excluir a chave do KMS. No entanto, você pode importar seu próprio material de chave para uma chave do KMS ou usar um armazenamento de

chaves personalizado para criar chaves do KMS que utilizam material de chave no cluster do AWS CloudHSM ou material de chave em um gerenciador de chaves externas que você possui e gerencia fora da AWS.

O AWS KMS também oferece suporte a chaves de várias regiões, que permitem criptografar dados em uma Região da AWS e descriptografá-los em uma Região da AWS diferente.

Para obter mais informações sobre como criar e gerenciar chaves do KMS, consulte Gerenciar chaves do . Para obter mais informações sobre como usar chaves do KMS, consulte a Referência de APIs do AWS Key Management Service.

Chaves do cliente e chaves do AWS

As chaves do KMS que você cria são chaves gerenciadas pelo cliente. Os Serviços da AWSque usam chaves do KMS para criptografar seus recursos dos serviços geralmente criam chaves para você. As chaves do KMS que os Serviços da AWS criam em sua conta da AWS são Chaves gerenciadas pela AWS. As chaves do KMS que os Serviços da AWS criam em uma conta de serviço são Chaves pertencentes à AWS.

Tipo de chave do KMS	Pode visualizar metadados da chave do KMS	Pode gerenciar a chave do KMS	Usado apenas para a minha Conta da AWS	Rotação automática	Definição de preço
Chave gerenciada pelo cliente	Sim	Sim	Sim	Opcional. A cada ano (aproxima damente 365 dias)	Tarifa mensal (proporcional por hora) Tarifa por uso
Chave gerenciada pela AWS	Sim	Não	Sim	Obrigatório. A cada ano (aproxima damente 365 dias)	Nenhuma tarifa mensal Tarifa por uso (alguns Serviços da AWS pagam

Tipo de chave do KMS	Pode visualizar metadados da chave do KMS	Pode gerenciar a chave do KMS	Usado apenas para a minha Conta da AWS	Rotação automática	Definição de preço
					essa tarifa para você)
Chave pertencente à AWS	Não	Não	Não	Varia	Nenhuma tarifa

Os serviços da AWS que se integram ao AWS KMS são diferentes no que se refere ao suporte para chaves do KMS. Alguns serviços da AWS criptografam seus dados por padrão com uma Chave pertencente à AWS ou com uma Chave gerenciada pela AWS. Alguns serviços da AWS oferecem suporte a chaves gerenciadas pelo cliente. Outros serviços da AWS são compatíveis com todos os tipos de chaves do KMS para proporcionar a facilidade de uma Chave pertencente à AWS, a visibilidade de uma Chave gerenciada pela AWS ou o controle de uma chave gerenciada pelo cliente. Para obter informações detalhadas sobre as opções de criptografia oferecidas por um serviço da AWS, consulte o tópico Criptografia em repouso no manual do usuário ou no guia do desenvolvedor do serviço.

Chaves gerenciadas pelo cliente

As chaves do KMS que você cria são chaves gerenciadas pelo cliente. Chaves gerenciadas pelo cliente são chaves do KMS em sua Conta da AWS que você cria, detém e gerencia. Você tem controle total sobre essas chaves do KMS, incluindo estabelecer e manter suas políticas de chaves, políticas do IAM e concessões, além de habilitá-las e desabilitá-las, alternar seu material criptográfico, adicionar etiquetas, criar aliases que fazem referência às chaves do KMS e programar a exclusão de chaves do KMS.

Chaves gerenciadas pelo cliente são exibidas na página Customer managed keys (Chaves gerenciadas pelo cliente) do AWS Management Console para o AWS KMS. Para identificar definitivamente uma chave gerenciada pelo cliente, use a operação DescribeKey. Para chaves gerenciadas pelo cliente, o valor do campo `KeyManager` da resposta `DescribeKey` é `CUSTOMER`.

Você pode usar suas chaves gerenciadas pelo cliente em operações de criptografia e auditar o uso em logs do AWS CloudTrail. Além disso, muitos serviços da AWS que se integram com o AWS KMS permitem que você especifique uma chave gerenciada pelo cliente para proteger os dados armazenados e gerenciados.

Chaves gerenciadas pelo cliente geram uma taxa mensal e uma taxa para uso que excede o nível gratuito. Elas contam para as cotas do AWS KMS da sua conta. Para obter mais detalhes, consulte AWS Key Management Service Definição de preço e Cotas.

Chaves gerenciadas pela AWS

Chaves gerenciadas pela AWS são chaves do KMS em sua conta que são criadas, gerenciadas e usadas em seu nome por um serviço da AWS integrado ao AWS KMS.

Alguns serviços da AWS permitem escolher uma Chave gerenciada pela AWS ou uma chave gerenciada pelo cliente para proteger os recursos que ele contém. Em geral, a menos que seja necessário controlar a chave de criptografia que protege os recursos, uma Chave gerenciada pela AWS é uma boa escolha. Você não precisa criar ou manter a chave ou sua política de chave, e nenhuma tarifa mensal é necessária para uma Chave gerenciada pela AWS.

Você tem permissão para visualizar as Chaves gerenciadas pela AWS na sua conta, visualizar suas políticas de chave e auditar o uso delas em logs do AWS CloudTrail. Porém, não pode alterar nenhuma propriedade de Chaves gerenciadas pela AWS, alterná-las, modificar suas políticas de chave ou programá-las para exclusão. Você também não pode usar Chaves gerenciadas pela AWS em operações de criptografia de forma direta. Elas são usadas em seu nome pelo serviço que as cria.

Chaves gerenciadas pela AWS aparece na página Chaves gerenciadas pela AWS do AWS Management Console para o AWS KMS. Também é possível identificar Chaves gerenciadas pela AWS por seus aliases, que têm o formato `aws/`*`service-name`*, como `aws/redshift`. Para identificar definitivamente umChaves gerenciadas pela AWS, use a DescribeKeyoperação. Para Chaves gerenciadas pela AWS, o valor do campo `KeyManager` da resposta `DescribeKey` é `AWS`.

Todas as Chaves gerenciadas pela AWS são alternadas automaticamente a cada ano. alternarNão é possível alterar essa programação de rotação.

> **Note**
>
> Em maio de 2022, o AWS KMS alterou o cronograma de alternância para Chaves gerenciadas pela AWS de a cada 3 anos (aproximadamente 1.095 dias) para a cada ano (aproximadamente 365 dias).
> Novas Chaves gerenciadas pela AWS são alternadas automaticamente um ano após serem criadas e aproximadamente a cada ano depois disso.
> As Chaves gerenciadas pela AWS existentes são alternadas automaticamente um ano após sua alternância mais recente e a cada ano depois disso.

Não há uma tarifa mensal para Chaves gerenciadas pela AWS. Elas podem estar sujeitas a taxas de uso que excede o nível gratuito, mas alguns serviços da AWS abrangem esses custos para você. Para obter detalhes, consulte o tópico Criptografia em repouso, no manual do usuário ou no guia do desenvolvedor do serviço. Para obter mais informações, consulte Definição de preço do AWS Key Management Service.

As Chaves gerenciadas pela AWS não são contabilizadas em relação às cotas de recursos para o número de chaves do KMS em cada região da sua conta. No entanto, quando usadas em nome de uma entidade principal na sua conta, essas chaves do KMS contam para as cotas de solicitações. Para obter detalhes, consulte Cotas.

Chaves pertencentes à AWS

Chaves pertencentes à AWS são uma coleção de chaves do KMS de propriedade de um serviço da AWS e que esse serviço gerencia para uso em várias Contas da AWS. Embora as Chaves pertencentes à AWS não estejam em sua Conta da AWS, um serviço da AWS pode usar uma Chave pertencente à AWS para proteger os recursos da conta.

Alguns serviços da AWS permitem escolher uma Chave pertencente à AWS ou uma chave gerenciada pelo cliente. Em geral, a menos que seja necessário auditar ou controlar a chave de criptografia que protege os recursos, uma Chave pertencente à AWS é uma boa escolha. Chaves pertencentes à AWS são totalmente gratuitas (sem tarifas mensais ou de uso), não contam para as cotas do AWS KMS da sua conta e são fáceis de usar. Você não precisa criar ou manter a chave ou sua política de chave.

A rotação das Chaves pertencentes à AWS varia de acordo com os serviços. Para obter informações sobre a rotação de uma Chave pertencente à AWS específica, consulte o tópico Criptografia em repouso no guia do usuário ou no guia do desenvolvedor do serviço.

Chaves do KMS de criptografia simétrica

Ao criar uma AWS KMS key, você recebe por padrão uma chave do KMS para criptografia simétrica. Esse é o tipo básico e mais comumente usado de chave do KMS.

No AWS KMS, uma chave do KMS de criptografia simétrica representa uma chave de criptografia AES-GCM de 256 bits, exceto nas regiões da China, em que ela representa uma chave de criptografia SM4 de 128 bits. O material de chave simétrica nunca sai descriptografado do AWS KMS. Para usar uma chave do KMS de criptografia simétrica, você deve chamar o AWS KMS. As chaves de criptografia simétrica são usadas na criptografia simétrica, na qual a mesma chave é usada para criptografia e descriptografia. A menos que sua tarefa exija explicitamente criptografia assimétrica, as chaves do KMS de criptografia simétrica, que nunca deixam o AWS KMS descriptografadas, são uma boa opção.

Os serviços da AWS que são integrados ao AWS KMS usam exclusivamente chaves do KMS de criptografia simétrica para criptografar seus dados. Esses serviços não fornecem suporte para criptografia com chaves do KMS assimétricas. Para obter ajuda para determinar se uma chave do KMS é simétrica ou assimétrica, consulte Identificar chaves do KMS assimétricas.

Tecnicamente, a especificação da chave para uma chave simétrica é SYMMETRIC_DEFAULT, o uso da chave é ENCRYPT_DECRYPT e o algoritmo de criptografia é SYMMETRIC_DEFAULT. Para obter detalhes, consulte Especificação da chave SYMMETRIC_DEFAULT.

É possível usar uma chave do KMS de criptografia simétrica no AWS KMS para criptografar, descriptografar e recriptografar dados, além de gerar chaves de dados e pares de chaves de dados. Você pode criar chaves do KMS de criptografia simétrica de várias regiões, importar seu próprio material de chaves para uma chave do KMS de criptografia simétrica e criar chaves do KMS de criptografia simétrica em armazenamentos personalizados de chaves. Para obter uma tabela comparando as operações que podem ser realizadas em chaves do KMS de diferentes tipos, consulte Referência de tipos de chaves.

Chaves do KMS assimétricas

É possível criar chaves do KMS assimétricas no AWS KMS. Uma chave do KMS assimétrica representa um par de chave pública e chave privada matematicamente relacionadas. A chave privada nunca deixa o AWS KMS descriptografado. Para usar a chave privada, é necessário chamar o AWS KMS. Você pode usar a chave pública no AWS KMS chamando as operações de API do AWS KMS ou pode fazer download da chave pública e usá-la fora do AWS KMS. Você também pode criar chaves do KMS assimétricas de várias regiões.

É possível criar chaves do KMS assimétricas que representam pares de chaves RSA ou pares de chaves SM2 (somente para regiões da China) para criptografia de chaves públicas ou de assinatura e verificação, ou pares de chaves de curva elíptica para assinatura e verificação.

Para saber mais sobre como criar e usar chaves do KMS assimétricas, consulte Chaves assimétricas no AWS KMS.

Chaves do KMS de HMAC

Uma chave do KMS de HMAC representa uma chave simétrica de comprimento variável que é usada para gerar e verificar códigos de autenticação de mensagens por hash (HMAC). O material de chave de uma chave de HMAC nunca sai descriptografado do AWS KMS. Para usar uma chave de HMAC, chame as operações de API `GenerateMac` ou `VerifyMac`.

Você também pode criar chaves do KMS de HMAC de várias regiões.

Para obter mais informações sobre como criar e usar chaves do KMS de HMAC, consulte Chaves de HMAC no AWS KMS.

Chaves de dados

Chaves de dados são chaves simétricas que você pode usar para criptografar dados, inclusive grandes quantidades de dados e outras chaves de criptografia dos dados. Ao contrário de chaves do KMS assimétricas, que não podem ser baixadas, as chaves de dados são devolvidas para você para uso fora do AWS KMS.

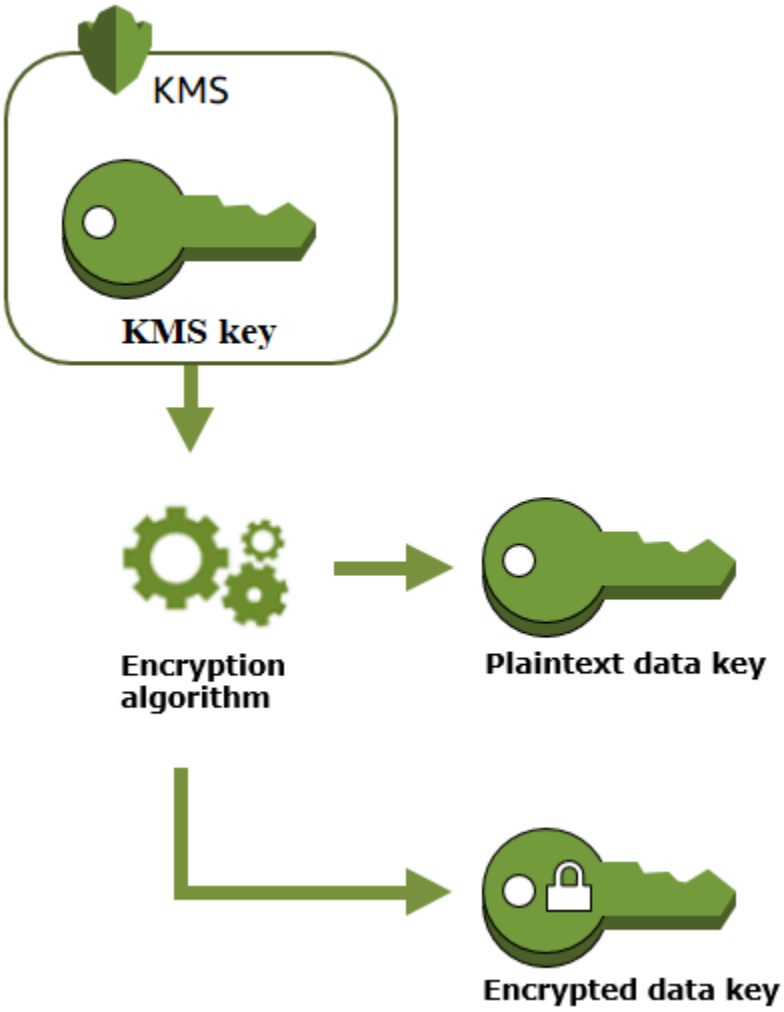
Quando o AWS KMS gera chaves de dados, ele retorna uma chave de dados em texto simples para uso imediato e uma cópia criptografada dessa chave de dados que você pode armazenar com os dados de maneira segura. Quando você pronto para descriptografar os dados, você primeiro solicita ao AWS KMS que descriptografe a chave de dados criptografada.

O AWS KMS gera, criptografa e descriptografa chaves de dados. No entanto, o AWS KMS não armazena, gerencia ou monitora as chaves de dados nem executa operações de criptografia com chaves de dados. Você deve usar e gerenciar as chaves de dados fora do AWS KMS. Para obter ajuda para usar as chaves de dados de forma segura, consulte a AWS Encryption SDK.

Criação de uma chave de dados

Para criar uma chave de dados, chame a GenerateDataKeyoperação. AWS KMSgera a chave de dados. Em seguida, ele criptografa uma cópia da chave de dados em uma chave do KMS de criptografia simétrica especificada por você. A operação retorna uma cópia em texto simples da

chave de dados e a cópia da chave de dados criptografada de acordo com a chave do KMS. A imagem a seguir mostra essa operação.

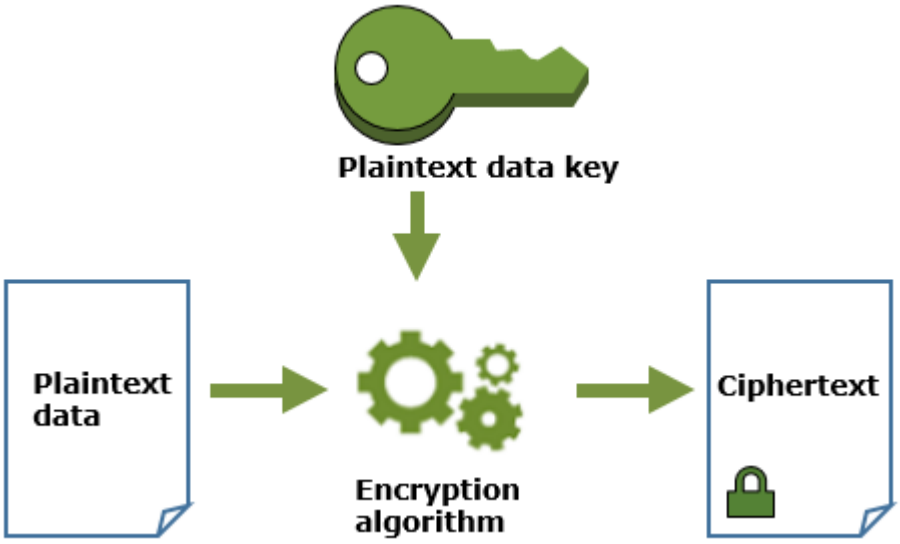


AWS KMStambém suporta a GenerateDataKeyWithoutPlaintextoperação, que retorna somente uma chave de dados criptografada. Quando precisar usar a chave de dados, peça ao AWS KMS para descriptografá-la.

Criptografia de dados com uma chave de dados

AWS KMSO não pode usar uma chave de dados para criptografar dados. No entanto, você pode usar a chave de dados fora do AWS KMS, como ao usar OpenSSL ou uma biblioteca de criptografia, como AWS Encryption SDK.

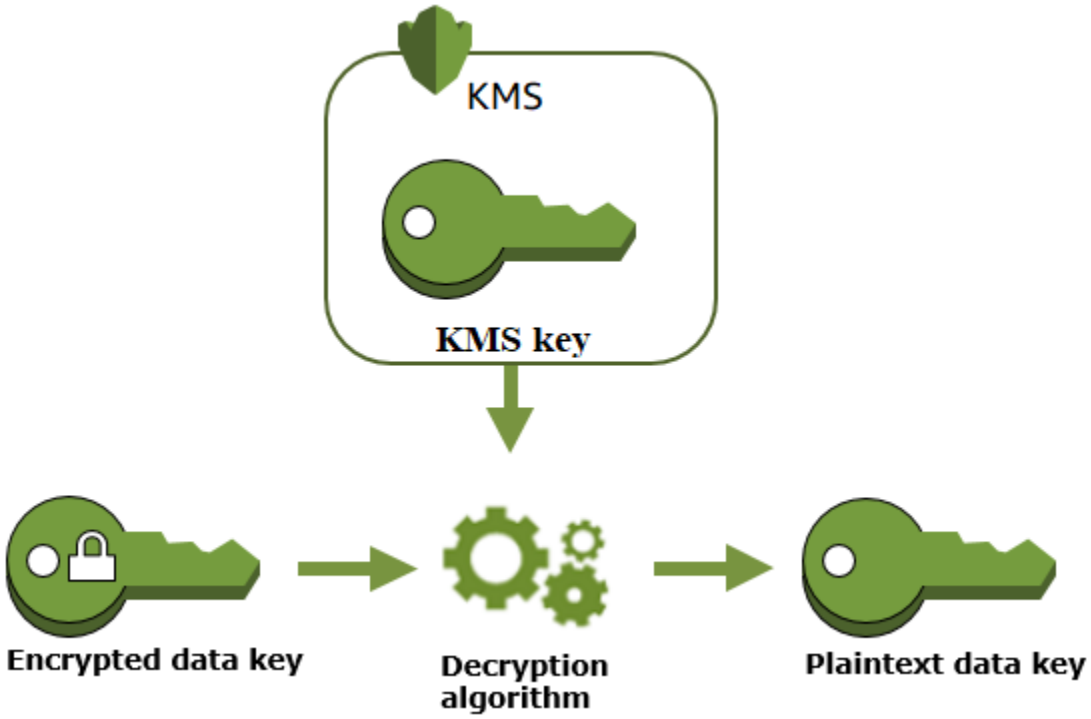
Depois de usar a chave de dados de texto simples para criptografar dados e remova-a da memória assim que possível. Você pode armazenar seguramente as chaves de dados criptografadas com os dados criptografados para que estejam disponíveis para descriptografar os dados.



Descriptografia dos dados com uma chave de dados

Para descriptografar dados, transmita a chave de dados criptografada para a operação Decrypt. O AWS KMS usa sua chave do KMS para descriptografar a chave de dados e, em seguida, retorna a chave de dados em texto simples. Use a chave de dados de texto simples para descriptografar seus dados e remove-a da memória assim que possível.

O diagrama a seguir mostra como usar a operação `Decrypt` para descriptografar uma chave de dados criptografada.



Como as chaves do KMS inutilizáveis afetam as chaves de dados

Quando uma chave do KMS torna-se inutilizável, o efeito é quase imediato (sujeito a consistência posterior). O estado de chave da chave do KMS é alterado para refletir sua nova condição, e todas as solicitações para usar a chave do KMS em operações de criptografia falham.

No entanto, o efeito nas chaves de dados criptografadas pela chave do KMS e nos dados criptografados pela chave de dados é adiado até que a chave do KMS seja usada novamente, por exemplo, para descriptografar a chave de dados.

As chaves do KMS podem se tornar inutilizáveis por vários motivos, inclusive pelas ações a seguir que você pode executar.

- Desabilitar a chave do KMS
- Agendar a exclusão da chave do KMS
- Excluir o material de chaves de uma chave do KMS com material de chaves importado ou permitir que o material de chaves importado expire.
- Desconectar o armazenamento de chaves do AWS CloudHSM que hospeda a chave do KMS ou excluir a chave do cluster do AWS CloudHSM que serve como material de chave para a chave do KMS.

- Desconectar o armazenamento de chaves externas que hospeda a chave do KMS ou qualquer outra ação que interfira nas solicitações de criptografia e descriptografia do proxy de armazenamento de chaves externas, inclusive excluir a chave externa do gerenciador de chaves externas.

Esse efeito é importante principalmente para muitos Serviços da AWS que usam chaves de dados para proteger os recursos que o serviço gerencia. O exemplo abaixo usa o Amazon Elastic Block Store (Amazon EBS) e o Amazon Elastic Compute Cloud (Amazon EC2). Diferentes Serviços da AWS usam chaves de dados de diferentes maneiras. Para obter detalhes, consulte a seção de proteção de dados do capítulo de segurança do AWS service (Serviço da AWS).

Por exemplo, considere este cenário:

1. Crie um volume do EBS criptografado e especifique uma chave do KMS para protegê-lo. O Amazon EBS solicita que o AWS KMS use a chave do KMS para gerar uma chave de dados criptografada para o volume. O Amazon EBS armazena a chave de dados criptografada com os metadados do volume.
2. Quando você anexa o volume do EBS a uma instância do EC2, o Amazon EC2 solicita usa a chave do KMS para descriptografar a chave de dados criptografada do volume do EBS. O Amazon EC2 usa a chave de dados no hardware Nitro, que é responsável por criptografar toda a E/S do disco no volume do EBS. A chave de dados persiste no hardware do Nitro, enquanto o volume do EBS está conectado à instância do EC2.
3. Você executa uma ação que torna a chave do KMS inutilizável. Isso não tem efeito imediato na instância de EC2 ou no volume do EBS. O Amazon EC2 usa a chave de dados (e não a chave do KMS) para criptografar toda a E/S de disco enquanto o volume está anexado à instância.
4. No entanto, quando o volume criptografado do EBS é desanexado da instância do EC2, o Amazon EBS remove a chave de dados do hardware do Nitro. Da próxima vez que o volume do EBS for anexado à instância do EC2, a anexação falhará porque o Amazon EBS não consegue usar a chave do KMS para descriptografar a chave de dados criptografada do volume. Para usar o volume do EBS novamente, é necessário tornar a chave do KMS utilizável novamente.

Pares de chaves de dados

Pares de chaves de dados são chaves de dados assimétricas que consistem em uma chave pública e uma chave privada matematicamente relacionadas. Eles foram projetados para uso na criptografia e descriptografia do lado do cliente ou na assinatura e verificação fora do AWS KMS.

Ao contrário dos pares de chaves de dados gerados por ferramentas como o OpenSSL, o AWS KMS protege a chave privada em cada par de chaves de dados sob uma chave do KMS de criptografia simétrica no AWS KMS que você especifica. No entanto, o AWS KMS não armazena, gerencia nem rastreia os pares de chaves de dados, nem executa operações de criptografia com pares de chaves de dados. É necessário usar e gerenciar pares de chaves fora do AWS KMS.

O AWS KMS oferece suporte aos seguintes tipos de pares de chaves de dados:

- Pares de chaves RSA: RSA_2048, RSA_3072 e RSA_4096
- Pares de chaves de curva elíptica: ECC_NIST_P256, ECC_NIST_P384, ECC_NIST_P521 e ECC_SECG_P256K1
- Pares de chaves SM (somente nas regiões da China): SM2

O tipo de par de chaves de dados selecionado geralmente depende do caso de uso ou dos requisitos regulatórios. A maioria dos certificados exige chaves RSA. As chaves de curva elíptica geralmente são usadas para assinaturas digitais. As chaves ECC_SECG_P256K1 são comumente usadas para criptomoedas. O AWS KMS recomenda usar pares de chaves ECC para assinatura e usar pares de chaves RSA para criptografia ou assinatura, mas não ambos. Porém, AWS KMS não podem impor restrições para o uso de pares de chaves fora do AWS KMS.

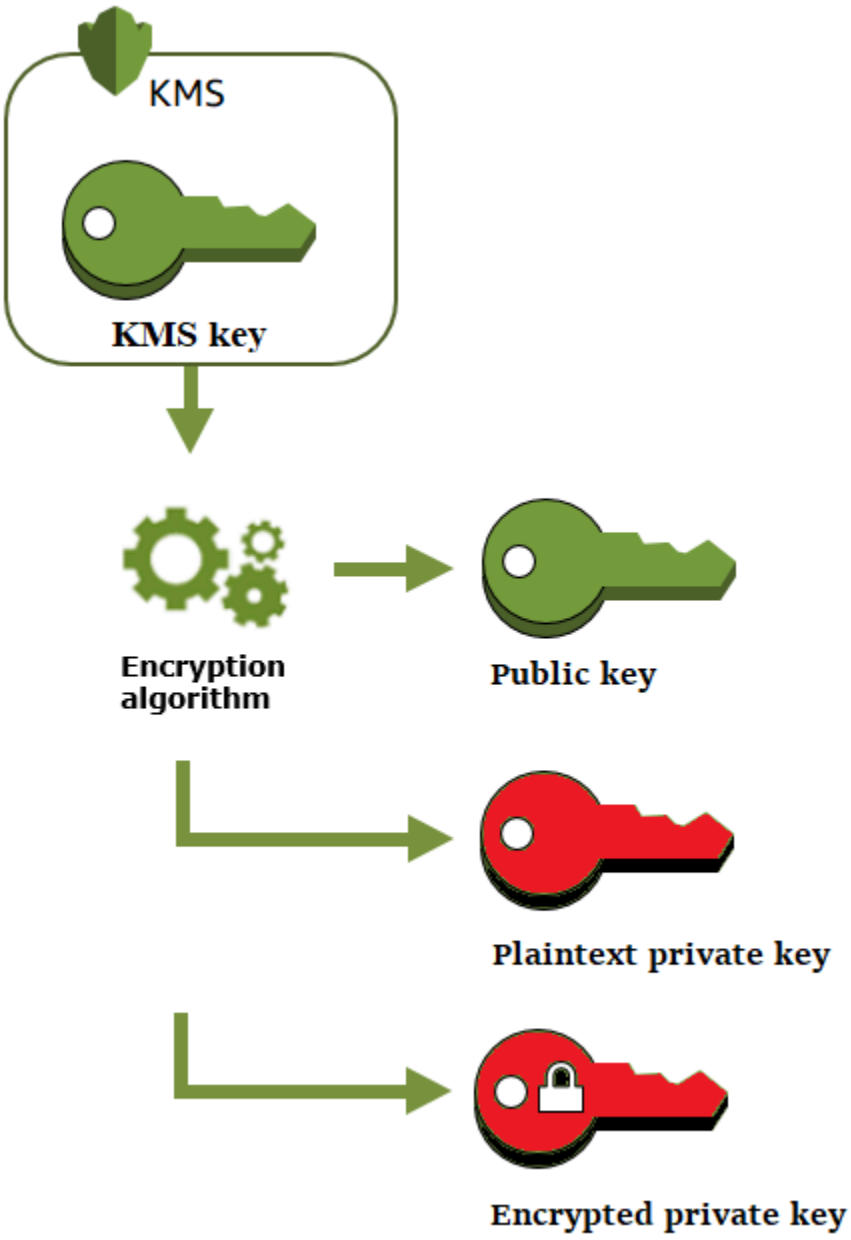
Criar um par de chaves de dados

Para criar um par de chaves de dados, chame as GenerateDataKeyPairWithoutPlaintextoperações GenerateDataKeyPairou. Especifique a chave do KMS de criptografia simétrica que você deseja usar para criptografar a chave privada.

`GenerateDataKeyPair` retorna uma chave pública de texto não criptografado, uma chave privada de texto não criptografado e uma chave privada criptografada. use essa operação quando precisar imediatamente de uma chave privada de texto não criptografado, como para gerar uma assinatura digital.

`GenerateDataKeyPairWithoutPlaintext` retorna uma chave pública de texto não criptografado e uma chave privada criptografada, mas não uma chave privada de texto não criptografado.
Use essa operação quando não precisar imediatamente de uma chave privada de texto não criptografado, como quando você está criptografando uma chave pública. Posteriormente, quando precisar de uma chave privada de texto não criptografado para descriptografar os dados, poderá chamar a operação Decrypt.

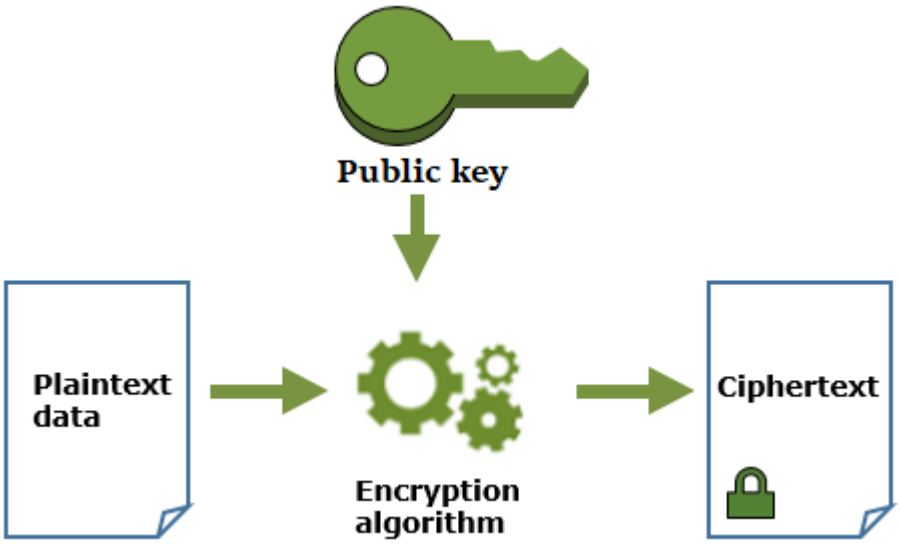
A imagem a seguir mostra a operação `GenerateDataKeyPair`. A operação `GenerateDataKeyPairWithoutPlaintext` omite a chave privada de texto não criptografado.



Criptografar dados com um par de chaves de dados

Ao criptografar com um par de chaves de dados, você usa a chave pública do par para criptografar os dados e a chave privada do mesmo par para descriptografar os dados. Normalmente, pares de chaves de dados são usados quando muitos usuários precisam criptografar dados que só o usuário que tem a chave privada pode descriptografar.

As partes com a chave pública usam essa chave para criptografar dados, conforme mostrado no diagrama a seguir.

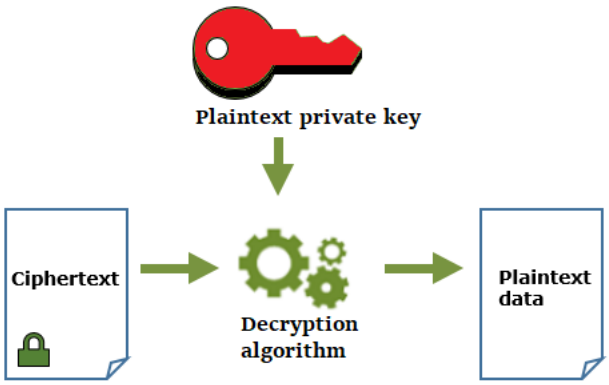


Descriptografar dados com um par de chaves de dados

Para descriptografar seus dados, use a chave privada no par de chaves de dados. Para que a operação seja bem-sucedida, as chaves pública e privada devem ser do mesmo par de chaves de dados e você deve usar o mesmo algoritmo de criptografia.

Para descriptografar a chave privada criptografada, transmita-a para a operação Decrypt. Use a chave privada de texto não criptografado para descriptografar os dados. Depois, remova a chave privada de texto não criptografado da memória assim que possível.

O diagrama a seguir mostra como usar a chave privada em um par de chaves de dados para descriptografar texto cifrado.



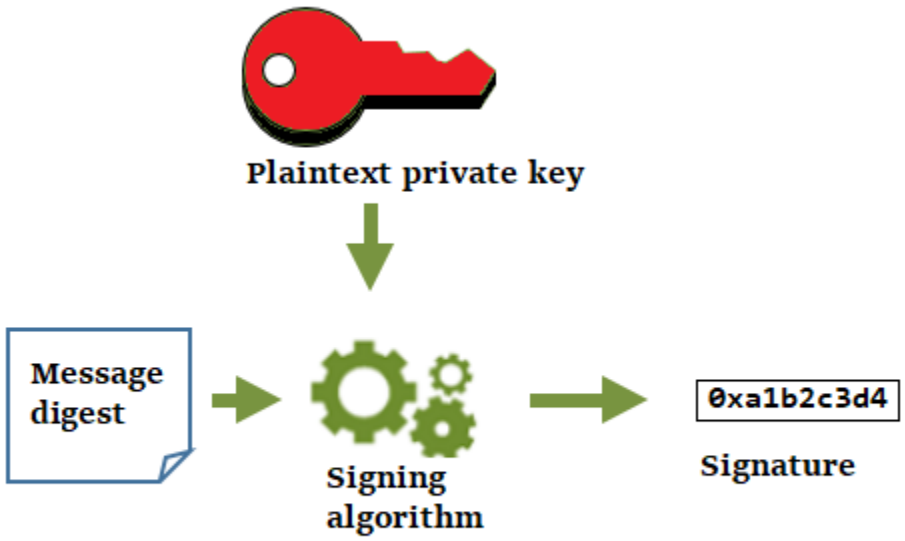
Assinar mensagens com um par de chaves de dados

Para gerar uma assinatura criptográfica para uma mensagem, use a chave privada no par de chaves de dados. Qualquer pessoa com a chave pública pode usá-la para verificar se a mensagem foi assinada com a chave privada e se ela não foi alterada desde que foi assinada.

Se você criptografar sua chave privada, transmita a chave privada criptografada para a operação Decrypt. O AWS KMS usa sua chave do KMS para descriptografar a chave de dados e, em seguida, retorna a chave privada em texto simples. Use a chave privada de texto não criptografado para gerar a assinatura. Depois, remova a chave privada de texto não criptografado da memória assim que possível.

Para assinar uma mensagem, crie um resumo de mensagens usando uma função de hash criptográfica, como o comando `dgst` no OpenSSL. Depois, transmita a chave privada de texto não criptografado ao algoritmo de assinatura. O resultado é uma assinatura que representa os conteúdos da mensagem. (Talvez seja possível assinar mensagens mais curtas sem antes criar um resumo. O tamanho máximo da mensagem varia de acordo com a ferramenta de assinatura que você usa.)

O diagrama a seguir mostra como usar a chave privada em um par de chaves para assinar a mensagem.

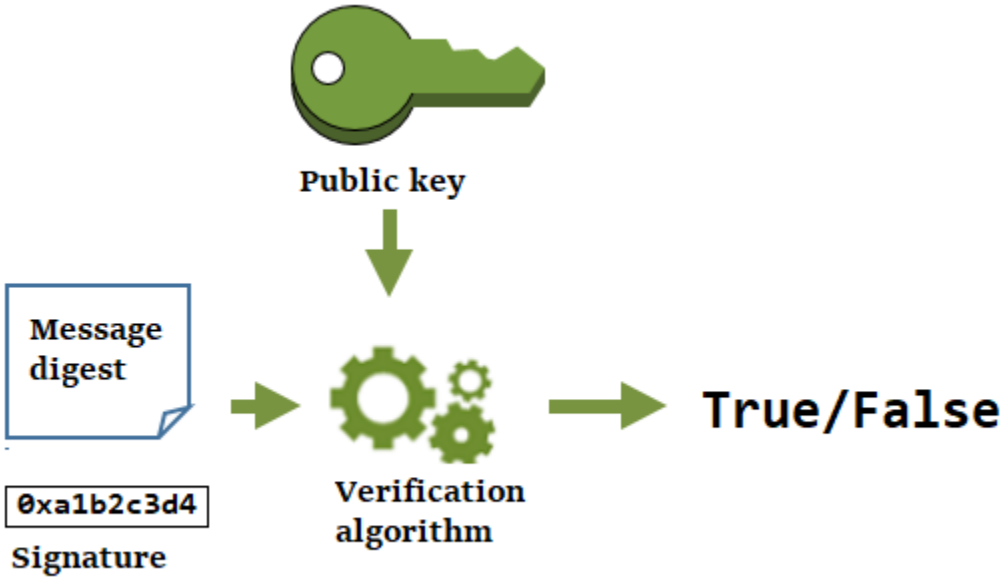


Verificar uma assinatura com um par de chaves de dados

Qualquer pessoa que tenha a chave pública no par de chaves de dados pode usá-la para verificar a assinatura gerada com sua chave privada. A verificação confirma que um usuário autorizado assinou a mensagem com a chave privada e o algoritmo de assinatura especificados, e que a mensagem não foi alterada desde que foi assinada.

Para ser bem-sucedida, a parte que está verificando a assinatura deve gerar o mesmo tipo de resumo, usar o mesmo algoritmo e usar a chave pública que corresponde à chave privada usada para assinar a mensagem.

O diagrama a seguir mostra como usar a chave pública em um par de chaves para verificar a assinatura de uma mensagem.



Aliases

Use um alias como um nome amigável para uma chave do KMS. Por exemplo, você pode fazer referência a uma chave do KMS como test-key em vez de 1234abcd-12ab-34cd-56ef-1234567890ab.

Aliases facilitam a identificação de uma chave do KMS no AWS Management Console. Você também pode usar um alias para identificar uma chave do KMS em algumas operações do AWS KMS, incluindo operações de criptografia. Em aplicações, é possível usar um único alias para fazer referência a diferentes chaves do KMS em cada Região da AWS.

Também é possível permitir e negar acesso a chaves do KMS com base em aliases sem precisar editar políticas ou gerenciar concessões. Esse recurso faz parte do suporte do AWS KMS para controle de acesso baseado em atributos (ABAC). Para obter mais detalhes, consulte ABAC para AWS KMS.

No AWS KMS, aliases são recursos independentes, e não são propriedades de uma chave do KMS. Dessa forma, você pode adicionar, alterar e excluir um alias sem afetar a chave do KMS associada.

> **Important**
>
> Não inclua informações confidenciais ou sigilosas no nome do alias. Os aliases podem aparecer em texto simples em CloudTrail registros e outras saídas.

Saiba mais:

- Para obter informações detalhadas sobre aliases, consulte Usar aliases.
- Para obter informações sobre os formatos de identificadores de chave, incluindo aliases, consulte Identificadores-chave () KeyId.
- Para obter ajuda para localizar os aliases associados a uma chave do KMS, consulte Encontrar o nome e o ARN do alias
- Para obter exemplos de criação e gerenciamento de aliases em várias linguagens de programação, consulte Trabalhar com aliases.

Armazenamentos de chaves personalizados

Um armazenamento de chaves personalizado é um recurso do AWS KMS baseado em um gerenciador de chaves fora do AWS KMS que você possui e gerencia. Quando você usa uma chave do KMS em um armazenamento de chaves personalizado para uma operação de criptografia, a operação de criptografia é executada no gerenciador de chaves usando as respectivas chaves de criptografia.

O AWS KMS oferece suporte a armazenamentos de chaves do AWS CloudHSM com base em um cluster do AWS CloudHSM e armazenamentos de chaves externas baseados em um gerenciador de chaves externas fora da AWS.

Para ter mais informações, consulte Armazenamentos de chaves personalizados.

Operações criptográficas

No AWS KMS, operações de criptografia são operações de API que usam chaves do KMS para proteger dados. Como as chaves do KMS permanecem no AWS KMS, é necessário chamar o AWS KMS para usar uma chaves do KMS em uma operação criptográfica.

Para executar operações de criptografia com chaves do KMS, use os AWS SDKs, a AWS Command Line Interface (AWS CLI) ou o AWS Tools for PowerShell. Não é possível executar operações de criptografia no console do AWS KMS. Para obter exemplos de chamadas de operações de criptografia em várias linguagens de programação, consulte Programação da API do AWS KMS.

A tabela a seguir lista as operações de criptografia do AWS KMS. Ela também mostra os requisitos de tipo de chave e uso de chave para chaves do KMS usadas na operação.

Operation	Tipo de chave	Uso da chave
Decrypt	Simétrico ou assimétrico	`ENCRYPT_DECRYPT`
Encrypt	Simétrico ou assimétrico	`ENCRYPT_DECRYPT`
GenerateDataKey	Simétrica	`ENCRYPT_DECRYPT`
GenerateDataKeyPair	Simétrica [1] Não é compatível com chaves do KMS em armazenamentos de chaves personalizados.	`ENCRYPT_DECRYPT`
GenerateDataKeyPairWithoutPlaintext	Simétrica [1] Não é compatível com chaves do KMS em armazenamentos de chaves personalizados.	`ENCRYPT_DECRYPT`

Operation	Tipo de chave	Uso da chave
GenerateDataKeyWithoutPlaintext	Simétrica	ENCRYPT_DECRYPT
GenerateMac	HMAC	GENERATE_ VERIFY_MAC
GenerateRandom	N/D. Essa operação não usa uma chave do KMS.	N/D
ReEncrypt	Simétrico ou assimétrico	ENCRYPT_DECRYPT
Sign	Assimétrica	SIGN_VERIFY
Verificar	Assimétrica	SIGN_VERIFY
VerifyMac	HMAC	GENERATE_ VERIFY_MAC

[1] Gera um par de chaves de dados assimétricas que é protegido por uma chave do KMS de criptografia simétrica.

Para obter informações sobre as permissões para operações de criptografia, consulte a the section called “Referência de permissões”.

Para tornar o AWS KMS responsivo e altamente funcional para todos os usuários, o AWS KMS estabelece cotas para o número de operações de criptografia chamadas em cada segundo. Para obter mais detalhes, consulte the section called “Cotas compartilhadas para operações de criptografia”.

Identificadores-chave () KeyId

Identificadores de chave atuam como nomes para suas chaves do KMS. Eles ajudam a reconhecer suas chaves do KMS no console. Você poderá usá-las para indicar quais chaves do KMS deseja usar em operações de API do AWS KMS, políticas do IAM e concessões. Os valores do identificador de chave não estão completamente relacionados ao material de chaves associado à chave KMS.

AWS KMSO define vários identificadores de chave. Quando você cria uma chave do KMS, o AWS KMS gera um ARN e um ID de chave, que são propriedades da chave do KMS. Quando você cria um alias, o AWS KMS gera o ARN de alias com base no nome do alias que você define. É possível exibir os identificadores de chave e alias no AWS Management Console e na API do AWS KMS.

No console do AWS KMS, é possível visualizar e filtrar chaves do KMS por ARN de chave, ID de chave ou nome de alias e classificar por ID de chave e nome de alias. Para obter ajuda para encontrar os identificadores de chave no console, consulte the section called “Como encontrar o ID e o ARN da chave”.

Na API do AWS KMS, os parâmetros usados para identificar uma chave do KMS se chamam `KeyId` ou uma variação, como `TargetKeyId` ou `DestinationKeyId`. No entanto, os valores desses parâmetros não estão limitados a IDs de chave. Alguns podem usar qualquer identificador de chave válido. Para obter informações sobre os valores de cada parâmetro, consulte a descrição do parâmetro na Referência de APIs do AWS Key Management Service.

> **Note**
>
> Ao usar a API do AWS KMS, preste atenção ao identificador de chave usado. APIs diferentes requerem identificadores de chave diferentes. Em geral, use o identificador de chave mais completo e prático para a sua tarefa.

AWS KMSO é compatível com os seguintes identificadores de chave.

ARN de chave

O ARN de chave é o Amazon Resource Name (ARN) de uma chave do KMS. É um identificador exclusivo e totalmente qualificado para a chave do KMS. Um ARN de chave inclui a Conta da AWS, a região e o ID de chave. Para obter ajuda para encontrar o ARN de chave de uma chave do KMS, consulte the section called “Como encontrar o ID e o ARN da chave”.

O formato de um ARN de chave é o seguinte:

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

Veja a seguir um exemplo de ARN de chave para uma chave do KMS de região única.

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

O elemento *key-id* dos ARNs de chaves de várias regiões começa com o prefixo `mrk-`. Veja a seguir um exemplo de ARN de chave para uma chave do KMS de várias regiões.

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

ID da chave

O ID de chave identifica exclusivamente uma chave do KMS dentro de uma conta e uma região. Para obter ajuda para encontrar o ID de chave de uma chave do KMS, consulte the section called "Como encontrar o ID e o ARN da chave".

Veja a seguir um exemplo de ID de chave para uma chave do KMS de região única.

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

Os IDs de chave de chaves de várias regiões começam com o prefixo `mrk-`. Veja a seguir um exemplo de ID de chave para uma chave do KMS de várias regiões.

```
mrk-1234abcd12ab34cd56ef1234567890ab
```

ARN do alias

O ARN do alias é o Amazon Resource Name (ARN) de um alias do AWS KMS. É um identificador exclusivo e totalmente qualificado para o alias e para a chave do KMS que ele representa. Um ARN de alias inclui a Conta da AWS, a região e o nome do alias.

A qualquer momento, um ARN de alias identificará uma chave do KMS específica. No entanto, como é possível alterar a chaves do KMS associada ao alias, o ARN do alias pode identificar diferentes chaves do KMS em momentos diferentes. Para obter ajuda para encontrar o ARN de alias de uma chave do KMS, consulte Encontrar o nome e o ARN do alias.

O formato de um ARN de alias é o seguinte:

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

Veja a seguir o ARN de alias de um fictício `ExampleAlias`.

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

Nome do alias

O nome do alias é uma string com até 256 caracteres. Ele identifica exclusivamente uma chave do KMS associada em uma conta e uma região. Na API do AWS KMS, os nomes de alias sempre começam com `alias/`. Para obter ajuda para encontrar o nome de alias de uma chave do KMS, consulte Encontrar o nome e o ARN do alias.

O formato de um nome de alias é o seguinte:

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

Por exemplo:

```
alias/ExampleAlias
```

O prefixo `aws/` de um nome de alias é reservado para Chaves gerenciadas pela AWS. Não é possível criar um alias com esse prefixo. Por exemplo, o nome do alias da Chave gerenciada pela AWS para o Amazon Simple Storage Service (Amazon S3) é o seguinte.

```
alias/aws/s3
```

Material de chave

O material de chave é a string de bits usada em um algoritmo criptográfico. O material de chave secreta deve ser mantido em segredo para proteger as operações de criptografia que o utilizam. O material de chave pública foi projetado para ser compartilhado.

Cada chave do KMS inclui uma referência ao material de chave em seus metadados. A origem do material de chave de chaves do KMS de criptografia simétrica pode variar. Você pode usar material de chave gerado pelo AWS KMS, material chave gerado no cluster do AWS CloudHSMde um armazenamento de chaves personalizado ou pode importar seu próprio material de chave. Se usar material de chave do AWS KMS para sua chave do KMS de criptografia simétrica, você poderá habilitar a alternância automática do seu material de chave.

Por padrão, cada chave do KMS tem material de chave exclusivo. No entanto, você pode criar um conjunto de chaves de várias regiões com o mesmo material de chave.

Origem do material de chave

A origem do material de chave é uma propriedade da chave do KMS que identifica a origem do material de chave na chave do KMS. Você escolhe a origem do material de chave ao criar a chave do KMS e não é possível alterá-la. A origem do material de chave afeta as características de segurança, durabilidade, disponibilidade, latência e throughput da chave do KMS.

Para encontrar a origem do material de chave de uma chave KMS, use a DescribeKeyoperação ou veja o valor da origem na guia Configuração criptográfica da página de detalhes de uma chave KMS no console. AWS KMS Para obter ajuda, consulte Visualizar chaves.

As chaves do KMS podem ter um dos valores de origem de material de chave a seguir.

`AWS_KMS`

O AWS KMS cria e gerencia o material de chave para a chave do KMS no seu próprio armazenamento de chaves. Esse é o valor padrão e o recomendado para a maioria das chaves do KMS.

Para obter ajuda na criação de chaves com material de chave do AWS KMS, consulte Criar chaves.

`EXTERNAL (Import key material)`

A chave do KMS tem material de chave importado. Quando uma chave do KMS é criada com uma origem de material de chave `External`, ela não tem material de chave. Mais tarde, você poderá importar material de chave para a chave do KMS. Ao usar material de chave importada, é necessário proteger e gerenciar esse material de chave fora do AWS KMS, incluindo a substituição do material de chave se ele expirar. Para obter mais detalhes, consulte Sobre o material de chave importada.

Para obter ajuda na criação de uma chave do KMS para material de chave importado, consulte Etapa 1: criar uma chave do KMS sem material de chave.

`AWS_CLOUDHSM`

O AWS KMS cria o material de chave no cluster do AWS CloudHSM para seu armazenamento de chaves do AWS CloudHSM.

Para obter ajuda na criação de uma chave do KMS em um armazenamento de chaves do AWS CloudHSM, consulte Criar chaves do KMS em um armazenamento de chaves do AWS CloudHSM.

`EXTERNAL_KEY_STORE`

O material da chave é uma chave de criptografia em um gerenciador de chaves externas fora da AWS. Essa origem é compatível somente com chaves do KMS em um armazenamento de chaves externas.

Para obter ajuda na criação de uma chave do KMS em um armazenamento de chaves externas, consulte Criar chaves do KMS em um armazenamento de chaves externas.

Especificação da chave

A especificação da chave é uma propriedade que representa a configuração criptográfica de uma chave. O significado da especificação de chave difere com o tipo de chave.

- Chaves do AWS KMS — A especificação da chave determina se a chave do KMS é simétrica ou assimétrica. Ela também determina o tipo do material de chave e os algoritmos compatíveis. Você escolhe a especificação de chave ao criar a chave do KMS e não pode alterá-la. A especificação de chaves padrão, SYMMETRIC_DEFAULT, representa uma chave de criptografia simétrica de 256 bits.

> **Note**
>
> A `KeySpec` de uma chave do KMS era conhecida como `CustomerMasterKeySpec`. O `CustomerMasterKeySpec` parâmetro da CreateKeyoperação está obsoleto. Em vez disso, use o parâmetro `KeySpec`, que funciona da mesma maneira. Para evitar alterações significativas, a resposta das DescribeKeyoperações `CreateKey` e agora inclui ambos `KeySpec` e `CustomerMasterKeySpec` membros com os mesmos valores.

Para obter uma lista de especificações de chave e ajuda com a escolha de uma especificação de chave, consulte Selecionar a especificação de chave. Para encontrar a especificação chave de uma chave KMS, use a DescribeKeyoperação ou consulte a guia Configuração criptográfica na página de detalhes de uma chave KMS no console. AWS KMS Para obter ajuda, consulte Visualizar chaves.

Para limitar as principais especificações que os diretores podem usar ao criar chaves KMS, use a chave kms: condition. KeySpec Também é possível usar a chave de condição `kms:KeySpec` para permitir que as entidades principais chamem operações do AWS KMS somente para

chaves do KMS com uma determinada especificação de chave. Por exemplo, é possível negar permissão para programar a exclusão de qualquer chave do KMS com uma especificação de chave `RSA_4096`.

- Chaves de dados (GenerateDataKey) — A especificação da chave determina o comprimento de uma chave de dados AES.
- Pares de chaves de dados (GenerateDataKeyPair) — A especificação do par de chaves determina o tipo de material de chave no par de chaves de dados.

Uso da chave

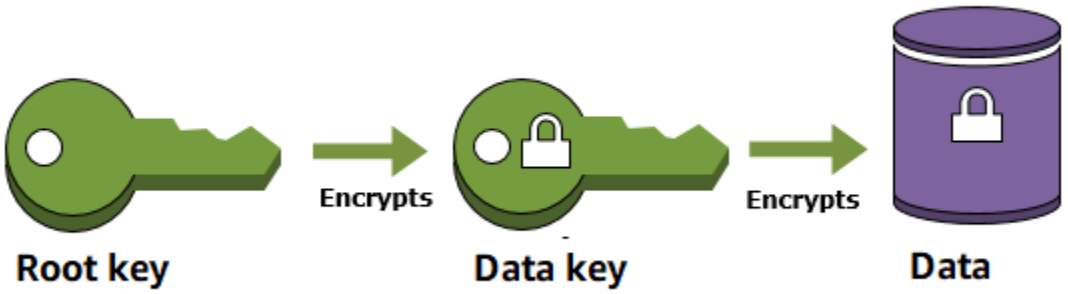
O uso da chave é uma propriedade que determina as operações de criptografia compatíveis com a chave. As chaves do KMS podem ter um uso de chave de `ENCRYPT_DECRYPT`, `SIGN_VERIFY` ou `GENERATE_VERIFY_MAC`. Cada chave do KMS pode ter apenas um uso de chave. O uso de uma chave do KMS para mais de um tipo de operação torna o produto de ambas as operações mais vulnerável a ataques.

Para obter ajuda na escolha do uso da chave do KMS, consulte Selecionar o uso de chave. Para encontrar o uso da chave KMS, use a DescribeKeyoperação ou escolha a guia Configuração criptográfica na página de detalhes de uma chave KMS no console. AWS KMS Para obter ajuda, consulte Visualizar chaves.

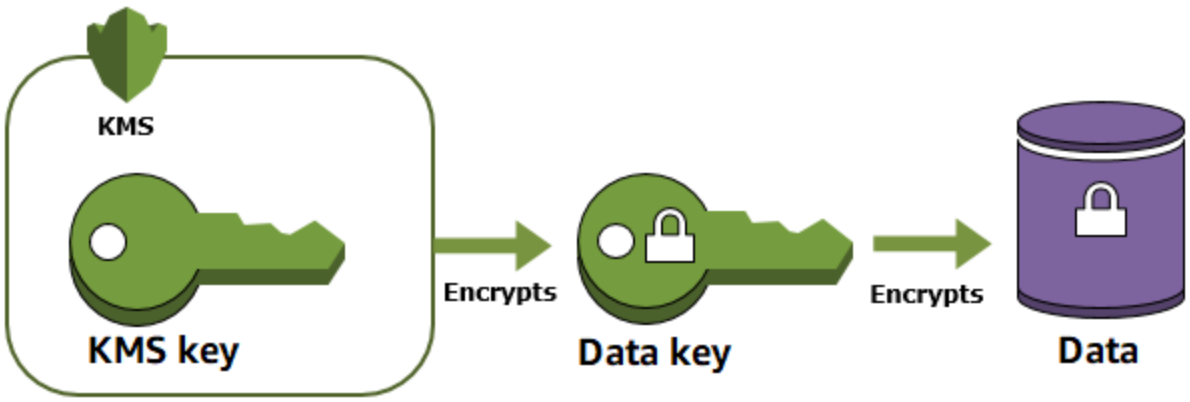
Criptografia de envelope

Quando você criptografa seus dados, os dados são protegidos, mas é necessário proteger a chave de criptografia. Uma estratégia é para criptografá-la. Criptografia de envelope é a prática de criptografar dados de texto simples com uma chave de dados e criptografar a chave de dados em outra chave.

Você pode até mesmo criptografar a chave de criptografia dos dados em outra chave de criptografia e criptografar essa chave de criptografia em outra chave de criptografia. Mas em algum momento deverá manter uma chave em texto simples para que possa descriptografar as chaves e seus dados. Essa chave de criptografia em texto simples de nível superior é chamada de chave raiz.



O AWS KMS ajuda você a proteger suas chaves de criptografia armazenando-as e gerenciando-as com segurança. As chaves-raiz armazenadas no AWS KMS, conhecidas como AWS KMS keys, nunca saem descriptografadas dos módulos de segurança de hardware validados para FIPS do AWS KMS. Para usar uma chave do KMS, é necessário chamar o AWS KMS.



A criptografia de envelope oferece vários benefícios:

- Proteção de chaves de dados

  Quando você criptografa uma chave de dados, não precisa se preocupar em armazenar a chave de dados criptografada porque a chave de dados é inerentemente protegida pela criptografia. A chave de dados criptografada pode ser armazenada com segurança junto com os dados criptografados.
- Criptografar os mesmos dados com várias chaves

  As operações de criptografia podem ser demoradas, especialmente quando os dados que estão sendo criptografados são objetos grandes. Em vez de recriptografar dados brutos várias vezes com diferentes chaves, você pode recriptografar somente as chaves de dados que protegem os dados brutos.

- Combinação de pontos fortes de vários algoritmos

  Em geral, os algoritmos de chave simétrica são mais rápidos e geram textos cifrados menores do que os algoritmos de chave pública. No entanto, os algoritmos de chave pública fornecem separação inerente de funções e gerenciamento de chaves mais fácil. A criptografia de envelope permite associar os pontos fortes de cada estratégia.

Contexto de criptografia

Todas as operações criptográficas do AWS KMS com chaves do KMS de criptografia simétrica aceitam um contexto de criptografia, um conjunto opcional de pares de chave-valor não secretos que podem conter informações contextuais adicionais sobre os dados. O AWS KMS usa o contexto de criptografia como additional authenticated data (dados autenticados adicionais (AAD)) para oferecer suporte à criptografia autenticada.

Ao incluir um contexto de criptografia em uma solicitação de criptografia, ele é vinculado de maneira criptográfica ao texto cifrado, de modo que o mesmo contexto de criptografia seja necessário para descriptografar (ou descriptografar e criptografar novamente) os dados. Se o contexto de criptografia fornecido na solicitação de descriptografia não é uma correspondência exata, com distinção entre maiúsculas e minúsculas, a solicitação de descriptografia falha. Somente a ordem dos pares de chave-valor no contexto de criptografia pode variar.

> **Note**
>
> Não é possível especificar um contexto de criptografia em uma operação criptográfica com uma chave do KMS assimétrica ou uma chave do KMS de Hash-based message authentication code (HMAC – Código de autenticação de mensagem por hash). Algoritmos assimétricos e algoritmos de Message authentication code (MAC – Código de autenticação de mensagem) não são compatíveis com um contexto de criptografia.

O contexto de criptografia não é secreto nem criptografado. Ele é exibido em texto simples em Logs do AWS CloudTrail, para você possa usá-lo para identificar e categorizar suas operações de criptografia. Seu contexto de criptografia não deve incluir informações confidenciais. Recomendamos que o seu contexto de criptografia descreva os dados que estão sendo criptografados ou descriptografados. Por exemplo, quando você criptografar um arquivo, poderá usar parte do caminho do arquivo como contexto de criptografia.

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

Por exemplo, ao criptografar volumes e snapshots criados com a operação Amazon Elastic Block Store (Amazon EBS) CreateSnapshot, o Amazon EBS usa o ID do volume como valor do contexto de criptografia.

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

Você também pode usar o contexto de criptografia para refinar ou limitar o acesso a AWS KMS keys na sua conta. Você pode usar o contexto de criptografia como uma restrição em concessões e como uma condição nas declarações de política.

Para saber como usar o contexto de criptografia para proteger a integridade dos dados criptografados, consulte a postagem Como proteger a integridade de seus dados criptografados usando AWS Key Management Service e EncryptionContext no blog AWS de segurança.

Mais informações sobre contexto de criptografia.

Regras de contexto de criptografia

O AWS KMS impõe as seguintes regras para chaves e valores de contexto de criptografia.

- A chave e o valor em um par de contexto de criptografia devem ser strings literais simples. Se você usar um tipo diferente, como um inteiro ou flutuante, o AWS KMS o interpretará como uma string.
- As chaves e valores em um contexto de criptografia podem incluir caracteres Unicode. Se um contexto de criptografia incluir caracteres que não são permitidos em políticas de chaves ou políticas do IAM, você não poderá especificar o contexto de criptografia em chaves de condição de política, como `kms:EncryptionContext:context-key` e `kms:EncryptionContextKeys`. Para obter detalhes sobre as regras de documento de política de chaves, consulte Formato de política de chaves. Para obter detalhes sobre as regras de documento de política do IAM, consulte Requisitos de nome do IAM no Guia do usuário do IAM.

Contexto de criptografia em políticas

O contexto de criptografia é usado principalmente para verificar a integridade e a autenticidade. No entanto, também é possível usar o contexto de criptografia para controlar o acesso a AWS KMS keys de criptografia simétrica em políticas de chave e em políticas do IAM.

As chaves de EncryptionContextKeys condição kmsEncryptionContext:: e kms: permitem (ou negam) uma permissão somente quando a solicitação inclui chaves de contexto de criptografia específicas ou pares de valores-chave.

Por exemplo, a instrução de política de chave a seguir permite que a função `RoleForExampleApp` use a chave do KMS em operações `Decrypt`. Ela usa a chave da condição `kms:EncryptionContext:`*`context-key`* para conceder essa permissão somente quando o contexto de criptografia na solicitação inclui um par de contexto de criptografia `AppName:ExampleApp`.

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

Para obter mais informações sobre essas chaves de condição de contexto de criptografia, consulte Chaves de condição para AWS KMS.

Contexto de criptografia em concessões

Ao criar uma concessão, você pode incluir restrições de concessão que estabelecem condições para as permissões de concessão. O AWS KMS oferece suporte a duas restrições de concessão, `EncryptionContextEquals` e `EncryptionContextSubset`, ambas envolvendo o contexto de criptografia em uma solicitação para uma operação criptográfica. Quando você usa essas restrições de concessão, as permissões na concessão são efetivas apenas quando o contexto de criptografia na solicitação para a operação criptográfica atende aos requisitos das restrições de concessão.

Por exemplo, você pode adicionar uma restrição de `EncryptionContextEquals` concessão a uma concessão que permita a GenerateDataKeyoperação. Com essa restrição, a concessão permite a operação apenas quando o contexto de criptografia na solicitação é uma correspondência com maiúsculas e minúsculas ao contexto de criptografia na restrição de concessão.

```
$ 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}
```

Uma solicitação como a seguinte da entidade principal receptora da concessão atenderia à restrição `EncryptionContextEquals`.

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

Para obter detalhes sobre as restrições de concessão, consulte Usar restrições de concessão. Para obter informações detalhadas sobre concessões, consulte the section called “Concessões”.

Registrar em log o contexto de criptografia

O AWS KMS usa o AWS CloudTrail para registrar em log o contexto de criptografia, para que você possa determinar quais chaves do KMS e dados foram acessados. A entrada de log mostra exatamente quais chaves do KMS foram usada para criptografar ou descriptografar dados específicos referenciados pelo contexto de criptografia na entrada de log.

> **Important**
>
> Como o contexto de criptografia é registrado em log, ele não deve conter informações confidenciais.

Armazenar o contexto de criptografia

Para simplificar o uso de qualquer contexto de criptografia quando você chama as operações `Decrypt` ou `ReEncrypt`, é possível armazenar o contexto de criptografia com os dados

criptografados. Recomendamos que você armazene apenas o suficiente do contexto de criptografia para ajudar a criar o contexto de criptografia por completo quando você precisar dele para criptografia ou descriptografia.

Por exemplo, se o contexto de criptografia é o caminho para um arquivo, armazene apenas parte desse caminho com o conteúdo do arquivo criptografado. Quando você precisar do contexto de criptografia completo, reconstrua-o do fragmento armazenado. Se alguém tentar violar o arquivo, como renomear ou mover para um local diferente, o valor do contexto de criptografia será alterado e a solicitação de descriptografia falhará.

Política de chaves

Ao criar uma chave do KMS, você determina quem pode usar e gerenciar essa chave do KMS. Essas permissões estão contidas em um documento chamado política de chaves. É possível usar a política de chaves para adicionar, remover ou alterar permissões a qualquer momento para uma chave gerenciada pelo cliente. Porém, não é possível editar a política de chaves para uma Chaves gerenciadas pela AWS. Para ter mais informações, consulte Políticas-chave em AWS KMS.

Concessão

Uma concessão é um instrumento de política com o qual as entidades principais da AWS podem usar AWS KMS keys em operações de criptografia. Ela também pode permitir que essas entidades visualizem uma chave do KMS (DescribeKey) e criem e gerenciem concessões. Ao autorizar o acesso a uma chave do KMS, concessões são consideradas junto com políticas de chave e políticas do IAM. Concessões geralmente são usadas para permissões temporárias, pois você pode criar uma, usar suas permissões e excluí-la sem alterar suas principais políticas ou políticas do IAM. Como concessões podem ser muito específicas e são fáceis de criar e revogar, elas geralmente são usadas para fornecer permissões temporárias ou permissões mais detalhadas.

Para obter informações detalhadas sobre concessões, incluindo a terminologia de concessões, consulte Concessões no AWS KMS.

Auditar o uso de chaves do KMS

Você pode usar AWS CloudTrail para auditar o uso da chave. CloudTrail cria arquivos de log que contêm um histórico de chamadas de AWS API e eventos relacionados à sua conta. Esses arquivos de log incluem todas as solicitações de API do AWS KMS feitas com o Console de Gerenciamento da AWS, os AWS SDKs e as ferramentas de linha de comando. Os arquivos de log também incluem solicitações para o AWS KMS que os serviços da AWS fazem em seu nome. É possível usar esses

arquivos de log para encontrar informações importantes, incluindo quando a chave do KMS foi usada, a operação solicitada, a identidade do solicitante e o endereço IP de origem. Para obter mais informações, consulte Fazendo login com AWS CloudTrail e o Manual do usuário do AWS CloudTrail.

Infraestrutura de gerenciamento de chaves

Uma prática comum na criptografia é criptografar e descriptografar com um algoritmo revisado em pares e publicamente disponível, por exemplo, AES (Advanced Encryption Standard) e uma chave secreta. Um dos principais problemas na criptografia é a grande dificuldade de manter uma chave secreta. Geralmente, esse é o trabalho de uma infraestrutura de gerenciamento de chaves (KMI). O AWS KMS opera essa infraestrutura para você. O AWS KMS cria e armazena com segurança as suas chaves raiz, chamadas de AWS KMS keys. Para obter mais informações sobre como o AWS KMS opera, consulte Detalhes criptográficos do AWS Key Management Service.

Gerenciar chaves do

Para começar a usar o AWS KMS, crie uma AWS KMS key.

Os tópicos nesta seção explicam como gerenciar a chave básica do KMS, uma chave do KMS de criptografia simétrica, desde a criação até a exclusão. Ele inclui tópicos sobre edição e visualização de teclas, marcação de chaves, habilitação e desabilitação de chaves, alternância de materiais de chaves e uso de ferramentas e serviços da AWSpara monitorar o uso de suas chaves do KMS. Ele também inclui informações sobre o uso de AWS CloudFormation para criar e gerenciar suas chaves do KMS e uma referência do estado da chave que mostra o estado de chave necessário para cada operação do AWS KMS.

Para mais informações sobre como criar, usar e gerenciar outros tipos de chaves do KMS, consulte Chaves para fins especiais.

Tópicos

- Criar chaves
- Usar aliases
- Visualizar chaves
- Editar chaves
- Marcar chaves com tags
- Habilitar e desabilitar chaves
- Girando AWS KMS keys
- Como monitorar o AWS KMS keys
- Criando AWS KMS recursos com AWS CloudFormation
- Excluir AWS KMS keys
- Principais estados das AWS KMS chaves

Criar chaves

Você pode criar AWS KMS keys no AWS Management Console ou usando a CreateKeyoperação ou um AWS CloudFormationmodelo. Durante esse processo, você escolhe o tipo de chave do KMS, sua regionalidade (região única ou várias regiões) e a origem do material de chave (o AWS KMS cria o material de chave por padrão). Não é possível alterar essas propriedades depois que a chave do

KMS é criada. Você também define a política de chaves da chave do KMS, que pode ser alterada a qualquer momento.

Este tópico explica como criar a chave básica do KMS, uma chave do KMS de criptografia simétrica para uma só região com material de chave do AWS KMS. Você pode usar essa chave do KMS para proteger seus recursos em um AWS service (Serviço da AWS). Para obter informações detalhadas sobre chaves do KMS de criptografia simétrica, consulte Especificação da chave SYMMETRIC_DEFAULT. Para obter ajuda na criação de outros tipos de chaves, consulte Chaves para fins especiais.

Se estiver criando uma chave do KMS para criptografar dados que você armazena ou gerencia em um serviço da AWS, crie uma chave do KMS de criptografia simétrica. Os serviços da AWS que são integrados ao AWS KMS usam apenas chaves do KMS de criptografia simétrica para criptografar seus dados. Esses serviços não fornecem suporte para criptografia com chaves do KMS assimétricas. Para ajudar a decidir qual tipo de chave do KMS deve ser criada, consulte Escolha de um tipo de chave do KMS.

> **Note**
>
> Agora as chaves do KMS simétricas são chamadas de chaves do KMS de criptografia simétrica. O AWS KMS é compatível com dois tipos de chaves do KMS simétricas, chaves do KMS de criptografia simétrica (o tipo padrão) e chaves do KMS de Hash-based message authentication code (HMAC – Código de autenticação de mensagem por hash), que também são chaves simétricas.

Quando você cria uma chave do KMS no console do AWS KMS, é necessário fornecer um alias (nome amigável) a ela. A operação `CreateKey` não cria um alias para a nova chave do KMS. Para criar um alias para uma chave KMS nova ou existente, use a CreateAliasoperação. Para obter informações detalhadas sobre aliases no AWS KMS, consulte Usar aliases.

Este tópico explica como criar uma chave do KMS de criptografia simétrica. Use a tabela a seguir para encontrar instruções sobre como criar chaves do KMS de diferentes tipos.

Instruções para criar chaves do KMS

Tipo de chave do KMS	Instruções
Chave de criptografia simétrica (SYMMETRIC_DEFAULT)	the section called “Criar chaves do KMS de criptografia simétrica”
Chave assimétrica	the section called “Criar chaves do KMS assimétricas”
Chave de HMAC	the section called “Criar chaves de HMAC”
Chave de várias regiões (de qualquer tipo)	the section called “Criar uma chave primária com material de chave importado” the section called “Criar uma chave de réplica com material de chave importado”
Material de chave importado (“Traga sua própria chave — BYOK”)	the section called “Etapa 1: criar uma chave do KMS sem material de chave”
Armazenamento de chaves do AWS CloudHSM	the section called “Criar chaves do KMS em um armazenamento de chaves do AWS CloudHSM”
Armazenamento externo de chaves (“Mantenha sua própria chave — HYOK”)	the section called “Criar chaves do KMS em um armazenamento de chaves externas”

Saiba mais:

- Para criar chaves de dados para criptografia do lado do cliente, use a GenerateDataKeyoperação.
- Para criar uma chave do KMS assimétrica para criptografia ou assinatura, consulte Criar chaves do KMS assimétricas.
- Para criar uma chave do KMS de HMAC, consulte Criar chaves do KMS de HMAC.
- Para criar uma chave KMS com material de chave importado (“traga sua própria chave”), consulte Etapa 1 da importação de material de chave: criar uma AWS KMS key sem material de chave.
- Para criar uma chave primária ou uma chave de réplica de várias regiões, consulte Criar chaves de várias regiões.

- Para criar uma chave do KMS em um armazenamento personalizado de chaves (a origem do material de chave é o armazenamento personalizado de chaves [CloudHSM]), consulte Criar chaves do KMS em um armazenamento de chaves do AWS CloudHSM.
- Para usar um AWS CloudFormation modelo para criar uma chave KMS, consulte AWS::KMS::Keyo Guia do AWS CloudFormation usuário.
- Para determinar se uma chave do KMS existente é simétrica ou assimétrica, consulte Identificar chaves do KMS assimétricas.
- Para usar sua chave do KMS de forma programática e em operações da interface da linha de comando, é necessário um ID de chave ou um ARN de chave. Para obter instruções detalhadas, consulte Como encontrar o ID e o ARN da chave.
- Para obter informações sobre cotas que se aplicam a chaves do KMS, consulte Cotas.

Tópicos

- Permissões para criar chaves do KMS
- Criar chaves do KMS de criptografia simétrica

Permissões para criar chaves do KMS

Para criar uma chave do KMS no console ou usando as APIs, você deve ter a seguinte permissão em uma política do IAM. Sempre que possível, use chaves de condição para limitar as permissões. Por exemplo, você pode usar a chave de KeySpec condição kms: em uma política do IAM para permitir que os diretores criem somente chaves de criptografia simétricas.

Para obter um exemplo de uma política do IAM para entidades principais que criam chaves, consulte Permitir que um usuário crie chaves do KMS.

> **Note**
>
> Tenha cuidado ao conceder permissão a entidades principais para gerenciar etiquetas e aliases. Alterar uma etiqueta ou um alias pode conceder ou negar uma permissão à chave gerenciada pelo cliente. Para obter detalhes, consulte ABAC para AWS KMS.

- kms: CreateKey é obrigatório.
- kms: CreateAlias é necessário para criar uma chave KMS no console em que um alias é necessário para cada nova chave KMS.

- kms: TagResource é necessário adicionar tags ao criar a chave KMS.
- iam: CreateServiceLinkedRole é necessário para criar chaves primárias multirregionais. Para obter detalhes, consulte Controlar o acesso a chaves de várias Regiões.

A PutKeyPolicy permissão kms: não é necessária para criar a chave KMS. A permissão `kms:CreateKey` inclui permissão para definir a política de chaves inicial. Porém, você deve adicionar essa permissão à política de chaves ao criar a chave do KMS para garantir que seja possível controlar o acesso à chave do KMS. A alternativa é usar o BypassLockoutSafetyCheckparâmetro, o que não é recomendado.

As chaves do KMS pertencem à conta da AWS na qual foram criadas. O usuário do IAM que cria uma chave do KMS não é considerado o proprietário da chave e ele não recebe automaticamente permissão para usar ou gerenciar a chave do KMS que criou. Como qualquer outra entidade principal, o criador da chave precisa obter permissão por meio de uma política de chaves, política do IAM ou concessão. No entanto, as entidades principais que têm a permissão `kms:CreateKey` podem definir a política de chave inicial e conceder a si mesmas permissão para usar ou gerenciar a chave.

Criar chaves do KMS de criptografia simétrica

É possível criar chaves do KMS no AWS Management Console ou usando a API do AWS KMS.

Este tópico explica como criar a chave básica do KMS, uma chave do KMS de criptografia simétrica para uma só região com material de chave do AWS KMS. Você pode usar essa chave do KMS para proteger seus recursos em um AWS service (Serviço da AWS). Para obter ajuda na criação de outros tipos de chaves, consulte Chaves para fins especiais.

Criar chaves do KMS de criptografia simétrica (console)

Você pode usar o AWS Management Console para criar AWS KMS keys (chaves do KMS).

> **Important**
>
> Não inclua informações confidenciais ou sigilosas no alias, na descrição ou nas tags. Esses campos podem aparecer em texto simples em CloudTrail registros e outras saídas.

1. Faça login no AWS Management Console e abra o console do AWS Key Management Service (AWS KMS) em https://console.aws.amazon.com/kms.

2. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.
3. No painel de navegação, escolha Customer managed keys (Chaves gerenciadas pelo cliente).
4. Escolha Create key (Criar chave).
5. Para criar uma chave do KMS de criptografia simétrica, em Key type (Tipo de chave), selecione Symmetric (Simétrica).

   Para obter informações sobre como criar uma chave do KMS assimétrica no console do AWS KMS, consulte Criar chaves do KMS assimétricas (console).
6. Em Key usage (Uso da chave), a opção Encrypt and decrypt (Criptografar e descriptografar) é selecionada para você.

   Para obter informações sobre como criar chaves do KMS que geram e verificam códigos de Message authentication code (MAC – Código de autenticação de mensagem), consulte Criar chaves do KMS de HMAC.
7. Escolha Próximo.

   Para mais informações sobre as opções avançadas, consulte Chaves para fins especiais.
8. Digite um alias para a chave do KMS. O nome do alias não pode começar com **`aws/`**. O prefixo **`aws/`** é reservado pela Amazon Web Services para representar as Chaves gerenciadas pela AWS na sua conta.

   > **Note**
   >
   > Adicionar, excluir ou atualizar um alias pode conceder ou negar uma permissão à chave do KMS. Para obter mais detalhes, consulte ABAC para AWS KMS e Usar aliases para controlar o acesso a chaves do KMS.

   Um alias é um nome de exibição que identifica a chave do KMS. Recomendamos que você escolha um alias que indique o tipo de dados que pretende proteger ou a aplicação a ser usada com a chave do KMS.

   Aliases são necessários ao criar uma chave do KMS no AWS Management Console. Eles são opcionais quando você usa a CreateKeyoperação.
9. (Opcional) Digite uma descrição para a chave do KMS.

Você pode adicionar uma descrição agora ou atualizá-la a qualquer momento, a não ser que o estado da chave seja `Pending Deletion` ou `Pending Replica Deletion`. Para adicionar, alterar ou excluir a descrição de uma chave gerenciada pelo cliente existente, edite a descrição na operação AWS Management Console ou use a UpdateKeyDescriptionoperação.

10. (Opcional) Digite uma chave de tag e um valor de tag opcional. Para adicionar mais de uma etiqueta à chave do KMS, selecione Add tag (Adicionar etiqueta).

> **Note**
>
> Marcar ou desmarcar uma chave do KMS pode conceder ou negar uma permissão a essa chave do KMS. Para obter mais detalhes, consulte ABAC para AWS KMS e Usar etiquetas para controlar o acesso a chaves do KMS.

Ao adicionar tags aos recursos da AWS, a AWS gera um relatório de alocação de custos com utilização e custos agrupados por tags. Etiquetas também podem ser utilizadas para controlar o acesso a uma chave do KMS. Para informações sobre marcação de chaves do KMS, consulte Marcar chaves com tags e ABAC para AWS KMS.

11. Escolha Próximo.
12. Selecione os usuários e as funções do IAM que podem administrar a chave do KMS.

> **Note**
>
> Esta política de chave concede controle total dessa chave do KMS à Conta da AWS. Ela permite que os administradores de conta usem políticas do IAM para conceder a outras entidades principais a permissão para gerenciar a chave do KMS. Para obter detalhes, consulte the section called “Política de chaves padrão”.
>
> As práticas recomendadas do IAM não encorajam o uso de usuários do IAM com credenciais de longo prazo. Sempre que possível, use os perfis do IAM, por fornecerem credenciais temporárias. Para obter detalhes, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

13. (Opcional) Para evitar que os usuários e funções do IAM selecionados excluam essa chave do KMS, na seção Key deletion (Exclusão de chaves) na parte inferior da página, desmarque a

caixa de seleção Allow key administrators to delete this key (Permitir que os administradores de chaves excluam essa chave).

14. Escolha Próximo.
15. Selecione os usuários e as funções do IAM que podem usar a chave em operações de criptografia.

> **Note**
>
> Esta política de chave concede controle total dessa chave do KMS à Conta da AWS. Ela permite que os administradores de conta usem políticas do IAM para conceder a outras entidades principais a permissão para usar a chave do KMS em operações de criptografia. Para obter detalhes, consulte the section called “Política de chaves padrão”.
>
> As práticas recomendadas do IAM não encorajam o uso de usuários do IAM com credenciais de longo prazo. Sempre que possível, use os perfis do IAM, por fornecerem credenciais temporárias. Para obter detalhes, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

16. (Opcional) Você pode permitir que outras Contas da AWS usem essa chave do KMS para operações de criptografia. Para fazer isso, na parte inferior da página na seção Other Contas da AWS (Outras), escolha Add another Conta da AWS (Adicionar outra) e insira o número de identificação da Conta da AWS de uma conta externa. Para adicionar várias contas externas, repita essa etapa.

> **Note**
>
> Para permitir que as entidades principais de contas externas usem a chave do KMS, os administradores da conta externa devem criar políticas do IAM que forneçam essas permissões. Para ter mais informações, consulte Permitir que usuários de outras contas usem uma chave do KMS.

17. Escolha Próximo.
18. Revise as configurações que você escolheu. Ainda é possível voltar e alterar todas as configurações.
19. Selecione Finish (Concluir) para criar a chave do KMS.

Criar chaves do KMS de criptografia simétrica (API do AWS KMS)

Você pode usar a CreateKeyoperação para criar AWS KMS keys de todos os tipos. Estes exemplos usam a AWS Command Line Interface (AWS CLI), mas você pode usar qualquer linguagem de programação compatível.

> **Important**
>
> Não inclua informações confidenciais ou sigilosas nos campos `Description` ou `Tags`. Esses campos podem aparecer em texto simples em CloudTrail registros e outras saídas.

A operação a seguir cria a chave do KMS mais usada, uma chave de criptografia simétrica em uma única região com o suporte de material de chave gerado por AWS KMS. Essa operação não tem os parâmetros obrigatórios. No entanto, você também pode usar o parâmetro `Policy` para especificar uma política de chaves. Você pode alterar a política de chaves (PutKeyPolicy) e adicionar elementos opcionais, como uma descrição e tags, a qualquer momento. Você também pode criar chaves assimétricas, chaves de várias Regiões, chaves com material de chave importado, e chaves em armazenamentos de chaves personalizados.

A `CreateKey` operação não permite que você especifique um alias, mas você pode usar a CreateAliasoperação para criar um alias para sua nova chave KMS.

Veja a seguir um exemplo de uma chamada para a operação `CreateKey` sem parâmetros. Esse comando usa todos os valores padrão. Ele cria uma chave do KMS de criptografia simétrica com o material de chave gerado pelo 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 você não especificar uma política de chaves para sua nova chave do KMS, a política de chave padrão aplicada por `CreateKey` será diferente da política de chaves padrão que o console aplica quando você o usa para criar uma nova chave do KMS.

Por exemplo, essa chamada para a GetKeyPolicyoperação retorna a política de chaves que `CreateKey` se aplica. Ela dá à Conta da AWS acesso à chave do KMS e permite que ele crie políticas do AWS Identity and Access Management(IAM) para a chave do KMS. Para obter informações detalhadas sobre as políticas do IAM e as políticas de chaves para chaves do KMS, consulte Autenticação e controle de acesso para o 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" : "*"
  } ]
}
```

Usar aliases

Um alias é um nome amigável para uma AWS KMS key. Por exemplo, um alias permite fazer referência a uma chave do KMS como `test-key` em vez de `1234abcd-12ab-34cd-56ef-1234567890ab`.

Você pode usar um alias para identificar uma chave KMS no AWS KMS console, na DescribeKeyoperação e em operações criptográficas, como Criptografar e. GenerateDataKey Aliases também facilitam o reconhecimento de uma Chave gerenciada pela AWS. Aliases para estas chaves do KMS sempre têm o formato: `aws/<service-name>`. Por exemplo, o alias para a Chave gerenciada pela AWS do Amazon DynamoDB é `aws/dynamodb`. É possível estabelecer padrões de alias semelhantes para seus projetos, como introduzir o nome de um projeto ou categoria em seus aliases.

Também é possível pode permitir e negar acesso a chaves do KMS com base em aliases sem precisar editar políticas ou gerenciar concessões. Esse recurso faz parte do suporte do AWS KMS para controle de acesso baseado em atributos(ABAC). Para obter mais detalhes, consulte Usar aliases para controlar o acesso a chaves do KMS.

Grande parte do poder dos aliases vem da sua capacidade de alterar a chave do KMS associada a um alias a qualquer momento. Aliases podem tornar seu código mais fácil de escrever e manter. Por exemplo, suponha que você use um alias para fazer referência a uma determinada chave do KMS e queira alterar essa chave do KMS. Nesse caso, basta associar o alias a outra chave do KMS. Você não precisa mudar o código.

Aliases também facilitam a reutilização do mesmo código em Regiões da AWS diferentes. Crie aliases com o mesmo nome em várias regiões e associe cada alias a uma chave do KMS em sua respectiva região. Quando o código é executado em cada região, o alias faz referência à chave do KMS associada nessa região. Para ver um exemplo, consulte Usar aliases em suas aplicações.

Você pode criar um alias para uma chave KMS no AWS KMS console, usando a CreateAliasAPI ou usando um AWS CloudFormation modelo.

A API do AWS KMS fornece controle total de aliases em cada conta e região. A API inclui operações para criar um alias (CreateAlias), visualizar nomes de alias e ARNs de alias (ListAliases), alterar a chave KMS associada a um alias () e excluir um alias (UpdateAlias). DeleteAlias Para obter exemplos de gerenciamento de aliases de várias linguagens de programação, consulte the section called “Trabalhar com aliases”.

Os seguintes recursos podem ajudá-lo a saber mais:

- Para obter informações sobre identificadores de chave do KMS, incluindo aliases, consulte Identificadores-chave () KeyId.
- Para obter ajuda sobre como usar um AWS CloudFormation modelo para criar um alias para uma chave KMS, consulte o AWS::KMS::AliasGuia do AWS CloudFormationusuário.

- Para obter ajuda para localizar os aliases associados a uma chave do KMS, consulte Encontrar o nome e o ARN do alias
- Para obter informações sobre cotas de recursos para aliases e cotas de taxa para operações de API relacionadas a aliases, consulte Cotas.
- Para obter exemplos de criação e gerenciamento de aliases em várias linguagens de programação, consulte Trabalhar com aliases.

Tópicos

- Sobre aliases
- Como gerenciar aliases
- Usar aliases em suas aplicações
- Controlar o acesso a aliases
- Usar aliases para controlar o acesso a chaves do KMS
- Localizar aliases em logs do AWS CloudTrail

Sobre aliases

Saiba como os aliases funcionam no AWS KMS.

Um alias é um recurso independente da AWS

Um alias não é uma propriedade de uma chave do KMS. As ações executadas no alias não afetam a chave do KMS associada. É possível criar um alias para uma chave do KMS e depois atualizá-lo para associá-lo a outra chave do KMS. Você pode até mesmo excluir o alias sem nenhum efeito sobre a chave do KMS associada. No entanto, se você excluir uma chave do KMS, todos os aliases associados a ela serão excluídos.

Se você especificar um alias como o recurso em uma política do IAM, esta fará referência ao alias, e não à chave do KMS associada.

Cada alias tem dois formatos

Quando criar um alias, especifique o nome dele. O AWS KMS cria o ARN do alias para você.

- Um ARN de alias é um Amazon Resource Name (ARN) que identifica exclusivamente o alias.

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

- Um nome de alias que é único na conta e na região. Na API do AWS KMS, o nome do alias é sempre prefixado com `alias/`. Esse prefixo é omitido no console do AWS KMS.

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

Os aliases não são secretos

Os aliases podem ser exibidos em texto simples em CloudTrail registros e outras saídas. Não inclua informações confidenciais ou sigilosas nos nomes dos alias.

Cada alias é associado a uma chave do KMS por vez

O alias e sua chave do KMS devem estar na mesma conta e região.

É possível associar um alias a qualquer chave gerenciada pelo cliente na mesma Conta da AWS e região. No entanto, você não tem permissão para associar um alias a uma Chave gerenciada pela AWS.

Por exemplo, essa ListAliasessaída mostra que o `test-key` alias está associado a exatamente uma chave KMS de destino, que é representada pela `TargetKeyId` propriedade.

```
{
     "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
}
```

Vários aliases podem ser associados à mesma chave do KMS

Por exemplo, você pode associar os aliases `test-key` e `project-key` à mesma chave do 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
}
```

O alias deve ser exclusivo em uma conta e região.

Por exemplo, é possível ter apenas um alias `test-key` em cada conta e região. Os aliases diferenciam maiúsculas de minúsculas, mas os aliases que diferem apenas no tamanho das letras são muito propensos a erros. Não é possível alterar um nome de alias. No entanto, você pode excluir o alias e criar um novo com o nome desejado.

É possível criar um alias com o mesmo nome em regiões diferentes

Por exemplo, é possível ter um alias `finance-key` na região Leste dos EUA (Norte da Virgínia) e um alias `finance-key` na região Europa (Frankfurt). Cada alias seria associado a uma chave do KMS em sua região. Se o seu código se referir a um nome de alias como `alias/finance-key`, você poderá executá-lo em várias regiões. Em cada região, ele usa uma chave do KMS diferente. Para obter detalhes, consulte Usar aliases em suas aplicações.

É possível alterar a chave do KMS associada a um alias

Você pode usar a UpdateAliasoperação para associar um alias a uma chave KMS diferente. Por exemplo, se o alias `finance-key` estiver associado à chave do KMS `1234abcd-12ab-34cd-56ef-1234567890ab`, você poderá atualizá-lo para associá-lo à chave do KMS `0987dcba-09fe-87dc-65ba-ab0987654321`.

No entanto, a chave do KMS atual e nova devem ser do mesmo tipo (ambas devem ser simétricas, assimétricas ou HMAC) e devem ter o mesmo uso de chave (ENCRYPT_DECRYPT ou SIGN_VERIFY or GENERATE_VERIFY_MAC). Essa restrição impede erros no código que usa aliases. Se for necessário associar um alias a um tipo diferente de chave e você tiver atenuado os riscos, poderá excluir e recriar o alias.

Algumas chaves do KMS não têm aliases

Ao criar uma chave do KMS no console do AWS KMS, você deve fornecer um novo alias a ela. Mas um alias não é necessário quando você usa a CreateKeyoperação para criar uma chave KMS. Além disso, você pode usar a UpdateAliasoperação para alterar a chave KMS associada a um alias e a DeleteAliasoperação para excluir um alias. Como resultado, algumas chaves do KMS podem ter vários aliases, e outras podem não ter nenhum.

A AWS cria aliases em sua conta

A AWS cria aliases em sua conta para Chaves gerenciadas pela AWS. Esses aliases têm nomes no formato `alias/aws/<service-name>`, como `alias/aws/s3`.

Alguns aliases da AWS não têm uma chave do KMS. Esses aliases predefinidos são geralmente associados a uma Chave gerenciada pela AWS quando você começa a usar o serviço.

Usar aliases para identificar chaves do KMS

Você pode usar um nome de alias ou ARN de alias para identificar uma chave KMS em operações criptográficas, e. DescribeKeyGetPublicKey (Se a chave do KMS estiver em uma Conta da AWS diferente, você deverá usar seu ARN de chave ou ARN de alias.) Aliases não são identificadores válidos para chaves do KMS em outras operações do AWS KMS. Para obter informações sobre os identificadores de chave válidos para cada operação de API do AWS KMS, consulte as descrições dos parâmetros `KeyId` na Referência de APIs do AWS Key Management Service.

Não é possível usar um nome ou um ARN de alias para identificar uma chave do KMS em uma política do IAM. Para controlar o acesso a uma chave KMS com base em seus aliases, use as chaves de condição kms: RequestAlias ou kms:. ResourceAliases Para obter detalhes, consulte ABAC para AWS KMS.

Como gerenciar aliases

Usuários autorizados podem criar, exibir e excluir aliases. Você também pode atualizar um alias, ou seja, associar um alias existente com uma chave do KMS diferente.

Tópicos

- Criar um alias
- Visualizar aliases
- Atualizar aliases
- Excluir um alias

Criar um alias

É possível criar aliases no console do AWS KMS ou usando operações de API do AWS KMS.

O alias deve ser uma string contendo de 1 até 256 caracteres. Só pode conter caracteres alfanuméricos, barras (/), sublinhados (_) e traços (-). O nome do alias de uma chave gerenciada pelo cliente não pode começar com `alias/aws/`. O prefixo `alias/aws/` está reservado para a Chave gerenciada pela AWS.

É possível criar um alias para uma nova chave do KMS ou para uma chave do KMS existente. Você pode adicionar um alias para que uma determinada chave do KMS seja usada em um projeto ou uma aplicação.

Criar um alias (console)

Quando você cria uma chave do KMS no AWS KMS, deve criar um alias para essa nova chave do KMS. Para criar um alias para uma chave do KMS existente, use a guia Aliases na página de detalhes da chave do KMS.

1. Faça login no AWS Management Console e abra o console do AWS Key Management Service (AWS KMS) em https://console.aws.amazon.com/kms.
2. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.
3. No painel de navegação, escolha Customer managed keys (Chaves gerenciadas pelo cliente). Não é possível gerenciar aliases para Chaves gerenciadas pela AWS ou Chaves pertencentes à AWS.
4. Na tabela, escolha o ID de chave ou alias da chave do KMS. Em seguida, na página de detalhes da chave do KMS, escolha a guia Aliases.

   Se uma chave do KMS tiver vários aliases, a coluna Aliases na tabela exibe um alias e um resumo de alias, como (Mais n). Escolher o resumo de aliases leva diretamente à guia Aliases na página de detalhes da chave do KMS.
5. Na guia Aliases, escolha Create alias (Criar alias). Insira um nome de alias e escolha Create alias (Criar alias).

> **Important**
>
> Não inclua informações confidenciais ou sigilosas nesse campo. Esse campo pode ser exibido em texto simples em CloudTrail registros e outras saídas.

> **Note**
>
> Não adicione o prefixo `alias/`. O console adiciona isso para você automaticamente. Se você inserir `alias/ExampleAlias`, o nome do alias real será `alias/alias/ExampleAlias`.

Criar um alias (API do AWS KMS)

Para criar um alias, use a CreateAliasoperação. Diferentemente do processo de criação de chaves KMS no console, a CreateKeyoperação não cria um alias para uma nova chave KMS.

> **Important**
>
> Não inclua informações confidenciais ou sigilosas nesse campo. Esse campo pode ser exibido em texto simples em CloudTrail registros e outras saídas.

Você pode usar a operação `CreateAlias` para criar um alias para uma nova chave do KMS sem alias. Você também pode usar a operação `CreateAlias` para adicionar um alias a qualquer chave do KMS existente ou para recriar um alias excluído acidentalmente.

Nas operações da API do AWS KMS, o nome do alias deve começar com `alias/` seguido de um nome, como `alias/ExampleAlias`. O alias deve ser exclusivo na conta e na região da . Para encontrar os nomes de alias que já estão em uso, use a ListAliasesoperação. O nome do alias diferencia maiúsculas de minúsculas.

O `TargetKeyId` pode ser qualquer chave gerenciada pelo cliente na mesma Região da AWS. Para identificar a chave do KMS, use seu ID de chave ou ARN de chave. Não é possível usar outro alias.

O exemplo a seguir cria o alias `example-key` e o associa à chave do KMS especificada. Estes exemplos usam a AWS Command Line Interface (AWS CLI). Para obter exemplos em várias linguagens de programação, consulte Trabalhar com aliases.

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

`CreateAlias` não retorna nenhuma saída. Para ver o novo alias, use a operação `ListAliases`. Para obter detalhes, consulte Exibir aliases (API AWS KMS).

Visualizar aliases

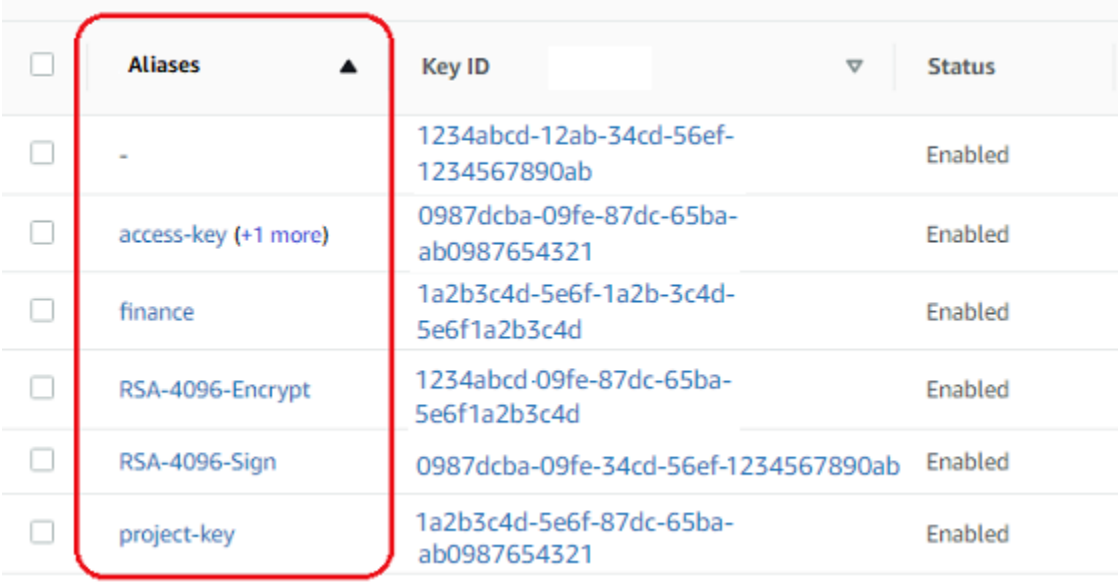
Aliases facilitam o reconhecimento de chaves do KMS no console do AWS KMS. Você pode visualizar os aliases de uma chave KMS no AWS KMS console ou usando a ListAliasesoperação. A DescribeKeyoperação, que retorna as propriedades de uma chave KMS, não inclui aliases.

Exibir aliases (console)

As páginas Customer managed keys (Chaves gerenciadas pelo cliente) e Chaves gerenciadas pela AWS no console do AWS KMS exibem o alias associado a cada chave do KMS. Você também pode pesquisar, classificar e filtrar chaves do KMS com base em seus aliases.

A imagem a seguir do console do AWS KMS mostra os aliases na página Chaves gerenciadas pelo cliente de uma conta demonstrativa. Como mostrado na imagem, algumas chaves do KMS não têm alias.

Quando uma chave do KMS tem diversos aliases, a coluna Aliases mostra um alias e um resumo de aliases (Mais n). O resumo de aliases mostra quantos aliases adicionais estão associados à chave do KMS e contém links para a exibição de todos os aliases da chave do KMS na guia Aliases.

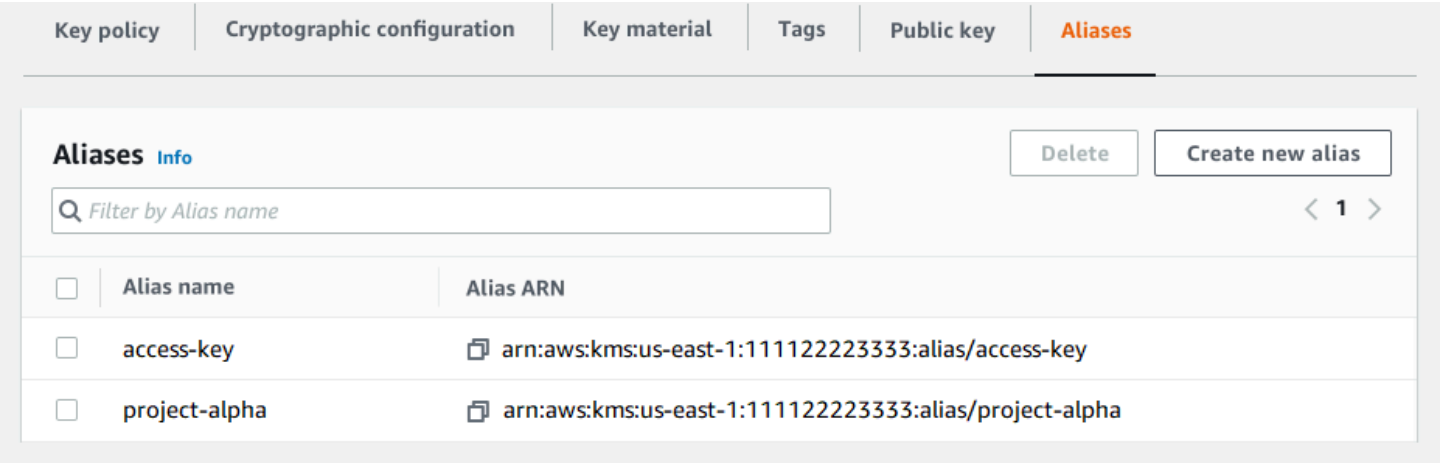


A guia Aliases na página de detalhes de cada chave do KMS mostra o nome e o ARN de todos os aliases para a chave do KMS na região e na Conta da AWS. Também é possível utilizar a guia Aliases para criar aliases e excluir aliases.

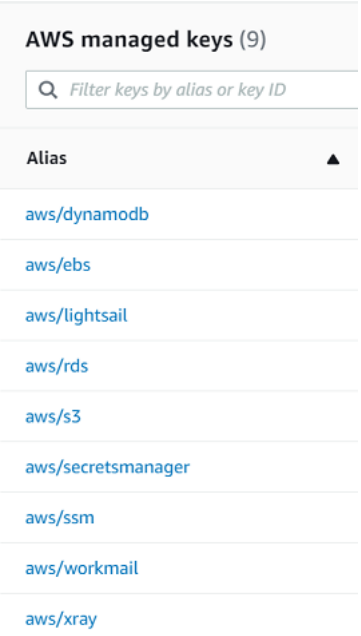
Para encontrar o nome e o ARN de todos os aliases para a chave do KMS, use a guia Aliases.

- Para acessar diretamente a guia Aliases, na coluna Aliases, escolha o resumo do alias (Mais n). Um resumo de aliases será exibido somente se a chave do KMS tiver mais de um alias.
- Outra opção é escolher o alias ou o ID da chave do KMS (que abre a página de detalhes da chave do KMS) e escolher a guia Aliases. As guias estão na seção General configuration (Configuração geral).

A seguinte imagem mostra a guia Aliases para um exemplo de chave do KMS.



É possível usar o alias para reconhecer Chave gerenciada pela AWS, como mostra este exemplo da página Chaves gerenciadas pela AWS. Os aliases de Chaves gerenciadas pela AWS sempre têm o formato: `aws/<service-name>`. Por exemplo, o alias para a Chave gerenciada pela AWS do Amazon DynamoDB é `aws/dynamodb`.



Exibir aliases (API AWS KMS)

A ListAliasesoperação retorna o nome do alias e o ARN do alias da conta e da região. A saída inclui aliases para Chaves gerenciadas pela AWS e para chaves gerenciadas pelo cliente. Os aliases para Chaves gerenciadas pela AWS têm o formato `aws/<service-name>`, como `aws/dynamodb`.

A resposta também pode incluir aliases sem campo `TargetKeyId`. Estes são aliases predefinidos criados pela AWS, mas que ainda não estão associados a uma chave do 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
        }
    ]
}
```

Para obter todos os aliases associados a uma determinada chave do KMS, use o parâmetro opcional `KeyId` da operação `ListAliases`. O parâmetro `KeyId` usa o ID de chave ou o ARN de chave da chave do KMS.

Esse exemplo obtém todos os aliases associados à chave do 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
        }
    ]
}
```

O parâmetro `KeyId` não usa caracteres curinga, mas você pode usar os recursos da linguagem de programação para filtrar a resposta.

Por exemplo, o comando da AWS CLI a seguir obtém apenas os aliases de Chaves gerenciadas pela AWS.

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

O comando a seguir obtém apenas o alias `access-key`. O nome do alias diferencia maiúsculas de minúsculas.

```
$ 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"
    }
]
```

Atualizar aliases

Como um alias é um recurso independente, é possível alterar a chave do KMS associada a ele. Por exemplo, se o `test-key` alias estiver associado a uma chave KMS, você poderá usar a UpdateAliasoperação para associá-lo a uma chave KMS diferente. Esta é uma das várias maneiras

de alternar manualmente uma chave do KMS sem alterar seu material de chave. Também é possível atualizar uma chave do KMS para que uma aplicação que estava usando uma determinada chave do KMS para novos recursos use agora uma diferente.

Não é possível atualizar um alias no console do AWS KMS. Além disso, você não pode usar `UpdateAlias` (nem qualquer outra operação) para alterar um nome de alias. Para alterar um nome de alias, exclua o alias atual e crie um novo para a chave do KMS.

Quando você atualiza um alias, a chave atual do KMS e a nova chave do KMS devem ser do mesmo tipo (ambas simétricas, assimétricas ou HMAC). Elas também devem ter o mesmo uso de chave (`ENCRYPT_DECRYPT` ou `SIGN_VERIFY` ou GENERATE_VERIFY_MAC). Essa restrição previne erros criptográficos no código que usa aliases.

O exemplo a seguir começa usando a ListAliasesoperação para mostrar que o `test-key` alias está atualmente associado à chave 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
        }
    ]
}
```

Em seguida, ele usará a operação `UpdateAlias` para alterar a chave do KMS associada ao alias `test-key` para a chave do KMS `0987dcba-09fe-87dc-65ba-ab0987654321`. Não é necessário especificar a chave do KMS atualmente associada, apenas a nova chave do KMS ("de destino"). O nome do alias diferencia maiúsculas de minúsculas.

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

Para verificar se o alias agora está associado à chave do KMS de destino, use a operação `ListAliases` novamente. Este comando de AWS CLI usa o parâmetro `--query` para obter apenas o alias `test-key`. Os campos `TargetKeyId` e `LastUpdatedDate` são atualizados.

```
$ 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
    }
]
```

Excluir um alias

Você pode excluir um alias no AWS KMS console ou usando a DeleteAliasoperação. Antes de excluir um alias, verifique se ele não está em uso. Embora a exclusão de um alias não afete a chave do KMS associada, ela pode criar problemas para qualquer aplicação que use esse alias. Se você excluir um alias por engano, poderá criar um novo alias com o mesmo nome e associá-lo à mesma chave do KMS ou a outra chave do KMS.

Se uma chave do KMS for excluída, todos os aliases associados a ela serão excluídos também.

Excluir aliases (console)

Para excluir um alias no console do AWS KMS, use a guia Aliases na página de detalhes da chave do KMS. É possível excluir vários aliases de uma chave do KMS ao mesmo tempo.

1. Faça login no AWS Management Console e abra o console do AWS Key Management Service (AWS KMS) em https://console.aws.amazon.com/kms.
2. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.
3. No painel de navegação, escolha Customer managed keys (Chaves gerenciadas pelo cliente). Não é possível gerenciar aliases para Chaves gerenciadas pela AWS ou Chaves pertencentes à AWS.
4. Na tabela, escolha o ID de chave ou alias da chave do KMS. Em seguida, na página de detalhes da chave do KMS, escolha a guia Aliases.

   Se uma chave do KMS tiver vários aliases, a coluna Aliases na tabela exibe um alias e um resumo de alias, como (Mais n). Escolher o resumo de aliases leva diretamente à guia Aliases na página de detalhes da chave do KMS.

5. Na guia Aliases, marque a caixa de seleção ao lado dos aliases que deseja excluir. Em seguida, selecione Excluir.

Excluir um alias (API do AWS KMS)

Para excluir um alias, use a DeleteAliasoperação. Essa operação exclui um alias por vez. O nome do alias faz distinção entre maiúsculas e minúsculas e deve ser precedido pelo prefixo `alias/`.

Por exemplo, o comando a seguir exclui o alias chamado `test-key`. Esse comando não retorna nenhuma saída.

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

Para verificar se o alias foi excluído, use a ListAliasesoperação. O comando a seguir usa o parâmetro `--query` na AWS CLI para obter somente o alias `test-key`. Os colchetes vazios na resposta indicam que a resposta `ListAliases` não incluiu um alias `test-key`. Para eliminar os colchetes, use o parâmetro `--output text` e o valor.

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

Usar aliases em suas aplicações

É possível usar um alias para representar uma chave do KMS no código da sua aplicação. O `KeyId` parâmetro em operações AWS KMS criptográficas, DescribeKey, e GetPublicKeyaceita um nome de alias ou ARN de alias.

Por exemplo, o comando `GenerateDataKey` a seguir usa um nome de alias (`alias/finance`) para identificar uma chave do KMS. O nome do alias é o valor do parâmetro `KeyId`.

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

Se a chave do KMS estiver em uma Conta da AWS diferente, você deverá usar um ARN de chave ou um ARN de alias nessas operações. Ao usar um ARN de alias, não se esqueça de que o alias de uma chave do KMS é definido na conta que tem a chave do KMS e que ele pode ser diferente em cada região. Para obter ajuda sobre como encontrar o ARN do alias, consulte Encontrar o nome e o ARN do alias.

Por exemplo, o seguinte comando `GenerateDataKey` usa uma chave do KMS que não está na conta do autor da chamada. O alias `ExampleAlias` está associado à chave do KMS na conta e região especificadas.

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

Um dos usos mais poderosos dos aliases é em aplicações executadas em várias Regiões da AWS. Por exemplo, você pode ter uma aplicação global que usa uma chave do KMS assimétrica RSA para assinatura e verificação.

- Na região Oeste dos EUA (Oregon) (us-west-2), você deseja usar `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.
- Na região Europa (Frankfurt) (eu-central-1), você deseja usar `arn:aws:kms:eu-central-1:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321`
- Na região Ásia-Pacífico (Singapura) (ap-southeast-1), você deseja usar `arn:aws:kms:ap-southeast-1:111122223333:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d`.

É possível criar uma versão diferente da sua aplicação em cada região ou usar um dicionário ou instrução de alternância para selecionar a chave do KMS correta para cada região. Mas é muito mais fácil criar um alias com o mesmo nome em cada região. Lembre-se de que o nome do alias diferencia maiúsculas de minúsculas.

```
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
```

Depois, use o alias em seu código. Quando seu código for executado em cada região, o alias fará referência à sua chave do KMS associada nessa região. Por exemplo, esse código chama a operação Sign com um nome de alias.

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

No entanto, existe o risco de que o alias seja excluído ou atualizado para ser associado a outra chave do KMS. Nesse caso, as tentativas da aplicação de verificar assinaturas usando o nome do alias falharão e talvez seja necessário recriar ou atualizar o alias.

Para atenuar esse risco, tenha cuidado ao conceder permissão às entidades principais para gerenciar os aliases usados em sua aplicação. Para obter detalhes, consulte Controlar o acesso a aliases.

Existem várias outras soluções para aplicações que criptografam dados em várias regiões da Regiões da AWS, incluindo AWS Encryption SDK.

Controlar o acesso a aliases

Ao criar ou alterar um alias, você afeta o alias e sua chave do KMS associada. Portanto, as entidades principais que gerenciam aliases devem ter permissão para chamar a operação no alias e em todas as chaves do KMS afetadas. É possível fornecer essas permissões usando políticas de chave, políticas do IAM e concessões.

> **Note**
>
> Tenha cuidado ao conceder permissão a entidades principais para gerenciar etiquetas e aliases. Alterar uma etiqueta ou um alias pode conceder ou negar uma permissão à chave gerenciada pelo cliente. Para obter mais detalhes, consulte ABAC para AWS KMS e Usar aliases para controlar o acesso a chaves do KMS.

Para obter informações sobre como controlar o acesso a todas as operações do AWS KMS, consulte Referência de permissões.

As permissões para criar e gerenciar aliases funcionam da forma a seguir.

kms: CreateAlias

Para criar um alias, a entidade principal precisa das seguintes permissões para o alias e a chave do KMS associada.

- `kms:CreateAlias` para o alias. Forneça essa permissão em uma política do IAM associada à entidade principal que tem permissão para criar o alias.

  A instrução de política de exemplo a seguir especifica o alias em um elemento `Resource`. Porém, é possível listar vários ARNs de alias ou especificar um padrão de alias, como “test*”. Porém, é possível especificar um valor de `Resource` de `"*"` para permitir que a entidade principal crie um alias na conta e na região. A permissão para criar um alias também pode ser incluída em uma permissão `kms:Create*` para todos os recursos em uma conta e região.

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

- `kms:CreateAlias` para a chave do KMS. Essa permissão deve ser fornecida em uma política de chave ou em uma política do IAM delegada a partir da política de chaves.

```
{
  "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": "*"
}
```

Você pode usar chaves de condição para limitar as chaves do KMS que podem ser associadas a um alias. Por exemplo, você pode usar a chave de KeySpec condição kms: para permitir que o principal crie aliases somente em chaves KMS assimétricas. Para obter uma lista completa de chaves de condições que podem ser usadas para limitar a permissão `kms:CreateAlias` em recursos de chaves do KMS, consulte AWS KMS permissões.

kms: ListAliases

Para listar aliases na conta e na região, a entidade principal deve ter a permissão `kms:ListAliases` em uma política do IAM. Como essa política não está relacionada a uma chave do KMS ou recurso de alias específico, o valor do elemento de recurso na política deve ser `"*"`.

Por exemplo, a instrução de política do IAM a seguir dá à entidade principal permissão para listar todas as chaves do KMS e aliases na conta e na região.

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

kms: UpdateAlias

Para alterar a chave do KMS associada a um alias, a entidade principal precisa de três elementos de permissão: um para o alias, um para a chave do KMS atual e outro para a nova chave do KMS.

Por exemplo, suponha que você queira alterar o alias `test-key` da chave do KMS com ID de chave 1234abcd-12ab-34cd-56ef-1234567890ab para a chave do KMS com ID de chave 0987dcba-09fe-87dc-65ba-ab0987654321. Nesse caso, inclua declarações de política semelhantes aos exemplos desta seção.

- `kms:UpdateAlias` para o alias. Forneça essa permissão em uma política do IAM associada à entidade principal. A política do IAM a seguir define um alias específico. Porém, é possível listar vários ARNs de alias ou especificar um padrão de alias, como `"test*"`. Porém, é possível

especificar um valor de `Resource` de `"*"` para permitir que a entidade principal atualize um alias na conta e na região.

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

- `kms:UpdateAlias` para a chave do KMS que está atualmente associada ao alias. Essa permissão deve ser fornecida em uma política de chave ou em uma política do IAM delegada a partir da política de chaves.

```
{
  "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` para a chave do KMS que a operação associa ao alias. Essa permissão deve ser fornecida em uma política de chave ou em uma política do IAM delegada a partir da política de chaves.

```
{
  "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": "*"
```

```
}
```

Você pode usar chaves de condição para limitar uma ou ambas as chaves do KMS em uma operação `UpdateAlias`. Por exemplo, você pode usar uma chave de ResourceAliases condição kms: para permitir que o principal atualize os aliases somente quando a chave KMS de destino já tiver um alias específico. Para obter uma lista completa de chaves de condições que podem ser usadas para limitar a permissão `kms:UpdateAlias` em um recurso de chave do KMS, consulte AWS KMS permissões.

kms: DeleteAlias

Para excluir um alias, a entidade principal precisa de permissão para o alias e a chave do KMS associada.

Como sempre, tenha cuidado ao conceder permissão às entidades principais para excluir um recurso. No entanto, a exclusão de um alias não afeta a chave do KMS associada. Embora isso possa causar uma falha em uma aplicação dependente do alias, se você excluir um alias por engano, poderá recriá-lo.

- `kms:DeleteAlias` para o alias. Forneça essa permissão em uma política do IAM associada à entidade principal que tem permissão para excluir o alias.

  A declaração de política demonstrativa a seguir especifica o alias em um elemento `Resource`. Porém, é possível listar vários ARNs de alias ou especificar um padrão de alias, como `"test*"`. Também é possível especificar um valor `Resource` de `"*"` para permitir que a entidade principal exclua qualquer alias na conta e na região.

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

- `kms:DeleteAlias` para a chave do KMS associada. Essa permissão deve ser fornecida em uma política de chave ou em uma política do IAM delegada a partir da política de chaves.

```
{
  "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": "*"
}
```

Limitar permissões de alias

É possível usar chaves de condição para limitar permissões de alias quando o recurso é uma chave do KMS. Por exemplo, a política do IAM a seguir permite as operações de alias em chaves do KMS em uma determinada conta e região. No entanto, ele usa a chave de KeyOrigin condição kms: para limitar ainda mais as permissões às chaves KMS com material de chave de. AWS KMS

Para obter uma lista completa de chaves de condições que podem ser usadas para limitar a permissão de alias em um recurso de chave do KMS, consulte AWS KMS permissões.

```
{
  "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"
    }
  }
}
```

Você não pode usar chaves de condição em uma instrução de política na qual o recurso é um alias. Para limitar os aliases que uma entidade principal pode gerenciar, use o valor da propriedade `Resource` da instrução de política do IAM que controla o acesso ao alias. Por exemplo, as instruções de política a seguir permitem que a entidade principal crie, atualize ou exclua qualquer alias na região e Conta da AWS, a menos que o alias comece com `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*"
}
```

Usar aliases para controlar o acesso a chaves do KMS

Você pode controlar o acesso às chaves do KMS de acordo com os aliases associados à chave do KMS. Para fazer isso, use as teclas de ResourceAliases condição kms: RequestAlias e kms:. Esse recurso faz parte do suporte do AWS KMS para controle de acesso baseado em atributos(ABAC).

A chave de condição `kms:RequestAlias` permite ou nega acesso a uma chave do KMS de acordo com o alias em uma solicitação. A chave de condição `kms:ResourceAliases` permite ou nega acesso a uma chave do KMS de acordo com os aliases associados à chave do KMS.

Esses recursos não permitem identificar uma chave do KMS usando um alias no elemento `resource` de uma instrução de política. Quando um alias é o valor de um elemento `resource`, a política aplica-se ao recurso de alias, e não a qualquer chave do KMS que possa estar associada a ela.

> **Note**
>
> Pode levar até cinco minutos para que alterações de etiqueta e alias afetem a autorização de chaves do KMS. Alterações recentes podem estar visíveis em operações de API antes de afetarem a autorização.

Ao usar aliases para controlar o acesso a chaves do KMS, considere o seguinte:

- Use aliases para reforçar as práticas recomendadas de acesso com privilégio mínimo. Conceda às entidades principais do IAM somente as permissões de que eles precisam para as chaves do KMS que elas devem usar ou gerenciar. Por exemplo, use aliases para identificar as chaves do KMS usadas para um projeto. Em seguida, conceda permissão à equipe do projeto para usar apenas chaves do KMS com os aliases do projeto.
- Tenha cautela ao conceder às entidades principais as permissões `kms:CreateAlias`, `kms:UpdateAlias` ou `kms:DeleteAlias`, que permitem adicionar, editar e excluir aliases. Quando você usa aliases para controlar o acesso a chaves do KMS, a alteração de um alias pode conceder às entidades principais permissão para usar chaves do KMS para as quais, de outra forma, eles não teriam permissão para usar. Ele também pode negar acesso a chaves do KMS que outras entidades principais exigem para realizar seus trabalhos.
- Analise as entidades principais na sua Conta da AWS que atualmente têm permissão para gerenciar aliases e ajuste essas permissões, se necessário. Os administradores de chaves que não têm permissão para alterar políticas de chave ou criar concessões podem controlar o acesso a chaves do KMS quando têm a devida permissão para gerenciar aliases.

  Por exemplo, a política de chaves padrão para administradores de chaves do console inclui as permissões `kms:CreateAlias`, `kms:DeleteAlias` e `kms:UpdateAlias`. As políticas do IAM podem dar permissões de alias para todas as chaves do KMS na sua Conta da AWS. Por exemplo, a política AWSKeyManagementServicePowerUsergerenciada permite que os diretores criem, excluam e listem aliases para todas as chaves do KMS, mas não as atualizem.
- Antes de definir uma política que depende de um alias, analise os aliases nas chaves do KMS da sua Conta da AWS. Assegure-se de que sua política se aplique somente aos aliases que você pretende incluir. Use CloudTrail registros e CloudWatch alarmes para alertá-lo sobre alterações de alias que podem afetar o acesso às suas chaves KMS. Além disso, a ListAliasesresposta inclui a data de criação e a data da última atualização de cada alias.

- As condições de política de alias usam correspondência de padrões. Elas não estão vinculadas a uma instância específica de um alias. Uma política que usa chaves de condição com base em alias afeta todos os aliases novos e existentes que correspondem ao padrão. Se você excluir e recriar um alias que corresponde a uma condição de política, esta última se aplicará ao novo alias e também ao antigo.

A chave de condição `kms:RequestAlias` depende do alias especificado explicitamente em uma solicitação de operação. A chave de condição `kms:ResourceAliases` depende dos aliases associados a uma chave do KMS, mesmo que eles não apareçam na solicitação.

kms: RequestAlias

Permita ou negue o acesso a uma chave do KMS de acordo com o alias que identifica essa chave em uma solicitação. Você pode usar a chave de RequestAlias condição kms: em uma política de chaves ou política do IAM. Ela se aplica às operações que usam um alias para identificar uma chave KMS em uma solicitação, ou seja, operações criptográficas, e. DescribeKeyGetPublicKey Não é válido para operações de alias, como CreateAliasou DeleteAlias.

Na chave de condição, especifique um nome de alias ou um padrão de nome de alias. Você não pode especificar um ARN de alias.

Por exemplo, a seguinte instrução de política de chaves permite que as entidades principais usem as operações especificadas na chave do KMS. A permissão será efetiva apenas quando a solicitação usar um alias que inclui `alpha` para identificar a chave do 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*"
```

```
    }
  }
}
```

O seguinte exemplo de solicitação de uma entidade principal autorizada atenderia à condição. No entanto, uma solicitação que usasse um ID de chave, um ARN de chave ou um alias diferente não atenderia à condição, mesmo que esses valores identificassem a mesma chave do KMS.

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

kms: ResourceAliases

Permita ou negue acesso a uma chave do KMS de acordo com os aliases associados à chave do KMS, mesmo que o alias não seja usado em uma solicitação. A chave de ResourceAliases condição kms: permite especificar um alias ou padrão de alias, como`alias/test*`, para que você possa usá-la em uma política do IAM para controlar o acesso a várias chaves do KMS na mesma região. Isso é válido para qualquer operação AWS KMS que use uma chave do KMS.

Por exemplo, a seguinte política do IAM permite que as entidades principais gerenciem a alternância automática de chaves do KMS em duas Contas da AWS. No entanto, a permissão apenas é aplicada a chaves do KMS associadas a aliases que começam com `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*"
```

```
        }
      }
    }
  ]
}
```

A condição `kms:ResourceAliases` é uma condição do recurso, e não a solicitação. Dessa forma, uma solicitação que não especifique o alias ainda pode atender à condição.

O seguinte exemplo de solicitação, que especifica um alias correspondente, atende à condição.

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

No entanto, o seguinte exemplo de solicitação também atende à condição, desde que a chave do KMS especificada tenha um alias que comece com `restricted`, mesmo que este não seja utilizado na solicitação.

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

Localizar aliases em logs do AWS CloudTrail

Você pode usar um alias para representar uma AWS KMS key em uma operação de API do AWS KMS. Ao fazer isso, o alias e o ARN da chave do KMS são registrados na entrada de log do AWS CloudTrail referente ao evento. O alias é exibido no campo `requestParameters`. O ARN de chave é exibido no campo `resources`. Esse é o caso mesmo quando um serviço da AWS usa uma Chave gerenciada pela AWS na sua conta.

Por exemplo, a GenerateDataKeysolicitação a seguir usa o `project-key` alias para representar uma chave KMS.

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

Quando essa solicitação é registrada no CloudTrail registro, a entrada do registro inclui o alias e o ARN da chave KMS real que foi usada.

```
{
    "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"
}
```

Para obter detalhes sobre AWS KMS as operações de registro em CloudTrail registros, consulteRegistrando chamadas de AWS KMS API com AWS CloudTrail.

Visualizar chaves

Você pode usar o AWS Management Console ou a API do AWS Key Management Service (AWS KMS) para visualizar as AWS KMS keys em cada conta e região, incluindo chaves do KMS que você gerencia e chaves do KMS gerenciadas pela AWS.

Tópicos

- Visualizar chaves do KMS no console
- Visualizar chaves do KMS com a API
- Exibir a configuração criptográfica de chaves do KMS
- Como encontrar o ID e o ARN da chave
- Encontrar o nome e o ARN do alias

Visualizar chaves do KMS no console

No AWS Management Console, é possível visualizar listas de suas chaves do KMS na conta e região, além de detalhes sobre cada uma das chaves do KMS.

> **Note**
>
> O console do AWS KMS exibe as chaves do KMS para as quais você tem permissão de visualizar em sua conta e sua região. Chaves do KMS em outras Contas da AWS não aparecem no console, mesmo que você tenha permissão para visualizar, gerenciar e usá-las. Para visualizar as chaves KMS em outras contas, use a DescribeKeyoperação.

Tópicos

- Navegar até as tabelas de chaves
- Navegar até detalhes de chaves
- Classificar e filtrar as chaves do KMS
- Exibir detalhes de chaves do KMS
- Personalizar suas tabelas de chaves do KMS

Navegar até as tabelas de chaves

As AWS KMS keys em cada conta e região são exibidas em tabelas. Existem tabelas separadas para as chaves do KMS que você cria e aquelas que a AWS cria para você.

1. Faça login no AWS Management Console e abra o console do AWS Key Management Service (AWS KMS) em https://console.aws.amazon.com/kms.

2. Para alterar a Região da AWS, use o Region selector (Seletor de regiões) no canto superior direito da página.
3. Para exibir as chaves em sua conta que você cria e gerencia, no painel de navegação, escolha Customer managed keys (Chaves gerenciadas de cliente). Para visualizar as chaves na sua conta que a AWS cria e gerencia para você, no painel de navegação, escolha AWS managed keys (Chaves gerenciadas pela AWS). Para obter informações sobre os diferentes tipos de chaves do KMS, consulte AWS KMS keys.

> **Tip**
>
> Para visualizar as Chaves gerenciadas pela AWS que não têm um alias, use a página Customer managed keys (Chaves gerenciadas pelo cliente).
> O console do AWS KMS também exibe os armazenamentos de chaves personalizados na conta e na região. As chaves do KMS que você cria em armazenamentos de chaves personalizados aparecem na página Customer managed keys (Chaves gerenciadas pelo cliente). Para obter informações sobre os armazenamentos de chaves personalizados, consulte Armazenamentos de chaves personalizados.

Navegar até detalhes de chaves

Existe uma página de detalhes para cada AWS KMS key na conta e Região. A página de detalhes exibe a seção General configuration (Configuração geral) da chave do KMS e inclui guias para que os usuários autorizados visualizem e gerenciem a Configuração criptográfica e a Política de chaves da chave. Dependendo do tipo de chave, a página de detalhes também pode incluir as guias Aliases, Key material (Material de chave), Key rotation (Alternância de chaves), Public key (Chave pública), Regionality (Regionalidade) e Tags (Etiquetas).

Para navegar até a página de detalhes de uma chave do KMS.

1. Faça login no AWS Management Console e abra o console do AWS Key Management Service (AWS KMS) em https://console.aws.amazon.com/kms.
2. Para alterar a Região da AWS, use o Region selector (Seletor de regiões) no canto superior direito da página.
3. Para exibir as chaves em sua conta que você cria e gerencia, no painel de navegação, escolha Customer managed keys (Chaves gerenciadas de cliente). Para visualizar as chaves na sua conta que a AWS cria e gerencia para você, no painel de navegação, escolha AWS managed

keys (Chaves gerenciadas pela AWS). Para obter informações sobre os diferentes tipos de chaves do KMS, consulte AWS KMS key.

4. Para abrir a página de detalhes da chave, na tabela de chaves, escolha o ID ou alias da chave do KMS.

   Se a chave do KMS incluir vários aliases, um resumo de aliases (+mais n) será exibido do lado do nome de um dos aliases. Escolher resumo de aliases leva você diretamente à guia Aliases na página de detalhes da chave.

Classificar e filtrar as chaves do KMS

Para facilitar a localização das chaves do KMS no console, é possível classificar e filtrar as tabelas de chaves.

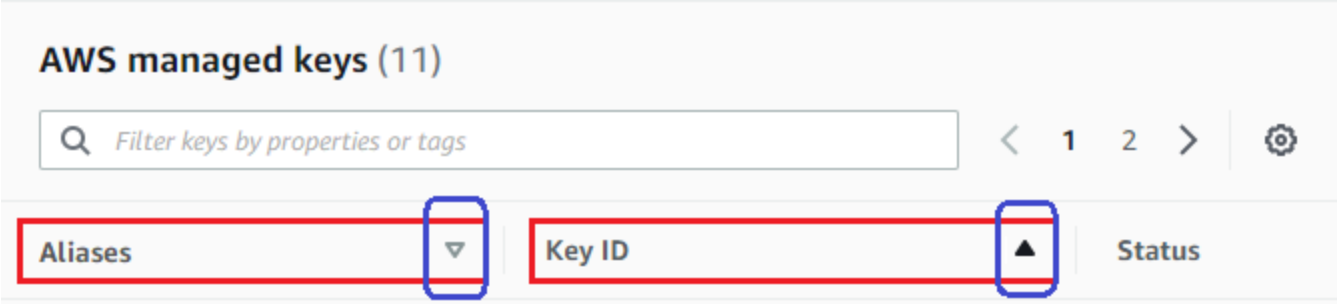
Classificar

É possível classificar chaves do KMS gerenciadas pelo cliente em ordem ascendente ou descendente pelos valores da coluna. Esse recurso classifica todas as chaves do KMS da tabela, mesmo se elas não forem exibidas na página atual da tabela.

As colunas classificáveis são indicadas por uma seta ao lado do nome da coluna. Na página Chaves gerenciadas pela AWS, você pode classificar por Aliases ou ID da chave. Na página Customer managed keys (Chaves gerenciadas pelo cliente), é possível classificar por Aliases, Key ID (ID de chave) ou Key type (Tipo de chave).

Para classificar em ordem ascendente, selecione o cabeçalho da coluna até que a seta aponte para cima. Para classificar em ordem descendente, selecione o cabeçalho da coluna até que a seta aponte para baixo. É possível classificar apenas por uma coluna de cada vez.

Por exemplo, é possível classificar chaves do KMS em ordem crescente por ID de chave, em vez de aliases, que é o padrão.



Ao classificar as chaves do KMS na página Customer managed keys (Chaves gerenciadas pelo cliente) em ordem crescente por Key type (Tipo de chave), todas as chaves assimétricas são exibidas antes de todas as chaves simétricas.

Filtro

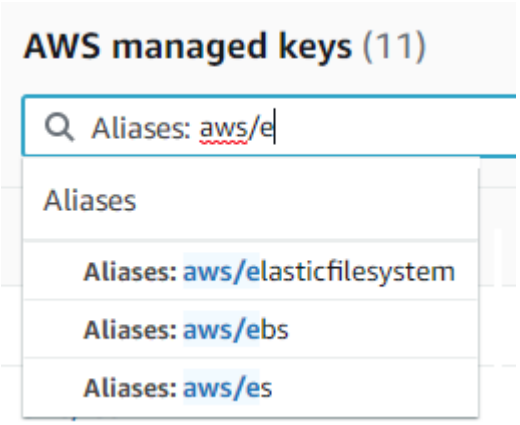
É possível filtrar todas as chaves do KMS com base em seus valores de propriedade ou etiquetas. O filtro aplica-se a todas as chaves do KMS da tabela, mesmo se elas não forem exibidas na página atual da tabela. O filtro não diferencia letras maiúsculas de minúsculas.

As propriedades filtráveis são listadas na caixa de filtro. Na página Chaves gerenciadas pela AWS, é possível filtrar por alias e ID da chave. Na página Customer managed keys (Chaves gerenciadas pelo cliente), é possível filtrar por alias, ID de chave e tipo de chave, bem como por etiquetas.

- Na página Chaves gerenciadas pela AWS, é possível filtrar por alias e ID da chave.
- Na página Customer managed keys (Chaves gerenciadas pelo cliente), é possível filtrar por etiquetas ou por alias, ID de chave, tipo de chave e regionalidade.

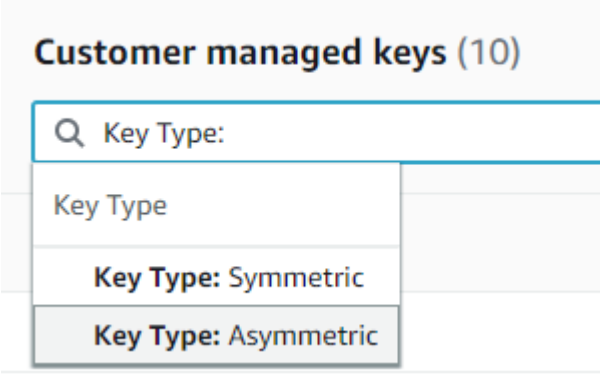
Para filtrar com base em um valor de propriedade, selecione o filtro, o nome da propriedade e uma opção na lista de valores de propriedade reais. Para filtrar com base em uma etiqueta, escolha a chave de etiqueta e depois selecione uma opção na lista de valores de etiquetas reais. Depois de escolher uma chave de etiqueta ou propriedade, também é possível digitar todo o valor da propriedade ou da etiqueta, ou parte do valor. Será exibida uma previsualização dos resultados antes de você fazer sua escolha.

Por exemplo, para exibir chaves do KMS com um nome de alias que contenha `aws/e`, escolha a caixa de filtro, escolha Alias, digite `aws/e` e pressione `Enter` ou `Return` para adicionar o filtro.

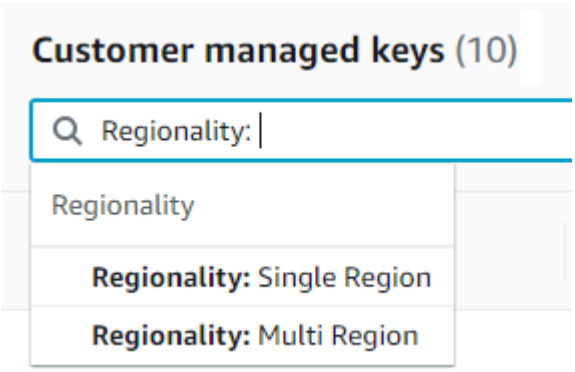


Para exibir somente chaves do KMS assimétricas na página Customer managed keys (Chaves gerenciadas pelo cliente), clique na caixa de filtro, escolha Key type (Tipo de chave) e escolha

Key type: Asymmetric (Tipo de chave: assimétrica). A opção Asymmetric (Assimétrica) é exibida somente quando você tem chaves do KMS assimétricas na tabela. Para saber mais sobre como identificar chaves do KMS assimétricas, consulte Identificar chaves do KMS assimétricas.



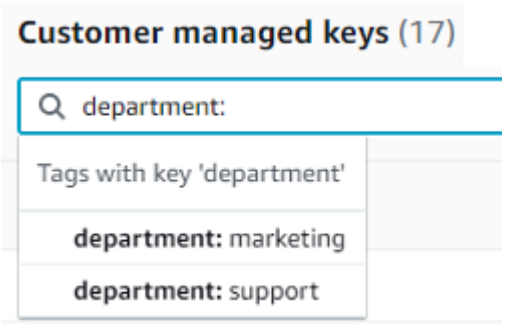
Para exibir apenas as chaves de várias Regiões, na página Customer managed keys (Chaves gerenciadas pelo cliente), selecione a caixa de filtro, escolha Regionality (Regionalidade) e depois Regionality: Multi-Region (Regionalidade: várias regiões). A opção Multi-Region (Várias regiões) será exibida apenas quando você tiver chaves de várias Regiões na tabela. Para saber mais sobre como identificar chaves de várias Regiões, consulte Visualizar chaves de várias regiões.



A filtragem de etiquetas é um processo relativamente diferente. Para exibir apenas chaves do KMS com uma etiqueta específica, selecione a caixa de filtro, a chave de etiqueta e entre os valores de etiquetas reais. Também é possível digitar todo o valor da etiqueta ou parte dele.

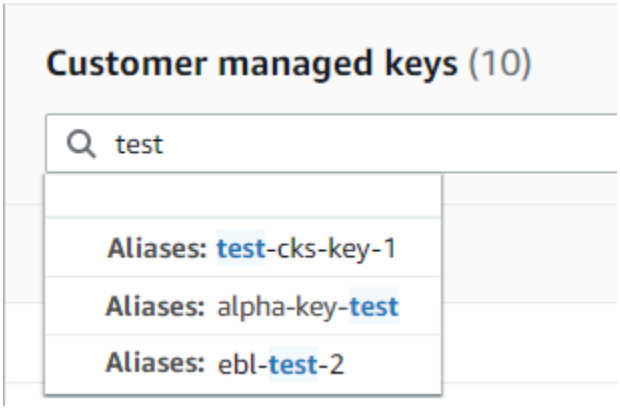
A tabela resultante mostra todas as chaves do KMS com a etiqueta selecionada. Porém, essa tabela não mostra a etiqueta. Para ver a etiqueta, selecione o alias ou o ID da chave da KMS e, na página de detalhes, escolha a guia Tags (Etiquetas). As guias aparecem sob a seção General configuration (Configuração geral).

Esse filtro exige a chave e o valor da etiqueta. Ele não localizará chaves do KMS apenas com a chave da etiqueta ou apenas com seu valor. Para filtrar as tags por toda ou parte da chave ou valor da tag, use a ListResourceTagsoperação para obter chaves KMS marcadas e, em seguida, use os recursos de filtragem da sua linguagem de programação. Para ver um exemplo, consulte ListResourceTags: Obtenha as tags nas chaves KMS.

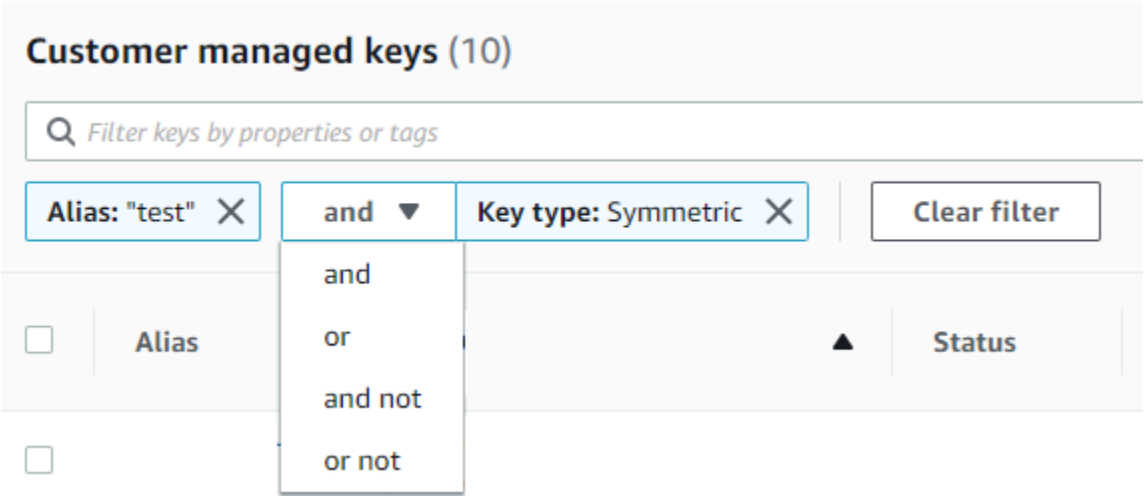


Para procurar texto, na caixa de filtragem, digite todo o alias, ou parte dele, o ID de chave, o tipo de chave ou a chave da etiqueta. (Após a seleção da chave da etiqueta, você poderá procurar um valor de etiqueta). Será exibida uma previsualização dos resultados antes de você fazer sua escolha.

Por exemplo, para mostrar chaves do KMS com `test` em suas chaves de etiqueta ou propriedades filtráveis, digite `test` na caixa de filtragem. A previsualização exibe as chaves do KMS que o filtro selecionará. Nesse caso, `test` aparece somente na propriedade Alias.



É possível usar vários filtros ao mesmo tempo. Ao adicionar outros filtros, você também poderá escolher um operador lógico.

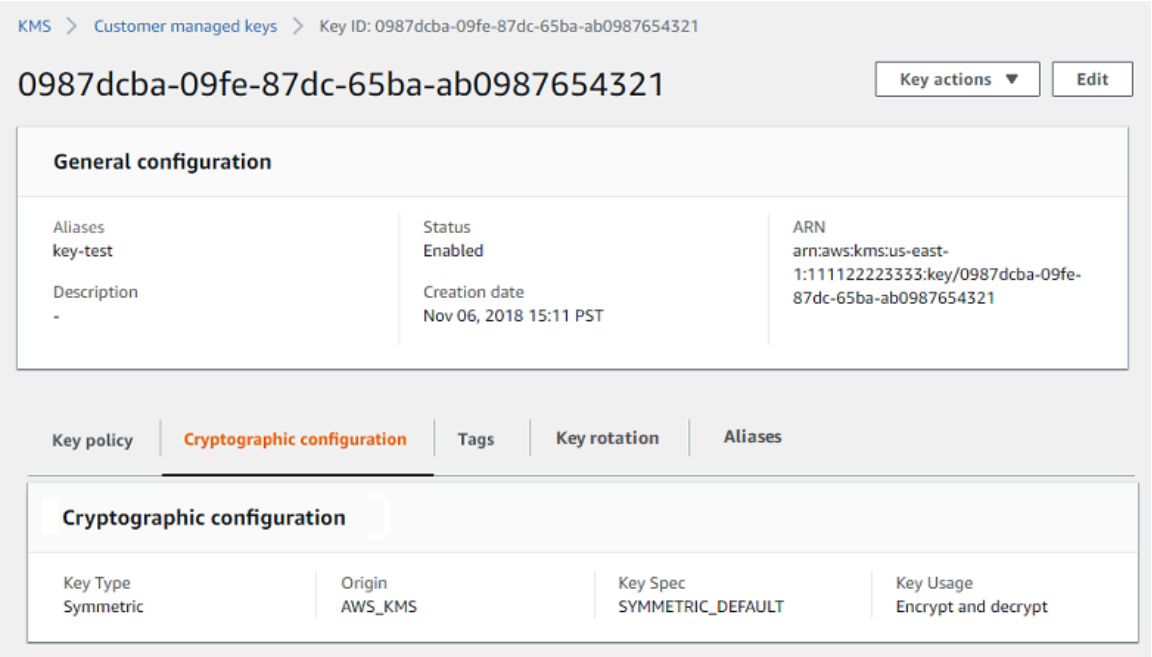


Exibir detalhes de chaves do KMS

A página de detalhes de cada chave do KMS mostra as propriedades da chave do KMS. Ela difere ligeiramente de acordo com os diversos tipos de chaves do KMS.

Para exibir informações detalhadas sobre uma chave do KMS, na página Chaves gerenciadas pela AWS ou Customer managed keys (Chaves gerenciadas pelo cliente), escolha o alias ou ID da chave do KMS.

A página de detalhes de uma chave do KMS contém uma seção General configuration (Configuração Geral), que mostra as propriedades básicas da chave do KMS. Ela também inclui guias nas quais é possível visualizar e editar propriedades da chave do KMS, Key policy (Política de chave), Cryptographic configuration (Configuração criptográfica), Tags (Etiquetas), Key material (Material de chave) (para chaves do KMS com material de chave importado), Key rotation (Alternância de chaves) (para chaves do KMS de criptografia simétrica), Regionality (Regionalidade) (para chaves de várias regiões) e Public key (Chave pública) (para chaves do KMS de criptografia assimétrica).



A lista a seguir descreve os campos na exibição detalhada, incluindo o campo nas guias. Alguns desses campos também estão disponíveis como colunas na exibição de tabela.

Aliases

Local: guia Aliases

Um nome amigável para a chave do KMS. Você pode usar um alias para identificar a chave do KMS no console e em algumas APIs do AWS KMS. Para obter detalhes, consulte Usar aliases.

A guia Aliases mostra os aliases associados à chave do KMS na Conta da AWS e na Região.

ARN

Local: seção General configuration (Configuração geral)

O nome do recurso da Amazon (ARN) da chave do KMS. Esse valor identifica exclusivamente a chave do KMS. É possível usá-lo para identificar a chave do KMS nas operações de API do AWS KMS.

Estado da conexão

Indica se um armazenamento de chaves personalizado está conectado a seu armazenamento de chaves de reserva. Esse campo é exibido somente quando a chave do KMS é criada em um armazenamento de chaves personalizado.

Para obter informações sobre os valores nesse campo, consulte ConnectionStatena Referência da AWS KMS API.

Data de Criação

Local: seção General configuration (Configuração geral)

A data e a hora em que a chave do KMS foi criada. Esse valor é exibido na hora local do dispositivo. O fuso horário não depende da região.

Diferente de Expiration (Validade), a criação se refere somente à chave do KMS, e não ao seu material de chave.

ID do cluster do CloudHSM

Local: guia Cryptographic configuration (Configuração criptográfica)

O ID do cluster do AWS CloudHSM que contém o material de chave da chave do KMS. Esse campo é exibido somente quando a chave do KMS é criada em um armazenamento de chaves personalizado.

Se você escolher o ID do cluster do CloudHSM, a página Clusters será aberta no console do AWS CloudHSM.

ID do armazenamento de chaves personalizado

Local: guia Cryptographic configuration (Configuração criptográfica)

O ID do armazenamento de chaves personalizado que contém a chave do KMS. Esse campo é exibido somente quando a chave do KMS é criada em um armazenamento de chaves personalizado.

Se você escolher ID do armazenamento de chaves personalizado, a página Custom key stores (Armazenamentos de chaves personalizados) será aberta no console do AWS KMS.

Nome do armazenamento de chaves personalizado

Local: guia Cryptographic configuration (Configuração criptográfica)

O nome do armazenamento de chaves personalizado que contém a chave do KMS. Esse campo é exibido somente quando a chave do KMS é criada em um armazenamento de chaves personalizado.

Tipo do armazenamento de chaves personalizado

Local: guia Cryptographic configuration (Configuração criptográfica)

Indica se o armazenamento de chaves personalizado é um armazenamento de chaves do AWS CloudHSM ou um armazenamento de chaves externas. Esse campo é exibido somente quando a chave do KMS é criada em um armazenamento de chaves personalizado.

Descrição

Local: seção General configuration (Configuração geral)

Uma descrição breve e opcional da chave do KMS que é possível escrever e editar. Para adicionar ou atualizar a descrição de uma chave gerenciada pelo cliente, acima de General Configuration (Configuração geral), selecione Edit (Editar).

Algoritmos de criptografia

Local: guia Cryptographic configuration (Configuração criptográfica)

Lista os algoritmos de criptografia que podem ser usados com a chave do KMS no AWS KMS. Esse campo é exibido somente quando o Key type (Tipo de chave) é Asymmetric (Assimétrico) e o Key usage (Uso da chave) é Encrypt and decrypt (Criptografar e descriptografar). Para obter informações sobre os algoritmos de criptografia compatíveis com o AWS KMS, consulte Especificação da chave SYMMETRIC_DEFAULT e Especificações de chave RSA para criptografia e descriptografia.

Data de validade

Local: guia Key material (Material da chave)

A data e a hora quando o material de chave da chave do KMS expira. Esse campo é exibido somente para chaves do KMS com material de chave importado, ou seja, quando a Origem é Externa e a chave do KMS tem material de chave que expira.

ID da chave externa

Local: guia Cryptographic configuration (Configuração criptográfica)

O ID da chave externa associada a uma chave do KMS que está em um armazenamento de chaves externas. Esse campo é exibido somente para chaves do KMS em um armazenamento de chaves externas.

Status da chave externa

Local: guia Cryptographic configuration (Configuração criptográfica)

O status mais recente que o proxy do armazenamento de chaves externas relatou para a chave externa associada à chave do KMS. Esse campo é exibido somente para chaves do KMS em um armazenamento de chaves externas.

Uso de chaves externas

Local: guia Cryptographic configuration (Configuração criptográfica)

As operações de criptografia que estão habilitadas na chave externa associada à chave do KMS. Esse campo é exibido somente para chaves do KMS em um armazenamento de chaves externas.

Política de chave

Local: guia Key policy (Política de chaves)

Controla o acesso à chave do KMS juntamente com políticas do IAM e concessões. Cada chave do KMS tem uma política de chaves. Ela é o único elemento de autorização obrigatório. Para alterar a política de chaves de uma chave gerenciada pelo cliente, na guia Key policy (Política de chaves), selecione Edit (Editar). Para obter detalhes, consulte the section called “Políticas de chaves”.

Alternância de chaves

Local: Guia Key rotation (Alternância de chaves)

Habilita e desabilita a alternância automática do material da chave em uma chave do KMS gerenciada pelo cliente. Para alterar o status da alternância de chaves de uma chave gerenciada pelo cliente, use a caixa de seleção na guia Key rotation (Alternância de chaves).

Não é possível habilitar ou desabilitar a alternância do material da chave em uma Chave gerenciada pela AWS. As Chaves gerenciadas pela AWS são alternadas automaticamente a cada ano.

Especificação da chave

Local: guia Cryptographic configuration (Configuração criptográfica)

O tipo de material de chave na chave do KMS. O AWS KMS é compatível com chaves do KMS de criptografia simétrica (SYMMETRIC_DEFAULT), chaves do KMS de Hash-based message authentication code (HMAC – Código de autenticação de mensagem por hash) com diferentes tamanhos, chaves do KMS para chaves RSA com diferentes tamanhos e chaves de curva elíptica com diferentes curvas. Para obter detalhes, consulte Especificação da chave.

Tipo de chave

Local: guia Cryptographic configuration (Configuração criptográfica)

Indica se a chave do KMS é Simétrica ou Assimétrica.

Uso da chave

Local: guia Cryptographic configuration (Configuração criptográfica)

Indica se uma chave do KMS pode ser usada para criptografar e descriptografar, assinar e verificar ou gerar e verificar um MAC. Para obter detalhes, consulte Uso da chave.

Origem

Local: guia Cryptographic configuration (Configuração criptográfica)

A origem do material de chave da chave do KMS. Os valores válidos são:

- AWS KMS para material de chaves gerado pelo AWS KMS
- AWS CloudHSM para chaves do KMS no armazenamento de chaves do AWS CloudHSM
- Externa para material de chave importado (BYOK)
- Armazenamento de chaves externas para chaves do KMS em um armazenamento de chaves externas

Algoritmos de Message authentication code (MAC – Código de autenticação de mensagem)

Local: guia Cryptographic configuration (Configuração criptográfica)

Lista os algoritmos de Message authentication code (MAC – Código de autenticação de mensagem) que podem ser usados com uma chave do KMS de HMAC no AWS KMS. Esse campo só aparece quando a Key spec (Especificação da chave) é uma especificação de chave de HMAC (HMAC_*). Para obter informações sobre os algoritmos de MAC compatíveis com o AWS KMS, consulte Especificações de chave para chaves do KMS de HMAC.

Chave primária

Local: guia Regionality (Regionalidade)

Indica que essa chave do KMS é uma chave primária de várias regiões. Os usuários autorizados podem usar essa seção para transformar a chave primária em uma chave de várias Regiões relacionada diferente. Esse campo só aparece quando a chave do KMS é uma chave primária de várias regiões.

Chave pública

Local: guia Public key (Chave pública)

Exibe a chave pública de uma chave do KMS assimétrica. Os usuários autorizados podem usar essa guia para copiar e fazer download da chave pública.

Regionalidade

Local: seção General configuration (Configuração geral) e guias Regionality (Regionalidade)

Indica se uma chave do KMS é de região única, uma chave primária de várias regiões ou uma chave de réplica de várias regiões. Esse campo só aparece quando a chave do KMS é uma chave de várias regiões.

Chaves de várias regiões relacionadas

Local: guia Regionality (Regionalidade)

Exibe todas as chaves primárias e chaves de réplica de várias regiões relacionadas, exceto a chave do KMS atual. Esse campo só aparece quando a chave do KMS é uma chave de várias regiões.

Na seção Related multi-Region keys (Chaves de várias regiões relacionadas) de uma chave primária, os usuários autorizados podem criar novas chaves de réplica.

Chave de réplica

Local: guia Regionality (Regionalidade)

Indica que essa chave do KMS é uma chave de réplica de várias regiões. Esse campo só aparece quando a chave do KMS é uma chave de réplica de várias regiões.

Algoritmos de assinatura

Local: guia Cryptographic configuration (Configuração criptográfica)

Lista os algoritmos de assinatura que podem ser usados com a chave do KMS no AWS KMS. Esse campo é exibido somente quando o Key type (Tipo de chave) é Asymmetric (Assimétrico) e o Key usage (Uso da chave) é Sign and verify (Assinar e verificar). Para obter informações sobre os algoritmos de assinatura compatíveis com o AWS KMS, consulte Especificações de chave RSA para assinatura e verificação e Especificações da chave de curva elíptica.

Status

Local: seção General configuration (Configuração geral)

O estado da chave do KMS. É possível usar a chave do KMS em operações criptográficas somente quando o status é Enabled (Habilitado). Para obter uma descrição detalhada do status de cada chave do KMS e seu efeito nas operações que podem ser executadas na chave do KMS, consulte Principais estados das AWS KMS chaves.

Tags

Local: guia Tags (Etiquetas)

Pares de chave-valor opcionais que descrevem a chave do KMS. Para adicionar ou alterar as etiquetas de uma chave do KMS, na guia Tags (Etiquetas), selecione Edit (Editar).

Ao adicionar tags aos recursos da AWS, a AWS gera um relatório de alocação de custos com utilização e custos agrupados por tags. Etiquetas também podem ser utilizadas para controlar o acesso a uma chave do KMS. Para informações sobre marcação de chaves do KMS, consulte Marcar chaves com tags e ABAC para AWS KMS.

Personalizar suas tabelas de chaves do KMS

É possível personalizar as tabelas exibidas nas páginas de Chaves gerenciadas pela AWS e Chaves gerenciadas pelo cliente do AWS Management Console para atender às suas necessidades. Você pode escolher as colunas da tabela, o número de AWS KMS keys em cada página (Tamanho da página) e a quebra de texto. A configuração escolhida será salva quando você confirmá-la e será reaplicada sempre que você abrir as páginas.

Como personalizar suas tabelas de chaves do KMS

1. Na página de Chaves gerenciadas pela AWS ou de chaves gerenciadas pelo cliente, escolha o ícone de configurações

   ()

   no canto superior direito da página.
2. Na página Preferences (Preferências), escolha as configurações de preferência e selecione Confirm (Confirmar).

Considere o uso da configuração Page size (Tamanho da página) para aumentar o número de chaves do KMS exibidas em cada página, principalmente se você costuma usar um dispositivo que tem a rolagem fácil.

As colunas de dados exibidas podem variar dependendo da tabela, da função do trabalho e dos tipos de chaves do KMS na conta e na região. A tabela a seguir oferece algumas configurações sugeridas. Para obter descrições das colunas, consulte Exibir detalhes de chaves do KMS.

Configurações sugeridas para a tabela de chaves do KMS

Você pode personalizar as colunas que aparecem na tabela de chaves do KMS para exibir as informações necessárias sobre as suas chaves do KMS.

Chaves gerenciadas pela AWS

Por padrão, a tabela Chave gerenciada pela AWS exibe as colunas Aliases, Key ID (ID da chave) e Status. Essas colunas são ideais para a maioria dos casos de uso.

Chaves do KMS de criptografia simétrica

Se você usar apenas chaves do KMS de criptografia simétrica com o material de chave gerado pelo AWS KMS, provavelmente as colunas Aliases, Key ID (ID da chave), Status e Creation date (Data de criação) serão as mais úteis.

Chaves do KMS assimétricas

Se você usar chaves do KMS assimétricas, além das colunas Aliases, Key ID (ID da chave) e Status, considere adicionar as colunas Key type (Tipo de chave), Key spec (Especificação da chave) e Key usage (Uso da chave). Essas colunas mostrarão se uma chave do KMS é simétrica ou assimétrica, o tipo do material de chave e se a chave do KMS pode ser usada para criptografia ou para assinatura.

Chaves do KMS de HMAC

Se você usar chaves do KMS de HMAC, além das colunas Aliases, Key ID (ID da chave) e Status, avalie a possibilidade de adicionar as colunas Key spec (Especificação de chave) e Key usage (Uso da chave). Essas colunas mostrarão se uma chave do KMS é uma chave de HMAC. Como você não pode classificar chaves do KMS por especificação de chave ou uso de chaves, use aliases e etiquetas para identificar suas chaves de HMAC e, em seguida, use os recursos de filtro do console do AWS KMS para filtrar por aliases ou etiquetas.

Material de chave importado

Se você tiver chaves do KMS commaterial de chave importado, considere adicionar as colunas Origin (Origem) eExpiration date (Data de validade). Essas colunas mostrarão se o material de chave em uma chave do KMS é importado ou gerado pelo AWS KMS e quando o material de chave expira, se for o caso. O campo Creation date (Data de criação) exibe a data em que a

chave do KMS foi criada (sem o material de chave). Ele não reflete nenhuma característica do material de chave.

Chaves em armazenamentos de chaves personalizados

Se você tiver chaves do KMS em armazenamentos de chaves personalizados, considere adicionar as colunas Origin (Origem) e Custom key store ID (ID do armazenamento de chaves personalizado). Essas colunas informam se a chave do KMS está em um armazenamento de chaves personalizado, exibem o tipo do armazenamento de chaves personalizado e identificam o armazenamento de chaves personalizado.

Chaves de várias regiões

Se você tiver chaves de várias regiões, considere adicionar a coluna Regionality (Regionalidade). Ela mostra se uma chave do KMS é de região única, uma chave primária de várias regiões ou uma chave de réplica de várias regiões.

Visualizar chaves do KMS com a API

Você pode usar a API do AWS Key Management Service(AWS KMS) para ver suas chaves do KMS. Esta seção demonstra várias operações que retornam detalhes sobre as chaves do KMS existentes. Os exemplos usam a AWS Command Line Interface (AWS CLI), mas você pode usar qualquer linguagem de programação compatível.

Tópicos

- ListKeys: obtenha o ID e o ARN de todas as chaves KMS
- DescribeKey: Obtenha informações detalhadas sobre uma chave KMS
- GetKeyPolicy: Obtenha a política de chaves anexada a uma chave KMS
- ListAliases: Obtenha nomes de alias e ARNs para chaves KMS
- ListResourceTags: Obtenha as tags nas chaves KMS

ListKeys: obtenha o ID e o ARN de todas as chaves KMS

A ListKeysoperação retorna o ID e o Amazon Resource Name (ARN) de todas as chaves KMS na conta e na região.

Por exemplo, essa chamada para a operação `ListKeys` retorna o ID e o ARN de cada chave do KMS nessa conta fictícia. Para obter exemplos em várias linguagens de programação, consulte Obter IDs e ARNs de chaves do 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: Obtenha informações detalhadas sobre uma chave KMS

A DescribeKeyoperação retorna detalhes sobre a chave KMS especificada. Para identificar a chave do KMS, use seu ID de chave, ARN de chave, nome de alias ou ARN de alias.

Ao contrário da ListKeysoperação, que exibe somente as chaves KMS na conta e na região do chamador, os usuários autorizados podem usar a `DescribeKey` operação para obter detalhes sobre as chaves KMS em outras contas.

> **Note**
>
> A resposta de `DescribeKey` inclui os membros `KeySpec` e `CustomerMasterKeySpec` com os mesmos valores. O membro `CustomerMasterKeySpec` é defasado.

Por exemplo, essa chamada para `DescribeKey` retorna informações sobre uma chave do KMS de criptografia simétrica. Os campos na resposta variam de acordo com a especificação da AWS KMS key, o estado da chave e a origem do material de chave. Para obter exemplos em várias linguagens de programação, consulte Como visualizar um 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"
        ]
    }
}
```

Esse exemplo chama a operação `DescribeKey` em uma chave do KMS assimétrica usada para assinatura e verificação. A resposta inclui os algoritmos de assinatura compatíveis com o AWS KMS para essa chave do 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: Obtenha a política de chaves anexada a uma chave KMS

A GetKeyPolicyoperação obtém a política de chaves anexada à chave KMS. Para identificar a chave do KMS, use seu ID de chave ou ARN de chave. Você também deve especificar o nome da política, que é sempre `default`. (Se for difícil realizar a leitura de sua saída, adicione a opção `--output text` ao seu comando.) `GetKeyPolicy` só funciona em chaves do KMS na conta e na região do chamador.

Para obter exemplos em várias linguagens de programação, consulte Obter uma política de chaves.

```
$ 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: Obtenha nomes de alias e ARNs para chaves KMS

A ListAliasesoperação retorna aliases na conta e na região. O `TargetKeyId` na resposta exibe o ID de chave da chave do KMS ao qual o alias faz referência, caso exista.

Por padrão, o comando ListAliases gera todos os aliases na conta e na região. Isso inclui aliases que você criou e associou às suas chaves gerenciadas pelo cliente e aliases que a AWS criou e associou à Chave gerenciada pela AWS na sua conta. Você pode reconhecer aliases da AWS porque os nomes têm o formato `aws/<service-name>`, como `aws/dynamodb`.

A resposta também pode incluir aliases sem o campo `TargetKeyId`, como o alias `aws/redshift` neste exemplo. Estes são aliases predefinidos criados pela AWS, mas que ainda não estão associados a uma chave do KMS.

Para obter exemplos em várias linguagens de programação, consulte Listar aliases.

```
$ 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"
        },
    ]
}
```

Para obter os aliases que fazem referência a uma determinada chave do KMS, use o parâmetro `KeyId`. O valor do parâmetro pode ser o ID da chave ou o ARN da chave. Não é possível especificar um nome de alias ou um ARN de alias.

O comando no exemplo a seguir obtém os aliases que fazem referência a uma chave gerenciada pelo cliente. No entanto, também é possível usar um comando como esse para localizar os aliases que fazem referência a Chaves gerenciadas pela 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
        },
    ]
}
```

Para obter somente os aliases para Chaves gerenciadas pela AWS, use os recursos da sua linguagem de programação para filtrar a resposta.

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

ListResourceTags: Obtenha as tags nas chaves KMS

A ListResourceTagsoperação retorna as tags na chave KMS especificada. A API retorna etiquetas para uma chave do KMS, mas você pode executar o comando em um loop para obter etiquetas para todas as chaves do KMS na conta e região, ou para um conjunto de chaves do KMS selecionadas. Como essa API retorna uma página de cada vez, se você tiver várias etiquetas em várias chaves do KMS, talvez seja necessário usar o paginador na sua linguagem de programação para obter todas as etiquetas desejadas.

A operação `ListResourceTags` retorna tags para todas as chaves do KMS, mas Chave gerenciada pela AWS não são marcadas. Esse recurso só funciona em chaves do KMS na conta e na região do chamador.

Para localizar as etiquetas de uma chave do KMS, use a operação `ListResourceTags`. O parâmetro `KeyId` é obrigatório. Ela aceita um ID da chave ou um ARN de chave. Antes de executar este exemplo, substitua o ARN de chave de exemplo por um válido.

```
$  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
}
```

Talvez você queira usar a operação `ListResourceTags` para obter todas as chaves do KMS na conta e região com uma etiqueta, chave de etiqueta ou valor de etiqueta específico. Para fazer isso, use os recursos de filtragem da sua linguagem de programação.

Por exemplo, o script Bash a seguir usa as `ListResourceTags` operações ListKeyse para obter todas as chaves KMS na conta e na região com uma chave de `Project` tag. Ambas as operações obtêm apenas a primeira página de resultados. Se você tiver várias chaves do KMS ou várias etiquetas, use os recursos de paginação da sua linguagem para obter todo o resultado de cada operação. Antes de executar esse exemplo, substitua os IDs de chave de exemplo por IDs válidos.

```
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
```

A saída é formatada como a saída do exemplo a seguir.

```
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"
    }
]
```

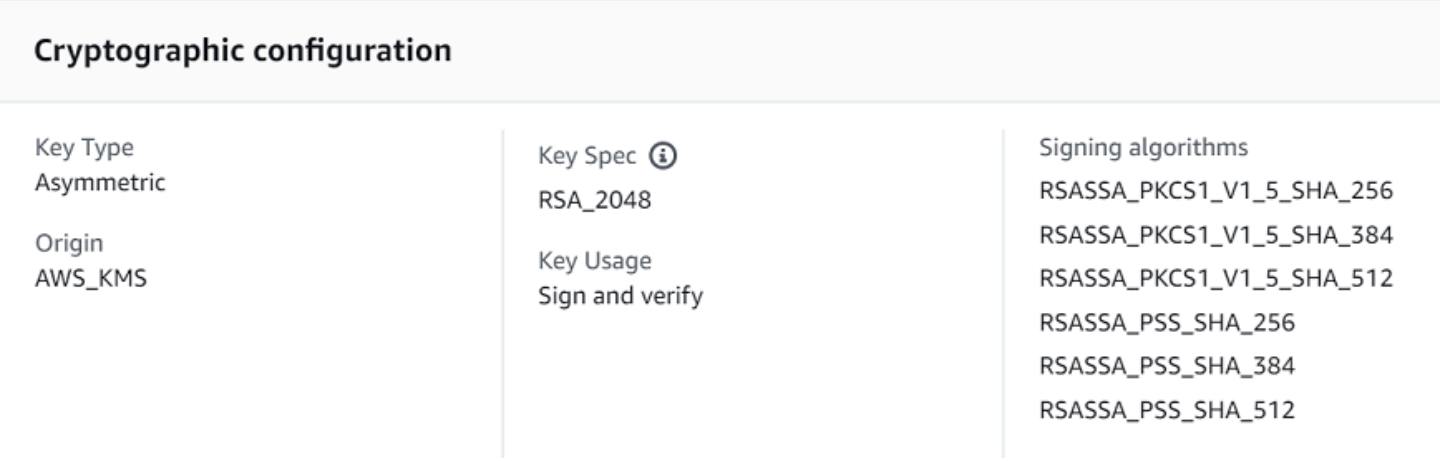
Exibir a configuração criptográfica de chaves do KMS

Após criar a chave do KMS, você pode visualizar suas configurações criptográficas. Não é possível alterar a configuração de uma chave do KMS depois que ela é criada. Se preferir uma configuração diferente, exclua a chave do KMS e crie-a novamente.

Você pode encontrar a configuração criptográfica das suas chaves do KMS, incluindo a especificação de chave, o uso de chave e os algoritmos de criptografia ou de assinatura compatíveis, no console do AWS KMS ou usando a API do AWS KMS. Para obter detalhes, consulte Identificar chaves do KMS assimétricas.

No console do AWS KMS, a página de detalhes de cada chave do KMS inclui uma guia Cryptographic configuration (Configuração criptográfica) que exibe os detalhes criptográficos sobre as suas chaves do KMS. Por exemplo, a imagem a seguir mostra a guia Cryptographic configuration (Configuração criptográfica) de uma chave do KMS RSA usada para assinatura e verificação.

A guia Cryptographic configuration (Configuração criptográfica) para algumas chaves do KMS de propósitos especiais tem outras seções especializadas. Por exemplo, a guia Cryptographic configuration (Configuração criptográfica) de uma chave do KMS em um armazenamento de chaves personalizado tem uma seção chamada Custom key stores (Armazenamentos de chaves personalizados). A guia Cryptographic configuration (Configuração criptográfica) de uma chave do KMS em um armazenamento de chaves externas tem uma seção chamada External key (Chave externa).



Na AWS KMS API, use a DescribeKeyoperação. A estrutura `KeyMetadata` na resposta inclui a configuração criptográfica da chave do KMS. Por exemplo, `DescribeKey` retorna a resposta a seguir para uma chave do KMS RSA usada para assinatura e verificação.

```
{
  "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"
    ]
  }
```

```
}
```

Como encontrar o ID e o ARN da chave

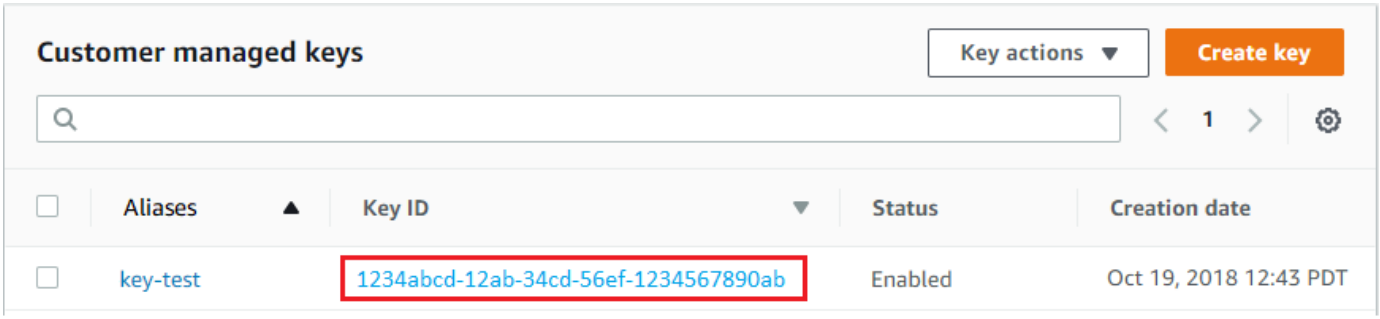
Para identificar uma AWS KMS key, é possível usar seu ID de chave ou seu nome de recurso da Amazon (ARN da chave). Em operações de criptografia, também é possível usar o nome do alias ou o ARN do alias.

Para obter informações detalhadas sobre os identificadores de chave do KMS com suporte pelo AWS KMS, consulte Identificadores-chave () KeyId. Para obter ajuda para encontrar um nome de alias e um ARN de alias, consulte Encontrar o nome e o ARN do alias.

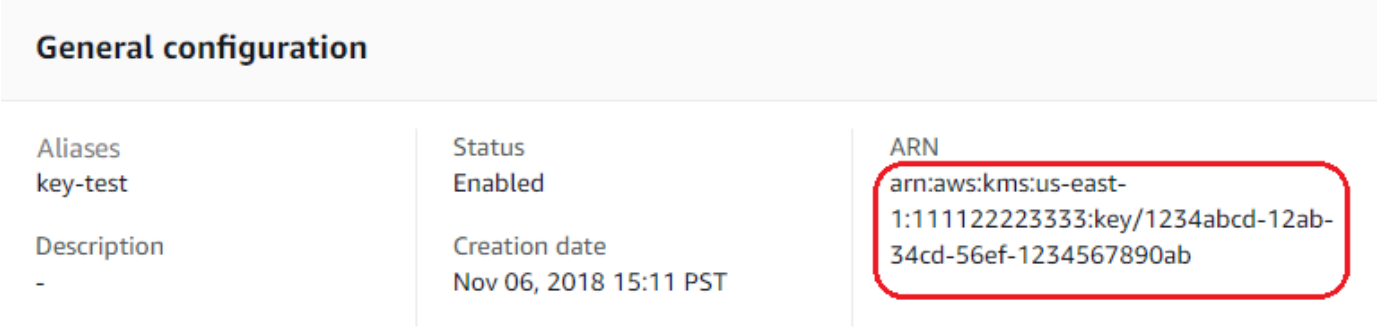
Para encontrar o ID e o ARN da chave (console)

1. Abra o console do AWS KMS em https://console.aws.amazon.com/kms.
2. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.
3. Para exibir as chaves em sua conta que você cria e gerencia, no painel de navegação, escolha Customer managed keys (Chaves gerenciadas de cliente). Para visualizar as chaves na sua conta que a AWS cria e gerencia para você, no painel de navegação, escolha AWS managed keys (Chaves gerenciadas pela AWS).
4. Para encontrar o ID de chave de uma chave do KMS, consulte a linha que começa com o alias da chave do KMS.

   A coluna Key ID (ID de chave) aparece na tabela por padrão. Se a coluna Key ID (ID de chave) não for exibida na tabela, use o procedimento descrito em the section called “Personalizar suas tabelas de chaves do KMS” para restaurá-la. Também é possível visualizar o ID de chave de uma chave do KMS em sua página de detalhes.



5. Para encontrar o Amazon Resource Name (ARN) da chave do KMS, escolha o alias ou o ID da chave. O ARN da chave é exibido na seção General Configuration (Configuração geral).



Como encontrar o ID e o ARN da chave (API do AWS KMS)

Para encontrar o ID da chave e o ARN da chave de umAWS KMS key, use a ListKeysoperação. Para obter exemplos em várias linguagens de programação, consulte Obter IDs e ARNs de chave e Obter IDs e ARNs de chave.

A resposta de `ListKeys` inclui o ID e o ARN da chave de cada chave do KMS na conta e região.

```
$ 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"
        }
    ]
}
```

Encontrar o nome e o ARN do alias

Um alias é um nome amigável para uma AWS KMS keys do AWS KMS (chave do KMS). Você pode encontrar o nome do alias e o ARN do alias no console do AWS KMS ou na API do AWS KMS.

Para obter informações detalhadas sobre os identificadores de chave do KMS com suporte pelo AWS KMS, consulte Identificadores-chave () KeyId. Para obter ajuda para encontrar o ID chave e o ARN da chave, consulte Como encontrar o ID e o ARN da chave.

Tópicos

- Para encontrar o nome de alias e o ARN do alias (console)
- Para encontrar o nome de alias e o ARN do alias (API do AWS KMS)

Para encontrar o nome de alias e o ARN do alias (console)

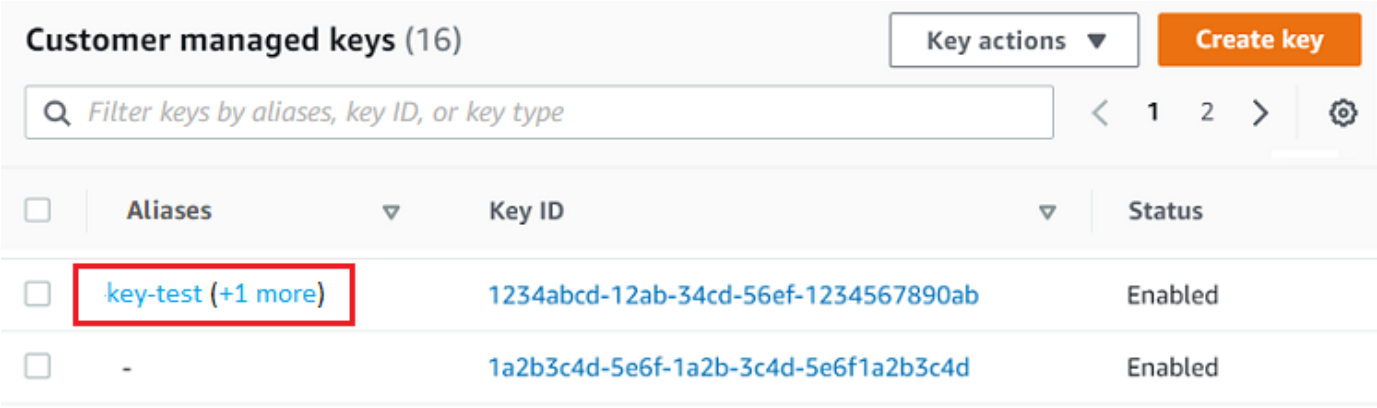
O console do AWS KMS exibe um nome de alias associado à chave do KMS.

1. Abra o console do AWS KMS em https://console.aws.amazon.com/kms.
2. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.
3. Para exibir as chaves em sua conta que você cria e gerencia, no painel de navegação, escolha Customer managed keys (Chaves gerenciadas de cliente). Para visualizar as chaves na sua conta que a AWS cria e gerencia para você, no painel de navegação, escolha AWS managed keys (Chaves gerenciadas pela AWS).
4. A coluna Aliases exibe o alias de cada chave do KMS. Se uma chave do KMS não tiver um alias, um traço (-) será exibido na coluna Aliases.

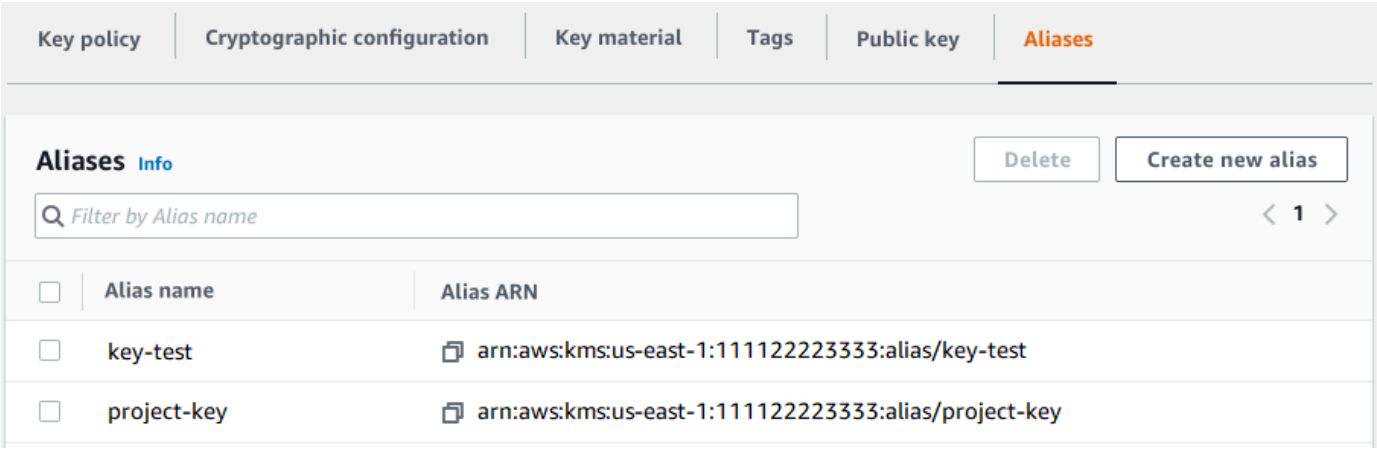
   Se uma chave do KMS tiver vários aliases, a coluna Aliases também terá um resumo dos aliases, como (mais n). Por exemplo, a seguinte chave do KMS tem dois aliases, um dos quais é `key-test`.

   Para encontrar o nome e o ARN de todos os aliases para a chave do KMS, use a guia Aliases.

   - Para acessar diretamente a guia Aliases, na coluna Aliases, escolha o resumo do alias (Mais n). Um resumo de aliases será exibido somente se a chave do KMS tiver mais de um alias.
   - Outra opção é escolher o alias ou o ID da chave do KMS (que abre a página de detalhes da chave do KMS) e escolher a guia Aliases. As guias estão na seção General configuration (Configuração geral).



5. A guia Aliases exibe o nome do alias e o ARN do alias de todos os aliases de uma chave do KMS. Também é possível criar e excluir aliases para a chave do KMS nessa guia.



Para encontrar o nome de alias e o ARN do alias (API do AWS KMS)

Para encontrar o nome do alias e o ARN do alias de umAWS KMS key, use a operação. ListAliases Para obter exemplos em várias linguagens de programação, consulte Listar aliases e Obter nomes de alias e ARNs.

Por padrão, a resposta inclui o nome e o ARN do alias para cada alias na conta e na região. Para obter somente os aliases de uma chave do KMS específica, use o parâmetro `KeyId`.

Por exemplo, o comando a seguir obtém apenas os aliases de uma chave do KMS de exemplo com o ID de chave `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
        }
    ]
}
```

Editar chaves

É possível alterar as seguintes propriedades de chaves gerenciadas pelo cliente no console do AWS KMS e usando a API do AWS KMS.

Não é possível editar as propriedade de Chaves gerenciadas pela AWS ou de Chaves pertencentes à AWS. Essas chaves são gerenciadas pelos serviços da AWS que as criaram.

Descrição

Você pode alterar a descrição da chave gerenciada pelo cliente na página de detalhes da chave KMS ou usando a UpdateKeyDescriptionoperação.

Para editar a descrição da chave no console, no canto superior direito da página de detalhes da chave do KMS, escolha Edit. (Editar)

Política de chave

Você pode alterar a política de chaves na guia Política de chaves da página de detalhes da chave gerenciada pelo cliente ou usando a PutKeyPolicyoperação.

Para obter detalhes, consulte Alterar uma política de chaves.

Tags

É possível criar e excluir etiquetas na página Customer managed keys (Chaves gerenciadas pelo cliente) do console do AWS KMS ou na guia Tags (Etiquetas) da página de detalhes da chave gerenciada pelo cliente. Ou você pode usar TagResourceas UntagResourceoperações e.

Para obter detalhes, consulte Marcar chaves com tags.

Habilitar e desabilitar

É possível habilitar e desabilitar chaves do KMS na página Customer managed keys (Chaves gerenciadas pelo cliente) do console do AWS KMS ou na página de detalhes da chave gerenciada pelo cliente. Ou você pode usar EnableKeyas DisableKeyoperações e.

Para obter detalhes, consulte Habilitar e desabilitar chaves.

Alternância automática de chaves

Você pode ativar e desativar a rotação automática de chaves na guia Rotação de chaves da página de detalhes da chave gerenciada pelo cliente ou usando as DisableKeyRotationoperações EnableKeyRotatione.

Para obter detalhes, consulte Girando AWS KMS keys.

Consulte também

Atualizar aliases

Marcar chaves com tags

No AWS KMS, é possível adicionar etiquetas a uma chaves gerenciada pelo cliente ao criar a chaves do KMS e adicionar ou remover etiquetas de chaves do KMS existentes, a menos que essas chaves estejam com exclusão pendente. Não é possível marcar aliases, armazenamentos de chaves personalizados, Chaves gerenciadas pela AWS, Chaves pertencentes à AWS ou chaves do KMS em outras Contas da AWS. Etiquetas são opcionais, mas podem ser bastante úteis.

Para obter mais informações, consulte Editar chaves e Criar chaves. Para obter informações gerais sobre etiquetas, incluindo práticas recomendadas, estratégias de marcação e o formato e a sintaxe de etiquetas, consulte Marcar recursos da AWS na Referência geral da Amazon Web Services.

Tópicos

- Sobre etiquetas no AWS KMS
- Gerenciar etiqueta de chaves no console
- Gerenciar etiquetas de chaves do KMS com operações de API
- Controlar o acesso a etiquetas
- Usar etiquetas para controlar o acesso a chaves do KMS

Sobre etiquetas no AWS KMS

Uma etiqueta é um rótulo de metadados que você (ou a AWS) pode atribuir a um recurso da AWS. Cada tag consiste em uma chave de tag e um valor de tag, sendo ambos strings que diferenciam maiúsculas de minúsculas. O valor da tag pode ser uma string vazia (nula). Cada tag em um recurso deve ter uma chave de tag diferente, mas você pode adicionar a mesma tag a vários recursos da AWS. Cada recurso pode ter até 50 tags criadas pelo usuário.

Não inclua informações confidenciais ou sigilosas na chave ou no valor da tag. As tags são acessíveis a muitos Serviços da AWS, incluindo faturamento.

No AWS KMS, é possível adicionar etiquetas a uma chaves gerenciada pelo cliente ao criar a chaves do KMS e adicionar ou remover etiquetas de chaves do KMS existentes, a menos que essas chaves estejam com exclusão pendente. Não é possível marcar aliases, armazenamentos de chaves personalizados, Chaves gerenciadas pela AWS, Chaves pertencentes à AWS ou chaves do KMS em outras Contas da AWS. Etiquetas são opcionais, mas podem ser bastante úteis.

Por exemplo, você pode adicionar uma etiqueta `"Project"="Alpha"` a todas as chaves do KMS e buckets do Amazon S3 usados para o projeto Alpha.

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

Para obter informações gerais sobre tags, incluindo o formato e a sintaxe, consulte Marcar recursos da AWS na Referência geral da Amazon Web Services.

As tags ajudam você a fazer o seguinte:

- Identificar e organizar seus recursos da AWS. Muitos serviços da AWS oferecem suporte à marcação para que você possa atribuir a mesma tag a recursos de diferentes serviços para indicar que os recursos estão relacionados. Por exemplo, é possível atribuir a mesma etiqueta a uma

chave do KMS e a um volume do Amazon Elastic Block Store (Amazon EBS) ou a um segredo do AWS Secrets Manager. Você também pode usar etiquetas para identificar as chaves do KMS para automação.

- Monitorar seus custos AWS. Ao adicionar tags aos recursos da AWS, a AWS gera um relatório de alocação de custos com utilização e custos agrupados por tags. Você pode usar esse recurso para monitorar os custos do AWS KMS para um projeto, aplicação ou centro de custo.

  Para obter mais informações sobre como usar etiquetas para alocação de custos, consulte Usar etiquetas de alocação de custos no Manual do usuário do AWS Billing. Para obter informações sobre as regras para chaves e valores de etiquetas, consulte Restrições de etiquetas definidas pelo usuário, no Manual do usuário do AWS Billing.
- Controle o acesso aos recursos da AWS. Permitir e negar acesso às chaves do KMS com base em suas etiquetas faz parte do suporte do AWS KMS para controle de acesso baseado em atributos (ABAC). Para obter mais informações sobre como controlar o acesso a AWS KMS keys com base em etiquetas, consulte Usar etiquetas para controlar o acesso a chaves do KMS. Para obter mais informações sobre como usar etiquetas para controlar o acesso a recursos da AWS, consulte Controlar o acesso aos recursos da AWS, no Manual do usuário do IAM.

AWS KMSgrava uma entrada no seu AWS CloudTrail registro quando você usa as ListResourceTagsoperações TagResourceUntagResource, ou.

Gerenciar etiqueta de chaves no console

É possível adicionar etiquetas a uma chave do KMS ao criar a chave do KMS no console do AWS KMS. Você também pode usar a guia Tags (Etiquetas) no console para adicionar, editar e excluir etiquetas em chaves gerenciadas pelo cliente. Para adicionar, editar, exibir e excluir etiquetas de uma chave do KMS, é necessário ter as devidas permissões. Para obter detalhes, consulte Controlar o acesso a etiquetas.

Adicionar etiquetas ao criar uma chave do KMS

Para adicionar etiquetas ao criar uma chave do KMS no console, é necessário ter uma permissão `kms:TagResource` em uma política do IAM, além das permissões necessárias para criar chaves do KMS e exibir essas chaves no console. Essa permissão deve abranger pelo menos todas as chaves do KMS na conta e na região.

1. Faça login no AWS Management Console e abra o console do AWS Key Management Service (AWS KMS) em https://console.aws.amazon.com/kms.

2. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.
3. No painel de navegação, escolha Customer managed keys (Chaves gerenciadas pelo cliente). (Você não pode gerenciar as etiquetas de uma Chave gerenciada pela AWS)
4. Escolha o tipo de chave e selecione Next (Avançar).
5. Insira um alias e uma descrição opcional.
6. Insira uma chave de etiqueta e, opcionalmente, um valor de etiqueta. Para adicionar mais etiquetas, selecione Add new tag (Adicionar nova etiqueta). Para remover uma etiqueta, escolha Remove tag (Remover etiqueta). Quando terminar de marcar sua nova chave do KMS, selecione Next (Avançar).
7. Finalize a criação da sua chave do KMS.

Visualizar e gerenciar etiquetas em chaves do KMS existentes

Para adicionar, visualizar, editar e excluir etiquetas no console, é necessário ter permissão para marcação na chave do KMS. É possível obter essa permissão da política de chaves da chave do KMS ou, se a política de chaves permitir, de uma política do IAM que inclua essa chave do KMS. Essas permissões são necessárias além das permissões para visualizar chaves do KMS no console.

1. Faça login no AWS Management Console e abra o console do AWS Key Management Service (AWS KMS) em https://console.aws.amazon.com/kms.
2. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.
3. No painel de navegação, escolha Customer managed keys (Chaves gerenciadas pelo cliente). (Você não pode gerenciar as etiquetas de uma Chave gerenciada pela AWS)
4. É possível usar o filtro de tabela para exibir somente chaves do KMS com etiquetas específicas. Para obter detalhes, consulte Classificar e filtrar as chaves do KMS .
5. Marque a caixa de seleção ao lado do alias de uma chave do KMS.
6. Selecione Key actions (Ações de chave), Add or edit tags (Adicionar ou editar tags).
7. Na página de detalhes da chave do KMS, selecione a guia Tags (Etiquetas).

   - Para criar sua primeira etiqueta, selecione Create tag (Criar etiqueta), digite um nome e um valor de etiqueta e selecione Save (Salvar).

     Se você deixar o valor da tag em branco, o valor da tag real será uma string nula ou vazia.
   - Para adicionar uma etiqueta, selecione Edit (Editar), Add tag (Adicionar etiqueta), digite um nome de etiqueta e um valor de etiqueta e selecione Save (Salvar).

- Para alterar o nome ou o valor de uma tag, selecione Edit (Editar), faça as alterações e selecione Save (Salvar).
- Para excluir uma tag, selecione Edit (Editar). Na linha da tag, selecione Remove (Remover) e Save (Salvar).

8. Para salvar suas alterações, escolha Salvar alterações.

Gerenciar etiquetas de chaves do KMS com operações de API

É possível usar a API do AWS Key Management Service (AWS KMS) para adicionar, excluir e listar etiquetas das chaves do KMS gerenciadas. Estes exemplos usam a AWS Command Line Interface (AWS CLI), mas você pode usar qualquer linguagem de programação compatível. Você não pode marcar Chaves gerenciadas pela AWS.

Para adicionar, editar, visualizar e excluir etiquetas de uma chave do KMS, é necessário ter as permissões apropriadas. Para obter detalhes, consulte Controlar o acesso a etiquetas.

Tópicos

- CreateKey: Adicionar tags a uma nova chave KMS
- TagResource: Adicionar ou alterar tags para uma chave KMS
- ListResourceTags: Obtenha as tags para uma chave KMS
- UntagResource: Excluir tags de uma chave KMS

CreateKey: Adicionar tags a uma nova chave KMS

Você pode adicionar tags ao criar uma chave gerenciada pelo cliente. Para especificar as tags, use o `Tags` parâmetro da CreateKeyoperação.

Para adicionar etiquetas ao criar uma chave do KMS, o chamador deve ter a permissão `kms:TagResource` em uma política do IAM. Essa permissão deve abranger pelo menos todas as chaves do KMS na conta e na região. Para obter detalhes, consulte Controlar o acesso a etiquetas.

O valor do parâmetro `Tags` de `CreateKey` é uma coleção de pares de chave de etiqueta e valor de etiqueta que faz distinção entre maiúsculas e minúsculas. Cada etiqueta em uma chave do KMS deve ter um nome de etiqueta diferente. O valor da tag pode ser uma string nula ou vazia.

Por exemplo, o seguinte comando da AWS CLI cria uma chave do KMS de criptografia simétrica com uma etiqueta `Project:Alpha`. Ao especificar mais de um par de chave-valor, use um espaço para separar cada par.

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

Quando esse comando é bem-sucedido, ele retorna um objeto `KeyMetadata` com informações sobre a nova chave do KMS. No entanto, o `KeyMetadata` não inclui tags. Para obter as tags, use a ListResourceTagsoperação.

TagResource: Adicionar ou alterar tags para uma chave KMS

A TagResourceoperação adiciona uma ou mais tags a uma chave KMS. Não é possível usar essa operação para adicionar ou editar etiquetas em uma Conta da AWS diferente.

Para adicionar uma tag, especifique uma nova chave e um valor de tag. Para editar uma tag, especifique uma chave de tag existente e um novo valor de tag. Cada etiqueta em uma chave do KMS deve ter um nome de etiqueta diferente. O valor da tag pode ser uma string nula ou vazia.

Por exemplo, o comando a seguir adiciona as etiquetas **`Purpose`** e **`Department`** a uma chave do KMS demonstrativa.

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

Quando esse comando for executado com êxito, ele não retornará nenhuma saída. Para visualizar as tags em uma chave KMS, use a ListResourceTagsoperação.

Você também pode usar TagResource para alterar o valor de uma tag existente. Para substituir um valor de tag, especifique a mesma chave de tag com um valor diferente.

Por exemplo, esse comando altera o valor da tag `Purpose` de `Pretest` para `Test`.

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

ListResourceTags: Obtenha as tags para uma chave KMS

A ListResourceTagsoperação obtém as tags de uma chave KMS. O parâmetro `KeyId` é obrigatório. Essa operação não pode ser usada para visualizar as etiquetas nas chaves do KMS em uma Conta da AWS diferente.

Por exemplo, o comando a seguir obtém as etiquetas para uma chave do KMS demonstrativa.

```
$ 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: Excluir tags de uma chave KMS

A UntagResourceoperação exclui as tags de uma chave KMS. Para identificar as etiquetas a serem excluídas, especifique as chaves de etiqueta. Essa operação não pode ser usada para excluir etiquetas de chaves do KMS em uma Conta da AWS diferente.

Quando é bem-sucedida, a operação `UntagResource` não retorna nenhuma saída. Além disso, se a chave de etiqueta especificada não for encontrada na chave do KMS, ela não lançará uma exceção nem retornará uma resposta. Para confirmar se a operação funcionou, use a ListResourceTagsoperação.

Por exemplo, esse comando exclui a etiqueta **`Purpose`** e seu valor da chave do KMS especificada.

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

Controlar o acesso a etiquetas

Para adicionar, visualizar e excluir etiquetas, seja no console do AWS KMS do usando a API, as entidades principais precisam de permissões de marcação. Você pode fornecer essas permissões em políticas de chaves. Também é possível fornecê-las em políticas do IAM (incluindo políticas de endpoint da VPC), mas somente se permitido pela política de chaves. A política AWSKeyManagementServicePowerUsergerenciada permite que os diretores marquem, desmarquem e listem as tags em todas as chaves KMS que a conta pode acessar.

Também é possível pode limitar essas permissões usando chaves de condição globais da AWS para etiquetas. EmAWS KMS, essas condições podem controlar o acesso às operações de marcação, como TagResourcee. UntagResource

> **Note**
>
> Tenha cuidado ao conceder permissão a entidades principais para gerenciar etiquetas e aliases. Alterar uma etiqueta ou um alias pode conceder ou negar uma permissão à chave gerenciada pelo cliente. Para obter mais detalhes, consulte ABAC para AWS KMS e Usar etiquetas para controlar o acesso a chaves do KMS.

Para mais informações e exemplos de políticas, consulte Controlar o acesso baseado em chaves de etiqueta, no Guia do Usuário do IAM.

As permissões para criar e gerenciar aliases funcionam como a seguir.

kms: TagResource

Permite que as entidades principais adicionem ou editem etiquetas. Para adicionar etiquetas ao criar uma chave do KMS, a entidade principal deve ter permissão em uma política do IAM que não esteja restrita a chaves do KMS específicas.

kms: ListResourceTags

Permite que as entidades principais visualizem etiquetas em chaves do KMS.

kms: UntagResource

Permite que as entidades principais excluam etiquetas de chaves do KMS.

Permissões de etiquetas em políticas

Você pode fornecer permissões de marcação em uma política de chaves ou política do IAM. O seguinte exemplo de política de chaves concede permissão de marcação a usuários selecionados na chave do KMS. Ele concede a todos os usuários que podem assumir os exemplos de funções Administrador ou Desenvolvedor permissão para visualizar etiquetas.

```
{
  "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": "*"
    }
  ]
```

```
}
```

Para conceder permissão de marcação de entidades principais em várias chaves do KMS, é possível usar uma política do IAM. Para que essa política seja eficiente, a política de chaves de cada chave do KMS deve permitir que a conta utilize políticas do IAM para controlar o acesso à chave do KMS.

Por exemplo, a seguinte política do IAM permite que as entidades principais criem chaves do KMS. Ela também permite que eles criem e gerenciem etiquetas em todas as chaves do KMS na conta especificada. Essa combinação permite que os diretores usem o parâmetro Tags da CreateKeyoperação para adicionar tags a uma chave KMS enquanto a criam.

```
{
  "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/*"
    }
  ]
}
```

Limitar permissões de etiquetas

É possível limitar permissões de marcação usando condições de política. As seguintes condições de política podem ser aplicadas às permissões `kms:TagResource` e `kms:UntagResource`. Por exemplo, você pode usar a condição `aws:RequestTag/`*`tag-key`* para permitir que uma entidade principal adicione apenas etiquetas específicas, ou pode impedir que uma entidade principal adicione etiquetas com chaves de etiqueta específicas. Você também pode usar a condição `kms:KeyOrigin`

para impedir que as entidades principais marquem ou desmarcem chaves do KMS com material de chave importado.

- leis: RequestTag
- aws:ResourceTag/tag-key (somente políticas do IAM)
- leis: TagKeys
- kms: CallerAccount
- kms: KeySpec
- kms: KeyUsage
- kms: KeyOrigin
- kms: ViaService

Como prática recomendada ao usar etiquetas para controlar o acesso a chaves do KMS, use a chave de condição `aws:RequestTag/`*`tag-key`* ou `aws:TagKeys` para determinar quais etiquetas (ou chaves de etiqueta) são permitidas.

Por exemplo, a política do IAM a seguir é semelhante à anterior. No entanto, essa política permite que as entidades principais criem etiquetas (`TagResource`) e excluam etiquetas `UntagResource` somente para etiquetas com um chave de etiqueta `Project`.

Como `TagResource` as `UntagResource` solicitações podem incluir várias tags, você deve especificar um operador `ForAllValues` ou `ForAnyValue` definir com a TagKeys condição aws:. O operador `ForAnyValue` exige que pelo menos uma das chaves de etiqueta na solicitação corresponda a uma das chaves de etiqueta na política. O operador `ForAllValues` requer que todas as chaves de etiqueta na solicitação correspondam a uma das chaves de etiqueta na política. O `ForAllValues` operador também retorna `true` se não houver tags na solicitação, mas TagResource UntagResource falhará quando nenhuma tag for especificada. Para detalhes sobre os operadores de conjunto, consulteUsar várias chaves e valores, no Manual do usuário do 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"}
      }
    }
  ]
}
```

Usar etiquetas para controlar o acesso a chaves do KMS

É possível controlar o acesso aoAWS KMS keyscom base nas etiquetas na chave do KMS. Por exemplo, você pode escrever uma política do IAM que permite que as entidades principais habilitem e desabilitem somente as chaves do KMS que possuem uma etiqueta específica. Ou você pode usar uma política do IAM para impedir que as entidades principais usem chaves do KMS em operações de criptografia, a menos que a chave do KMS tenha uma etiqueta específica.

Esse recurso faz parte do suporte do AWS KMS para controle de acesso baseado em atributos(ABAC). Para informações sobre como usar etiquetas para controlar o acesso a recursos da AWS, consulte O que é o ABAC para a AWS? eControlar o acesso a recursos do AWS usando etiquetas de recursos, no Manual do usuário do IAM. Para obter ajuda para resolver problemas de acesso relacionados ao ABAC, consulte Solução de problemas com o ABAC para o AWS KMS.

> **Note**
>
> Pode levar até cinco minutos para que alterações de etiqueta e alias afetem a autorização de chaves do KMS. Alterações recentes podem estar visíveis em operações de API antes de afetarem a autorização.

AWS KMSsuporta a chave de contexto de condição global aws:ResourceTag/tag-key, que permite controlar o acesso às chaves KMS com base nas tags da chave KMS. Como várias chaves do KMS podem ter a mesma etiqueta, esse recurso permite que você aplique a permissão a um conjunto selecionado de chaves do KMS. Também é possível alterar facilmente as chaves do KMS no conjunto alterando suas etiquetas.

No AWS KMS, a chave de condição `aws:ResourceTag/`*`tag-key`* tem suporte apenas em políticas do IAM. Ela não é suportada em políticas de chaves, que se aplicam somente a uma chave KMS, ou em operações que não usam uma chave KMS específica, como as operações ListKeysou ListAliases.

Controlar o acesso com etiquetas é uma maneira simples, escalável e flexível de gerenciar permissões. No entanto, se isso não for projetado e gerenciado corretamente, poderá permitir ou negar acesso às chaves do KMS inadvertidamente. Se estiver usando etiquetas para controlar o acesso, considere as seguintes práticas.

- Use tags para reforçar a prática recomendada do acesso acesso com privilégio mínimo. Conceda às entidades principais do IAM somente as permissões de que eles precisam nas chaves do KMS que elas devem usar ou gerenciar. Por exemplo, use etiquetas para rotular as chaves do KMS usadas para um projeto. Em seguida, dê permissão à equipe do projeto para usar somente chaves do KMS com a etiqueta do projeto.
- Tenha cuidado ao conceder às entidades principais as permissões `kms:TagResource` e `kms:UntagResource`, com as quais elas podem adicionar, editar e excluir etiquetas. Quando você usa etiquetas para controlar o acesso a chaves do KMS, a alteração de uma etiqueta pode dar permissão às entidades principais para usar chaves do KMS que, de outra forma, elas não teriam permissão de usar. Ele também pode negar acesso a chaves do KMS que outras entidades principais exigem para realizar seus trabalhos. Os administradores de chaves que não tiverem permissão para alterar políticas de chaves ou criar concessões poderão controlar o acesso às chaves do KMS se tiverem permissão para gerenciar etiquetas.

  Sempre que possível, use uma condição de política, como `aws:RequestTag/`*`tag-key`* ou `aws:TagKeys`, paralimitar as permissões de marcação de uma entidade principal para etiquetas ou padrões de etiquetas específicos em chaves do KMS específicas.
- Revise as entidades principais na sua Conta da AWS que atualmente têm permissões de marcação e desmarcação e ajuste-as, se necessário. Por exemplo, a política de chaves padrão para administradores de chaves do console inclui as permissões `kms:TagResource` e `kms:UntagResource` nessa chave do KMS. As políticas do IAM podem conceder permissões de marcação ou desmarcação em todas as chaves do KMS. Por exemplo, a

política AWSKeyManagementServicePowerUsergerenciada permite que os diretores marquem, desmarquem e listem as tags em todas as chaves do KMS.

- Antes de definir uma política que dependa de uma etiqueta, revise as etiquetas nas chaves do KMS da sua Conta da AWS. Certifique-se de que sua política se aplica somente às etiquetas que você pretende incluir. Use CloudTrail registros e CloudWatch alarmes para alertá-lo sobre alterações nas tags que possam afetar o acesso às suas chaves KMS.
- As condições de políticas baseadas em etiquetas usam correspondência de padrões. Elas não estão vinculadas a uma instância específica de uma etiqueta. Uma política que usa chaves de condição baseadas em etiquetas afeta todas as etiquetas novas e existentes que correspondem ao padrão. Se você excluir e recriar uma etiqueta que corresponde a uma condição de política, a condição se aplicará à nova etiqueta, assim como à antiga.

Por exemplo, considere a seguinte política do IAM. Ele permite que os diretores liguem para as operações GenerateDataKeyWithoutPlaintexte descriptografem somente em chaves KMS em sua conta que estejam na região Ásia-Pacífico (Cingapura) e tenham uma tag. `"Project"="Alpha"` Você pode anexar essa política a funções no exemplo do projeto Alpha.

```
{
  "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"
        }
      }
    }
  ]
}
```

O exemplo de política do IAM a seguir permite que as entidades principais usem qualquer chave dp KMS na conta para determinadas operações de criptografia. Porém, ela proíbe as

entidades principais de usar estas operações criptográficas em chaves do KMS com uma tag `"Type"="Reserved"` ou sem etiqueta `"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"
        }
      }
    }
  ]
}
```

Habilitar e desabilitar chaves

É possível desabilitar e reabilitar chaves gerenciadas pelo cliente. Ao criar uma chave do KMS, ela é habilitada por padrão. Se você desabilitar uma chave do KMS, ela não poderá ser usada em nenhuma operação criptográfica até que seja reabilitada.

Por ser temporário e facilmente desfeito, desabilitar uma chave do KMS é uma alternativa segura a excluir uma chave do KMS, que é uma ação destrutiva e irreversível. Se você estiver pensando em excluir uma chave KMS, desative-a primeiro e defina um CloudWatch alarme ou mecanismo semelhante para garantir que você nunca precise usar a chave para descriptografar dados criptografados.

Quando você desabilita uma chave do KMS, ela se torna inutilizável imediatamente (sujeita a consistência posterior). Porém, os recursos criptografados com chaves de dados protegidas pela chave do KMS não são afetados até que a chave do KMS seja usada novamente, por exemplo, para descriptografar a chave de dados. Esse problema afeta os Serviços da AWS, pois muitos deles usam chaves de dados para proteger recursos. Para obter detalhes, consulte Como as chaves do KMS inutilizáveis afetam as chaves de dados.

Não é possível habilitar ou desabilitar Chaves gerenciadas pela AWS ou Chaves pertencentes à AWS. Chaves gerenciadas pela AWS são permanentemente habilitadas para uso pelos serviços que usam o AWS KMS. Chaves pertencentes à AWS são gerenciadas unicamente pelo serviço que as possui.

> **Note**
>
> O AWS KMS não alterna o material de chave das chaves gerenciadas pelo cliente enquanto elas estão desabilitadas. Para ter mais informações, consulte Como funciona a rotação de chaves.

Tópicos

- Habilitar e desabilitar chaves do KMS (console)
- Habilitar e desabilitar chaves do KMS (API do AWS KMS)

Habilitar e desabilitar chaves do KMS (console)

É possível usar o console do AWS KMS para habilitar e desabilitar chaves gerenciadas pelo cliente.

1. Faça login no AWS Management Console e abra o console do AWS Key Management Service (AWS KMS) em https://console.aws.amazon.com/kms.
2. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.
3. No painel de navegação, escolha Customer managed keys (Chaves gerenciadas pelo cliente).
4. Marque a caixa de seleção das chaves do KMS que deseja habilitar ou desabilitar.
5. Para habilitar uma chave do KMS, selecione Key actions (Ações de chaves), Enable (Habilitar). Para desativar chave do KMS, escolha Key actions (Ações de chaves), Disable (Desabilitar).

Habilitar e desabilitar chaves do KMS (API do AWS KMS)

A EnableKeyoperação ativa um desativadoAWS KMS key. Estes exemplos usam a AWS Command Line Interface (AWS CLI), mas você pode usar qualquer linguagem de programação compatível. O parâmetro `key-id` é obrigatório.

Esta operação não apresenta nenhuma saída. Para ver o status da chave, use a DescribeKeyoperação.

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

A DisableKeyoperação desativa uma chave KMS ativada. O parâmetro `key-id` é obrigatório.

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

Esta operação não apresenta nenhuma saída. Para ver o status da chave, use a DescribeKeyoperação e veja o `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"
        ]
    }
}
```

Girando AWS KMS keys

Para criar um novo material criptográfico para suas chaves gerenciadas pelo cliente, você pode criar novas chaves do KMS e, em seguida, alterar suas aplicações ou seus aliases para usar essas novas chaves do KMS. Ou você pode girar o material da chave associado a uma chave KMS existente ativando a rotação automática da chave ou executando a rotação sob demanda.

Por padrão, quando você ativa a rotação automática de chaves para uma chave KMS, AWS KMS gera novo material criptográfico para a chave KMS todos os anos. Você também pode especificar um personalizado rotation-period para definir o número de dias após ativar a rotação automática de chaves que AWS KMS girará o material da chave e o número de dias entre cada rotação automática a partir de então. Se precisar iniciar imediatamente a rotação de material-chave, você pode realizar a rotação sob demanda, independentemente de a rotação automática de chaves estar ativada ou não. As rotações sob demanda não alteram os cronogramas de rotação automática existentes.

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. Você pode acompanhar a rotação do material de chaves para suas chaves KMS na Amazon CloudWatch e no AWS Key Management Service console. AWS CloudTrail Você também pode usar a

GetKeyRotationStatusoperação para verificar se a rotação automática está habilitada para uma chave KMS e identificar quaisquer rotações sob demanda em andamento. Você pode usar a ListKeyRotationsoperação para visualizar os detalhes das rotações concluídas.

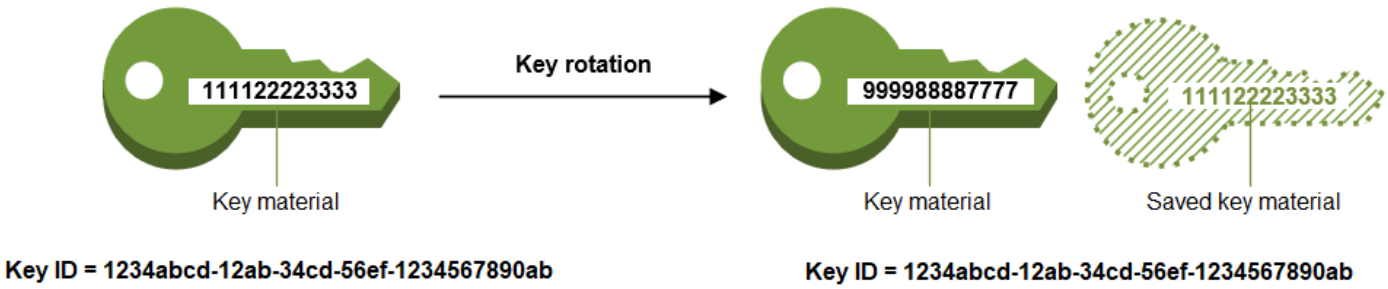
Quando você usa uma chave KMS rotacionada para criptografar dados, AWS KMS usa o material de chave atual. Quando você usa a chave KMS rotacionada para descriptografar texto cifrado, AWS KMS usa a versão do material da chave que foi usada para criptografá-la. Você não pode selecionar uma versão específica do material chave para operações de descriptografia, escolhe AWS KMS automaticamente a versão correta. Como a decodificação é AWS KMS transparente com o material de chave apropriado, você pode usar com segurança uma chave KMS girada em aplicativos e sem alterações no código. Serviços da AWS

No entanto, a alternância automática de chaves não afeta os dados protegidos pela chave do KMS. Ela não alterna as chaves de dados geradas pela chave do KMS, não criptografa novamente quaisquer dados protegidos pela chave do KMS e não reduzirá o impacto de uma chave de dados comprometida.

AWS KMS suporta rotação de chaves automática e sob demanda somente para chaves KMS de criptografia simétrica com material de chave criado por ele. AWS KMS A alternância automática é opcional para chaves do KMS gerenciadas pelo cliente. O AWS KMS sempre alterna o material de chave para chaves do KMS gerenciadas pela AWS a cada ano. A rotação das chaves KMS AWS próprias é gerenciada pelo AWS serviço que possui a chave.

> **Note**
>
> O período de rotação para Chaves gerenciadas pela AWS mudou em maio de 2022. Para obter detalhes, consulte Chaves gerenciadas pela AWS.

A alternância de chaves altera apenas o material de chave, que é o segredo criptográfico usado em operações de criptografia. A chave do KMS é o mesmo recurso lógico, independentemente da ocorrência de alterações ou do número de vezes que estas tenham sido feitas no material de chave. As propriedades da chave do KMS não são alteradas, conforme mostrado na imagem a seguir.



Você pode optar por criar uma nova chave do KMS e usá-la em vez da chave do KMS original. Isso tem o mesmo efeito que alternar o material da chave em uma chave do KMS existente e, portanto, normalmente é considerado como alternar manualmente a chave. A rotação manual é uma boa opção quando você deseja girar chaves KMS que não estão qualificadas para rotação automática de chaves, incluindo chaves KMS assimétricas, chaves HMAC KMS, chavesKMS em armazenamentos de chavespersonalizadas e chaves KMS com material de chave importado.

Alternância de chaves e definição de preço

AWS KMS cobra uma taxa mensal pela primeira e segunda rotação do material de chave mantido para sua chave KMS. Esse aumento de preço é limitado à segunda rotação, e quaisquer rotações subsequentes não serão cobradas. Para obter mais informações, consulte Definição de preço do AWS Key Management Service.

> **Note**
>
> É possível usar o AWS Cost Explorer Service para ver um detalhamento das cobranças de armazenamento de chaves. Por exemplo, é possível filtrar a visualização para ver o total de cobranças de chaves cobradas como chaves KMS atuais e alternadas especificando `$REGION-KMS-Keys` para o Tipo de Uso e agrupando os dados por Operação de API. Talvez você ainda veja instâncias da operação da API `Unknown` legada para datas históricas.

Alternância de chaves e cotas

Cada chave do KMS conta como uma chave ao calcular cotas de recursos de chaves, independentemente do número de versões de material de chave alternadas.

Para obter informações detalhadas sobre chaves de backup e alternância, consulte o Detalhes criptográficos do AWS Key Management Service.

Tópicos

- Por que alternar as chaves do KMS?
- Como funciona a rotação de chaves
- Como habilitar e desabilitar a rotação de chaves automática
- Como realizar a rotação de chaves sob demanda
- Alterar chaves manualmente

Por que alternar as chaves do KMS?

As melhores práticas criptográficas desencorajam a reutilização extensiva de chaves que criptografam dados diretamente, como as chaves de dados geradas. AWS KMS Quando as chaves de dados de 256 bits criptografam milhões de mensagens, elas podem se esgotar e começar a produzir texto cifrado com padrões sutis que atores inteligentes podem explorar para descobrir os bits da chave. Para evitar esse esgotamento de chaves, é melhor usar as chaves de dados uma vez ou apenas algumas vezes, o que alterna efetivamente o material da chave.

No entanto, as chaves do KMS são mais frequentemente usadas como chaves de empacotamento, também conhecidas como chaves de criptografia de chaves. Em vez de criptografar dados, as chaves de empacotamento criptografam as chaves de dados que criptografam seus dados. Dessa forma, elas são usadas com muito menos frequência do que as chaves de dados e quase nunca são reutilizadas o suficiente para correr o risco de esgotamento das chaves.

Apesar desse risco de exaustão muito baixo, talvez seja necessário alternar suas chaves do KMS devido a regras comerciais ou contratuais, ou regulamentações governamentais. Quando for obrigatório alternar as chaves do KMS, recomendamos que você use a alternância automática de chaves onde ela for compatível e a alternância manual de chaves quando a alternância automática de chaves não for compatível.

Você pode considerar realizar rotações sob demanda para demonstrar os principais recursos de rotação de materiais ou para validar scripts de automação. Recomendamos usar rotações sob demanda para rotações não planejadas e usar a rotação automática de chaves com um período de rotação personalizado sempre que possível.

Como funciona a rotação de chaves

A rotação de AWS KMS chaves foi projetada para ser transparente e fácil de usar. AWS KMS suporta rotação opcional de chaves automática e sob demanda somente para chaves gerenciadas pelo cliente.

Rotação automática de chaves

AWS KMS gira a chave KMS automaticamente na próxima data de rotação definida pelo seu período de rotação. Você não precisa lembrar nem programar a atualização.

Rotação sob demanda

Inicie imediatamente a rotação do material de chave associado à sua chave KMS, independentemente de a rotação automática de chaves estar ativada ou não.

Gerenciamento do material de chave

AWS KMS retém todo o material de chaves de uma chave KMS, mesmo se a rotação de chaves estiver desativada. AWS KMS exclui o material da chave somente quando você exclui a chave KMS.

Uso do material de chave

Quando você usa uma chave KMS rotacionada para criptografar dados, AWS KMS usa o material de chave atual. Quando você usa a chave do KMS alternada para descriptografar texto cifrado, o AWS KMS usa a mesma versão do material de chave que foi usado para criptografá-lo. Você não pode selecionar uma versão específica do material chave para operações de descriptografia, escolhe AWS KMS automaticamente a versão correta.

Período de rotação

O período de rotação define o número de dias após você ativar a rotação automática de chaves que AWS KMS girará seu material de chaves e o número de dias entre cada rotação automática de chaves a partir de então. Se você não especificar um valor para ativar `RotationPeriodInDays` a rotação automática de chaves, o valor padrão será 365 dias.

Você pode usar a chave de RotationPeriodInDays condição kms: para restringir ainda mais os valores que os principais podem especificar no parâmetro. `RotationPeriodInDays`

Data de alternância

AWS KMS gira automaticamente a chave KMS na data de rotação definida pelo seu período de rotação. O período de rotação padrão é de 365 dias.

Chaves gerenciadas pelo cliente

Como a alternância automática de chaves é opcional nas chaves gerenciadas pelo cliente e pode ser ativada e desativada a qualquer momento, a data de alternância dependerá da data em que a alternância foi ativada mais recentemente. A data pode mudar se você modificar o período de rotação de uma chave na qual você ativou anteriormente a rotação automática de chaves. A data de rotação pode mudar várias vezes ao longo da vida útil da chave.

Por exemplo, se você criar uma chave gerenciada pelo cliente em 1º de janeiro de 2022 e ativar a rotação automática de chaves com o período de rotação padrão de 365 dias em 15 de março de 2022, AWS KMS alterna o material da chave em 15 de março de 2023, 15 de março de 2024 e a cada 365 dias depois disso.

Os exemplos a seguir pressupõem que a rotação automática de chaves foi ativada com o período de rotação padrão de 365 dias. Esses exemplos demonstram casos especiais que podem afetar o período de rotação de uma chave.

- Desabilitar a alternância de chaves — Se você desabilitar a alternância de chaves automática a qualquer momento, a chave do KMS continuará usando a versão do material de chaves que estava usando quando a alternância foi desabilitada. Se você ativar a rotação automática da chave novamente, AWS KMS gira o material da chave com base na nova data de ativação da rotação.
- Chaves KMS desativadas — Quando uma chave KMS está desativada, AWS KMS ela não é girada. No entanto, o status da alternância de chaves não muda, e você não pode alterá-lo enquanto a chave do KMS está desabilitada. Quando a chave KMS é reativada, se o material da chave tiver passado da última data de rotação programada, ele será AWS KMS rotacionado imediatamente. Se o material da chave não tiver perdido a última data de rotação programada, AWS KMS retoma a programação de rotação da chave original.
- Chaves KMS com exclusão pendente — Enquanto uma chave KMS está pendente de exclusão, AWS KMS não a gira. O status da alternância de chaves é definido como `false` e você não pode alterá-lo enquanto a exclusão estiver pendente. Se a exclusão for cancelada, o status da alternância de chaves anterior será restaurado. Se o material principal tiver passado da última data de rotação programada, ele será AWS KMS rotacionado imediatamente. Se o material da chave não tiver perdido a última data de rotação programada, AWS KMS retoma a programação de rotação da chave original.

Chaves gerenciadas pela AWS

AWS KMS gira automaticamente a Chaves gerenciadas pela AWS cada ano (aproximadamente 365 dias). Não é possível habilitar ou desabilitar a alternância de chaves para Chaves gerenciadas pela AWS.

O material principal de um Chave gerenciada pela AWS é rotacionado primeiro um ano após a data de criação e, a partir de então, todos os anos (aproximadamente 365 dias a partir da última rotação).

> **Note**
>
> Em maio de 2022, AWS KMS alterou o cronograma de rotação Chaves gerenciadas pela AWS de três em três anos (aproximadamente 1.095 dias) para todos os anos (aproximadamente 365 dias).
> Chaves gerenciadas pela AWS Os novos são alternados automaticamente um ano após serem criados e aproximadamente a cada ano a partir de então.
> Chaves gerenciadas pela AWS Os existentes são alternados automaticamente um ano após a rotação mais recente e todos os anos a partir de então.

Chaves pertencentes à AWS

Não é possível habilitar ou desabilitar a alternância de chaves para Chaves pertencentes à AWS. A estratégia de rotação de chaves para um Chave pertencente à AWS é determinada pelo AWS serviço que cria e gerencia a chave. Para obter detalhes, consulte o tópico Criptografia em repouso, no manual do usuário ou no guia do desenvolvedor do serviço.

Tipos de chave do KMS com suporte

A alternância automática de chaves só é compatível com chaves do KMS de criptografia simétrica com material de chave que o AWS KMS gera (origem = AWS_KMS).

A alternância automática de chaves não tem suporte com os seguintes tipos de chaves do KMS, mas você pode alternar essas chaves do KMS manualmente.

- Chaves do KMS assimétricas
- Chaves do KMS de HMAC
- Chaves do KMS em armazenamentos de chaves personalizados

- Chaves do KMS com material de chave importado

Chaves de várias regiões

Você pode habilitar e desabilitar a alternância automática de chaves parachaves de várias regiões. Você define a propriedade apenas na chave primária. Quando AWS KMS sincroniza as chaves, ele copia a configuração da propriedade da chave primária para suas chaves de réplica. Quando o material da chave primária é girado, copia AWS KMS automaticamente esse material de chave para todas as suas chaves de réplica. Para obter detalhes, consulte Alternância de chaves de várias regiões.

AWS serviços

É possível habilitar a alternância automática de chaves nas chaves gerenciadas pelo cliente que você usa para criptografia no lado do servidor em serviços da AWS . A alternância anual é transparente e compatível com os serviços da AWS .

Monitoramento da alternância de chaves

Quando AWS KMS gira o material da chave para uma chave gerenciada Chave gerenciada pela AWSou gerenciada pelo cliente, ele grava um `KMS CMK Rotation` evento na Amazon EventBridge e um RotateKey evento em seu AWS CloudTrail registro. É possível usar esses registros para verificar se a chave do KMS foi alternada.

Você pode usar o AWS Key Management Service console para visualizar o número de rotações sob demanda restantes e uma lista de todas as rotações de material-chave concluídas para uma chave KMS.

Você pode usar a ListKeyRotationsoperação para visualizar os detalhes das rotações concluídas.

Consistência eventual

A rotação de chaves está sujeita aos mesmos efeitos de consistência eventuais de outras operações AWS KMS de gerenciamento. Pode haver um pequeno atraso antes que o novo material de chave esteja disponível no AWS KMS. Porém, o material de chave alternante não causa interrupção ou atraso em operações de criptografia. O material de chave atual será usado em operações de criptografia até que o novo material de chave esteja disponível no AWS KMS. Quando o material-chave de uma chave multirregional é rotacionado automaticamente, AWS KMS usa o material de chave atual até que o novo material de chave esteja disponível em todas as regiões com uma chave multirregional relacionada.

Como habilitar e desabilitar a rotação de chaves automática

Por padrão, quando você ativa a rotação automática de chaves para uma chave KMS, AWS KMS gera novo material criptográfico para a chave KMS todos os anos. Você também pode especificar um personalizado rotation-period para definir o número de dias após ativar a rotação automática de chaves que AWS KMS girará o material da chave e o número de dias entre cada rotação automática a partir de então.

A alternância de chaves automática tem os seguintes benefícios:

- As propriedades da chave do KMS, incluindo seu ID de chave, ARN de chave, região, políticas e permissões, não são alteradas quando há alternância na chave.
- Não é necessário alterar aplicações ou aliases que fazem referência ao ID de chave ou ARN de chave da chave do KMS.
- A alternância do material de chave não afeta o uso da chave do KMS em nenhum AWS service (Serviço da AWS).
- Depois de ativar a rotação da chave, AWS KMS gira a chave KMS automaticamente na próxima data de rotação definida pelo seu período de rotação. Você não precisa lembrar nem programar a atualização.

Usuários autorizados podem usar o AWS KMS console e a AWS KMS API para ativar e desativar a rotação automática de chaves e visualizar o status da rotação de chaves.

Tópicos

- Ativando e desativando a rotação automática de chaves (console)
- Ativando e desativando a rotação automática de chaves (AWS KMS API)

Ativando e desativando a rotação automática de chaves (console)

1. Faça login AWS Management Console e abra o console AWS Key Management Service (AWS KMS) em https://console.aws.amazon.com/kms.
2. Para alterar o Região da AWS, use o seletor de região no canto superior direito da página.
3. No painel de navegação, escolha Chaves gerenciadas pelo cliente. (Não é possível habilitar ou desabilitar a alternância de Chaves gerenciadas pela AWS. Elas são alternadas automaticamente a cada ano.)
4. Escolha o alias ou ID de chave de uma chave do KMS.

5. Selecione a guia Key rotation (Rotação de chaves).

   A guia Rotação de chaves aparece somente na página de detalhes das chaves KMS de criptografia simétrica com o material de chave AWS KMS gerado (a origem é AWS_KMS), incluindo chaves KMS de criptografia simétrica multirregional.

   Não é possível alternar automaticamente chaves do KMS assimétricas, chaves do KMS de HMAC, chaves do KMS com material de chave importado nem chaves do KMS em armazenamentos personalizados de chave. No entanto, é possível alterná-las manualmente.
6. Na seção Rotação automática de chaves, escolha Editar.
7. Em Rotação de chaves, selecione Ativar.

   > **Note**
   >
   > Se uma chave KMS estiver desativada ou pendente de exclusão, AWS KMS ela não rotacionará o material da chave e você não poderá atualizar o status da rotação automática da chave ou o período de rotação. Ative a chave KMS ou cancele a exclusão para atualizar a configuração de rotação automática de chaves. Para obter mais detalhes, consulte Como funciona a rotação de chaves e Principais estados das AWS KMS chaves.
8. (Opcional) Digite um período de rotação entre 90 e 2560 dias. O valor padrão é 365 dias. Se você não especificar um período de rotação personalizado, AWS KMS alternará o material da chave todos os anos.

   Você pode usar a chave de RotationPeriodInDays condição kms: para limitar os valores que os diretores podem especificar para o período de rotação.
9. Escolha Salvar.

Ativando e desativando a rotação automática de chaves (AWS KMS API)

Você pode usar a API AWS Key Management Service (AWS KMS) para ativar e desativar a rotação automática de chaves e visualizar o status atual da rotação de qualquer chave gerenciada pelo cliente. Estes exemplos usam a AWS Command Line Interface (AWS CLI), mas você pode usar qualquer linguagem de programação compatível.

A EnableKeyRotationoperação permite a rotação automática de chaves para a chave KMS especificada. A DisableKeyRotationoperação o desativa. Para identificar a chave do KMS nessas

operações, use seu ID de chave ou ARN de chave. Por padrão, a mudança de chaves está desabilitada nas chaves gerenciadas de cliente.

Você pode usar a chave de RotationPeriodInDays condição kms: para limitar os valores que os principais podem especificar para o `RotationPeriodInDays` parâmetro de uma `EnableKeyRotation` solicitação.

O exemplo a seguir permite a rotação de chaves com um período de rotação de 180 dias na chave KMS de criptografia simétrica especificada e usa a GetKeyRotationStatusoperação para ver o resultado. Ele desabilita a alternância de chaves e, novamente, usa GetKeyRotationStatus para ver a alteração.

```
$ aws kms enable-key-rotation \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --rotation-period-in-days 180

$ aws kms get-key-rotation-status --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
{
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "KeyRotationEnabled": true,
    "RotationPeriodInDays": 180,
    "NextRotationDate": "2024-02-14T18:14:33.587000+00:00"
}

$ 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
{
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "KeyRotationEnabled": false
}
```

Como realizar a rotação de chaves sob demanda

Você pode realizar a rotação sob demanda do material de chaves nas chaves KMS gerenciadas pelo cliente, independentemente de a rotação automática de chaves estar ativada ou não. Desativar a rotação automática (DisableKeyRotation) não afeta sua capacidade de realizar rotações sob demanda, nem cancela nenhuma rotação sob demanda em andamento. As rotações sob demanda não alteram os cronogramas de rotação automática existentes. Por exemplo, considere uma chave KMS que tenha a rotação automática de chaves ativada com um período de rotação de 730 dias. Se

a chave estiver programada para alternar automaticamente em 14 de abril de 2024 e você realizar uma rotação sob demanda em 10 de abril de 2024, a chave girará automaticamente, conforme programado, em 14 de abril de 2024 e a cada 730 dias depois disso.

Você pode realizar a rotação de chaves sob demanda no máximo 10 vezes por chave KMS. Você pode usar o AWS KMS console para visualizar o número de rotações sob demanda restantes disponíveis para uma chave KMS.

A rotação de chaves sob demanda é suportada somente em chaves KMS de criptografia simétrica. Você não pode realizar a rotação sob demanda de chaves KMS assimétricas, chaves HMAC KMS, chaves KMS com material de chave importado ou chaves KMS em um armazenamento de chaves personalizado. Para realizar a rotação sob demanda de um conjunto de chaves multirregionais relacionadas, invoque a rotação sob demanda na chave primária.

Usuários autorizados podem usar o AWS KMS console e a AWS KMS API para iniciar a rotação de chaves sob demanda e visualizar o status da rotação de chaves.

Tópicos

- Iniciando a rotação de chaves sob demanda (console)
- Iniciando a rotação de chaves sob demanda (API)AWS KMS

Iniciando a rotação de chaves sob demanda (console)

1. Faça login AWS Management Console e abra o console AWS Key Management Service (AWS KMS) em https://console.aws.amazon.com/kms.
2. Para alterar o Região da AWS, use o seletor de região no canto superior direito da página.
3. No painel de navegação, escolha Chaves gerenciadas pelo cliente. (Você não pode realizar a rotação sob demanda de. Chaves gerenciadas pela AWS Eles são alternados automaticamente a cada ano.)
4. Escolha o alias ou ID de chave de uma chave do KMS.
5. Selecione a guia Key rotation (Rotação de chaves).

   A guia Rotação de chaves aparece somente na página de detalhes das chaves KMS de criptografia simétrica com o material de chave AWS KMS gerado (a origem é AWS_KMS), incluindo chaves KMS de criptografia simétrica multirregional.

Você não pode realizar a rotação sob demanda de chaves KMS assimétricas, chaves HMAC KMS, chaves KMS com material de chave importado ou chaves KMS em armazenamentos de chaves personalizadas. No entanto, é possível alterná-las manualmente.

6. Na seção Rotação de chave sob demanda, escolha Girar chave.
7. Leia e considere o aviso e as informações sobre o número de rotações sob demanda restantes da chave. Se você decidir que não deseja continuar com a rotação sob demanda, escolha Cancelar.
8. Escolha Rotacionar chave para confirmar a rotação sob demanda.

> **Note**
>
> A rotação sob demanda está sujeita aos mesmos efeitos de consistência eventuais de outras operações AWS KMS de gerenciamento. Pode haver um pequeno atraso antes que o novo material de chave esteja disponível no AWS KMS. O banner na parte superior do console notifica você quando a rotação sob demanda for concluída.

Iniciando a rotação de chaves sob demanda (API)AWS KMS

Você pode usar a API AWS Key Management Service (AWS KMS) para iniciar a rotação de chaves sob demanda e visualizar o status atual da rotação de qualquer chave gerenciada pelo cliente. Estes exemplos usam a AWS Command Line Interface (AWS CLI), mas você pode usar qualquer linguagem de programação compatível.

A RotateKeyOnDemandoperação inicia imediatamente a rotação de chaves sob demanda para a chave KMS especificada. Para identificar a chave do KMS nessas operações, use seu ID de chave ou ARN de chave.

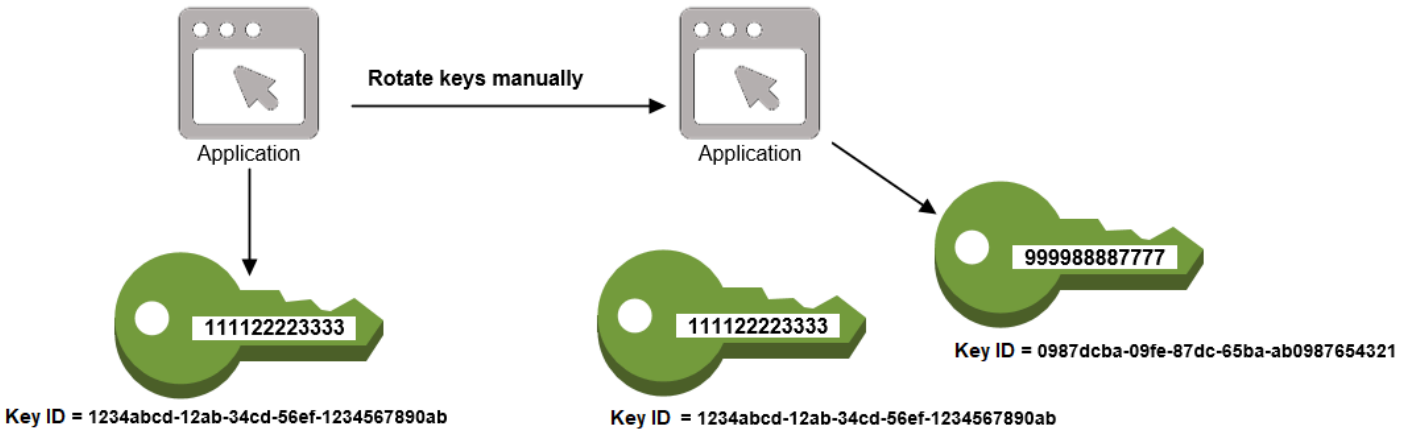
O exemplo a seguir inicia a rotação de chaves sob demanda na chave KMS de criptografia simétrica especificada e usa a GetKeyRotationStatusoperação para verificar se a rotação sob demanda está em andamento. O `OnDemandRotationStartDate` na `kms:GetKeyRotationStatus` resposta identifica a data e a hora em que uma rotação sob demanda em andamento foi iniciada.

```
$ aws kms rotate-key-on-demand --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
{
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
}
```

```
$ aws kms get-key-rotation-status --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
{
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "KeyRotationEnabled": true,
    "NextRotationDate": "2024-03-14T18:14:33.587000+00:00",
    "OnDemandRotationStartDate": "2024-02-24T18:44:48.587000+00:00"
    "RotationPeriodInDays": 365
}
```

Alterar chaves manualmente

Talvez você queira criar uma nova chave do KMS e usá-la no lugar de uma chave do KMS atual, em vez de habilitar a alternância de chaves automática. Quando a nova chave do KMS tem material criptográfico diferente daquele da chave do KMS atual, usar a nova chave do KMS tem o mesmo efeito de alterar o material de chave em uma chave do KMS existente. O processo de substituir uma chave do KMS por outra é conhecido como alternância manual de chaves.



A rotação manual é uma boa opção quando você deseja girar chaves KMS que não estão qualificadas para rotação automática de chaves, como chaves KMS assimétricas, chaves HMAC KMS, chaves KMS em armazenamentos de chaves personalizadas e chaves KMS com material de chave importado.

> **Note**
>
> Ao começar a usar a nova chave KMS, certifique-se de manter a chave KMS original ativada para que ela AWS KMS possa descriptografar os dados criptografados pela chave KMS original.

Ao alternar as chaves do KMS manualmente, você precisa atualizar as referências ao ARN ou ao ID da chave do KMS nas suas aplicações. Aliases, que associam um nome amigável a uma chave do KMS, tornam esse processo mais fácil. Use um alias para fazer referência a uma chave do KMS em suas aplicações. Quando quiser alterar a chave do KMS utilizada pela aplicação, em vez de editar o código da aplicação, altere a chave do KMS de destino do alias. Para obter detalhes, consulte Usar aliases em suas aplicações.

> **Note**
>
> Os aliases que apontam para a versão mais recente de uma chave KMS girada manualmente são uma boa solução para as operações Criptografar DescribeKey,, GenerateDataKeyGenerateDataKeyPairGenerateMac, e Assinar. Aliases não são permitidos em operações que gerenciam chaves KMS, como DisableKeyou. ScheduleKeyDeletion
> Ao chamar a operação Decrypt em chaves KMS de criptografia simétrica giradas manualmente, omita o parâmetro do comando. `KeyId` AWS KMS usa automaticamente a chave KMS que criptografou o texto cifrado.
> O `KeyId` parâmetro é obrigatório ao chamar `Decrypt` ou verificar com uma chave KMS assimétrica ou ao chamar VerifyMaccom uma chave HMAC KMS. Essas solicitações falham quando o valor do parâmetro `KeyId` é um alias que não aponta mais para a chave do KMS que executou a operação criptográfica, como quando uma chave é alternada manualmente. Para evitar esse erro, você deve rastrear e especificar a chave KMS correta para cada operação.

Para alterar a chave KMS de destino de um alias, use a UpdateAliasoperação na AWS KMS API. Por exemplo, este comando atualiza o alias `alias/TestKey` para apontar para uma nova chave do KMS. Como a operação não retorna nenhuma saída, o exemplo usa a ListAliasesoperação para mostrar que o alias agora está associado a uma chave KMS diferente e o `LastUpdatedDate` campo está atualizado. Os ListAliases comandos usam o `query`parâmetro no AWS CLI para obter somente o `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
        },
    ]
}
```

Como monitorar o AWS KMS keys

O monitoramento é uma parte importante do entendimento da disponibilidade, do estado e da utilização das suas AWS KMS keys no AWS KMS e da manutenção da confiabilidade, da disponibilidade e da performance de suas soluções da AWS. Coletar dados de monitoramento de todas as partes de sua solução da AWS irá ajudá-lo a depurar uma falha de vários pontos, caso ocorra. Porém, para começar a monitorar suas chaves do KMS, é necessário criar um plano de monitoramento que inclua respostas às seguintes perguntas:

- Quais são seus objetivos de monitoramento?
- Quais recursos você vai monitorar?
- Com que frequência você vai monitorar esses recursos?
- Quais ferramentas de monitoramento você usará?
- Quem realizará o monitoramento das tarefas?
- Quem deve ser notificado quando algo acontece?

A próxima etapa é monitorar as chaves do KMS ao longo do tempo para estabelecer uma linha de base para a utilização normal do AWS KMS e as expectativas no ambiente. Ao monitorar as suas chaves do KMS, armazene dados de monitoramento históricos para compará-los com os dados atuais, identificar padrões normais e anomalias e elaborar métodos para resolver problemas.

Por exemplo, é possível monitorar as atividades e os eventos da API do AWS KMS que afetam as chaves do KMS. Quando os dados ficam acima ou abaixo das normas estabelecidas, pode ser necessário investigar ou executar a ação corretiva.

Para estabelecer uma linha de base para padrões normais, monitore os seguintes itens:

- A atividade da API do AWS KMS para as operações do plano de dados. Essas são operações criptográficas que usam uma chave KMS, como Decrypt, Encrypt, e. ReEncryptGenerateDataKey
- A atividade da API do AWS KMS para operações do plano de controle que são importantes para você. Essas operações gerenciam uma chave KMS, e talvez você queira monitorar aquelas que alteram a disponibilidade de uma chave KMS (como ScheduleKeyDeletion,,, CancelKeyDeletionDisableKeyEnableKeyImportKeyMaterial, e DeleteImportedKeyMaterial) ou alteram o controle de acesso de uma chave KMS (como PutKeyPolicye). RevokeGrant
- Outras métricas do AWS KMS (como o tempo restante até a validade do material de chave importado) e eventos (como a validade do material de chave importado ou a exclusão ou a alternância de uma chave do KMS).

Ferramentas de monitoramento

A AWS fornece várias ferramentas que podem ser usadas para monitorar suas chaves do KMS. É possível configurar algumas dessas ferramentas para fazer o monitoramento em seu lugar, e, ao mesmo tempo, algumas das ferramentas exigem intervenção manual. Recomendamos que as tarefas de monitoramento sejam automatizadas ao máximo possível.

Ferramentas de monitoramento automatizadas

Use as seguintes ferramentas de monitoramento automatizadas para observar suas chaves do KMS e gerar relatórios quando algo for alterado.

- AWS CloudTrailMonitoramento de registros — compartilhe arquivos de log entre contas, monitore arquivos de CloudTrail log em tempo real enviando-os para o CloudWatch Logs, grave aplicativos de processamento de log com a Biblioteca de CloudTrail Processamento e valide se seus arquivos

de log não foram alterados após a entrega. CloudTrail Para obter mais informações, consulte Trabalhando com arquivos de CloudTrail log no Guia AWS CloudTrail do usuário.

- Amazon CloudWatch Alarms — Observe uma única métrica durante um período de tempo especificado por você e execute uma ou mais ações com base no valor da métrica em relação a um determinado limite em vários períodos. A ação é uma notificação enviada para um tópico do Amazon Simple Notification Service (Amazon SNS) ou para uma política do Amazon EC2 Auto Scaling. CloudWatch os alarmes não invocam ações simplesmente porque estão em um determinado estado; o estado deve ter sido alterado e mantido por um determinado número de períodos. Para ter mais informações, consulte Monitoramento com a Amazon CloudWatch.
- Amazon EventBridge — Combine eventos e encaminhe-os para uma ou mais funções ou fluxos de destino para capturar informações sobre o estado e, se necessário, fazer alterações ou tomar medidas corretivas. Para obter mais informações, consulte Monitoramento com a Amazon EventBridge o Guia do EventBridge usuário da Amazon.
- Amazon CloudWatch Logs — Monitore, armazene e acesse seus arquivos de log de AWS CloudTrail ou de outras fontes. Para obter mais informações, consulte o Guia do usuário do Amazon CloudWatch Logs.

Ferramentas de monitoramento manual

Outra parte importante do monitoramento das chaves KMS envolve o monitoramento manual dos itens que os CloudWatch alarmes e eventos não cobrem. Os AWS painéis AWS KMS CloudWatch,AWS Trusted Advisor,, e outros fornecem uma at-a-glance visão do estado do seu AWS ambiente.

É possível personalizar as páginas Chaves gerenciadas pela AWS e Customer managed keys (Chaves gerenciadas pelo cliente) do console do AWS KMS para exibir as seguintes informações sobre cada chave do KMS:

- ID da chave
- Status
- Data de Criação
- Data de validade (para chaves do KMS com material de chave importado)
- Origem
- ID de armazenamento de chave personalizado (para chaves do KMS em armazenamentos de chaves personalizados)

O painel do console do CloudWatch mostra o seguinte:

- Alertas e status atual
- Gráficos de alertas e recursos
- Estado de integridade do serviço

Além disso, você pode usar CloudWatch para fazer o seguinte:

- Crie painéis personalizados para monitorar os serviços com os quais você se preocupa.
- Colocar em gráfico dados de métrica para solucionar problemas e descobrir tendências
- Pesquisar e procurar todas as métricas de recursos da AWS
- Criar e editar alertas para ser notificado sobre problemas

O AWS Trusted Advisor pode ajudar a monitorar os recursos da AWS para melhorar a performance, a confiabilidade, a segurança e a economia. Quatro verificações do Trusted Advisor estão disponíveis a todos os usuários; mais de 50 verificações estão disponíveis para usuários com um plano de suporte Business ou Enterprise. Para ter mais informações, consulte AWS Trusted Advisor.

Registrando chamadas de AWS KMS API com AWS CloudTrail

AWS KMS é integrado com AWS CloudTrail, um serviço que registra todas as chamadas feitas AWS KMS por usuários, funções e outros AWS serviços. CloudTrail captura todas as chamadas de API para AWS KMS como eventos, incluindo chamadas do AWS KMS console, AWS KMS APIs, AWS CloudFormation modelos, o AWS Command Line Interface (AWS CLI) e. AWS Tools for PowerShell

CloudTrail registra todas as AWS KMS operações, incluindo operações somente para leitura, como ListAliasese GetKeyRotationStatus, operações que gerenciam chaves KMS, como e, CreateKeye operações criptográficas PutKeyPolicy, como e Decrypt. GenerateDataKey Ele também registra operações internas que AWS KMS chamam por você DeleteExpiredKeyMaterial, como DeleteKeySynchronizeMultiRegionKey,, RotateKeye.

CloudTrail registra operações bem-sucedidas e tentativas de chamadas que falharam, como quando o chamador não tem acesso a um recurso. As operações entre contas em chaves do KMS são registradas em log na conta do autor da chamada e na conta do proprietário da chave do KMS. No entanto, as AWS KMS solicitações entre contas que são rejeitadas porque o acesso foi negado são registradas somente na conta do chamador.

Por motivos de segurança, alguns campos são omitidos das entradas de AWS KMS registro, como o `Plaintext` parâmetro de uma solicitação Encrypt e a resposta GetKeyPolicyou qualquer operação criptográfica. Para facilitar a pesquisa de entradas de CloudTrail registro para chaves KMS específicas, AWS KMS adiciona o ARN da chave KMS afetada ao `responseElements` campo nas entradas de registro de AWS KMS algumas operações de gerenciamento de chaves, mesmo quando a operação da API não retorna o ARN da chave.

Embora, por padrão, todas AWS KMS as ações sejam registradas como CloudTrail eventos, você pode excluir AWS KMS ações de uma CloudTrail trilha. Para obter detalhes, consulte Excluindo AWS KMS eventos de uma trilha.

Saiba mais:

- Para obter exemplos de CloudTrail registros de AWS KMS operações para um enclave AWS Nitro, consulte. Solicitações de monitoramento para Nitro enclaves

Tópicos

- Registrando eventos em CloudTrail
- Pesquisando eventos em CloudTrail
- Excluindo AWS KMS eventos de uma trilha
- Exemplos de entradas de AWS KMS registro

Registrando eventos em CloudTrail

CloudTrail é ativado no seu Conta da AWS quando você cria a conta. Quando a atividade ocorre em AWS KMS, essa atividade é registrada em um CloudTrail evento junto com outros eventos AWS de serviço no histórico de eventos. Você pode exibir, pesquisar e baixar eventos recentes em sua Conta da AWS. Para obter mais informações, consulte Visualização de eventos com histórico de CloudTrail eventos.

Para um registro contínuo dos eventos em sua Conta da AWS, incluindo eventos para AWS KMS, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as Regiões da AWS. A trilha registra eventos de todas as regiões na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros Serviços da AWS para analisar e agir com base nos dados do evento coletados nos CloudTrail registros. Para obter mais informações, consulte:

- Visão geral da criação de uma trilha
- CloudTrail serviços e integrações suportados
- Configurando notificações do Amazon SNS para CloudTrail
- Recebendo arquivos de CloudTrail log de várias regiões e Recebendo arquivos de CloudTrail log de várias contas

Para saber mais sobre isso CloudTrail, consulte o Guia AWS CloudTrail do usuário. Para ver outras maneiras de monitorar o uso das suas chaves do KMS, consulte Como monitorar o AWS KMS keys.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi realizada com credenciais raiz ou as credenciais de um usuário do IAM.
- Se a solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado.
- Se a solicitação foi feita por outra pessoa AWS service (Serviço da AWS).

Para obter mais informações, consulte o elemento CloudTrail UserIdentity.

Pesquisando eventos em CloudTrail

Para pesquisar entradas de CloudTrail registro, use o CloudTrail console ou a CloudTrail LookupEventsoperação. CloudTrail suporta vários valores de atributos para filtrar sua pesquisa, incluindo nome do evento, nome do usuário e fonte do evento.

Para ajudá-lo a pesquisar entradas de AWS KMS registro em CloudTrail, AWS KMS preenche os seguintes campos de entrada de CloudTrail registro.

> **Note**
>
> A partir de dezembro de 2022, AWS KMS preenche os atributos Tipo de recurso e Nome do recurso em todas as operações de gerenciamento que alteram uma chave KMS específica. Esses valores de atributos podem ser nulos em CloudTrail entradas mais antigas para as seguintes operações: CreateAliasCreateGrantDeleteAlias, DeleteImportedKeyMaterial, ImportKeyMaterial, ReplicateKey, RetireGrant, RevokeGrant, UpdateAlias, e. UpdatePrimaryRegion

Atributo	Valor	Entradas de log
Origem do evento (`EventSource`)	`kms.amazonaws.com`	Todas as operações.
Tipo de recurso (`ResourceType`)	`AWS::KMS::Key`	Operações de gerenciamento que alteram uma chave do KMS específica, como `CreateKey` e `EnableKey`, mas não `ListKeys`.
Nome do recurso (`ResourceName`)	ARN da chave (ou ID da chave e ARN da chave)	Operações de gerenciamento que alteram uma chave do KMS específica, como `CreateKey` e `EnableKey`, mas não `ListKeys`.

Para ajudá-lo a encontrar entradas de registro para operações de gerenciamento em chaves KMS específicas, AWS KMS registra o ARN da chave KMS afetada no elemento `responseElements.keyId` da entrada de registro, mesmo quando a operação da API não AWS KMS retorna o ARN da chave.

Por exemplo, uma chamada bem-sucedida para a DisableKeyoperação não retorna nenhum valor na resposta, mas em vez de um valor nulo, o `responseElements.keyId` valor na entrada do DisableKey registro inclui o ARN da chave KMS desativada.

Esse recurso foi adicionado em dezembro de 2022 e afeta as seguintes entradas de CloudTrail registro: CreateAliasCreateGrantDeleteAlias, DeleteKey, DisableKey, EnableKey, EnableKeyRotation, ImportKeyMaterial, RotateKey, SynchronizeMultiRegionKey, TagResource, UntagResource, UpdateAlias,, UpdatePrimaryRegione.

Excluindo AWS KMS eventos de uma trilha

Para fornecer um registro do uso e gerenciamento de seus AWS KMS recursos, a maioria dos AWS KMS usuários confia nos eventos em uma CloudTrail trilha. A trilha pode ser uma fonte valiosa de dados para auditar eventos críticos, como criar, desativar e excluir AWS KMS keys, alterar a política de chaves e o uso de suas chaves KMS por AWS serviços em seu nome. Em alguns casos,

os metadados em uma entrada de CloudTrail registro, como o contexto de criptografia em uma operação de criptografia, podem ajudá-lo a evitar ou resolver erros.

No entanto, como AWS KMS pode gerar um grande número de eventos, AWS CloudTrail permite excluir AWS KMS eventos de uma trilha. Essa configuração por trilha exclui todos os AWS KMS eventos; você não pode excluir eventos específicos AWS KMS .

> **Warning**
>
> A exclusão de AWS KMS eventos de um CloudTrail registro pode obscurecer ações que usam suas chaves KMS. Tenha cuidado ao conceder aos principais a permissão `cloudtrail:PutEventSelectors` que é necessária para executar essa operação.

Para excluir AWS KMS eventos de uma trilha:

- No CloudTrail console, use a configuração Registrar eventos do Serviço de Gerenciamento de Chaves ao criar uma trilha ou atualizar uma trilha. Para obter instruções, consulte Registrar eventos de gerenciamento com o AWS Management Console no Guia AWS CloudTrail do usuário.
- Na CloudTrail API, use a PutEventSelectorsoperação. Adicione o atributo `ExcludeManagementEventSources` aos seletores de eventos com um valor de `kms.amazonaws.com`. Para ver um exemplo, consulte Exemplo: uma trilha que não registra AWS Key Management Service eventos no Guia do AWS CloudTrail usuário.

É possível desativar essa exclusão a qualquer momento alterando a configuração do console ou os seletores de eventos de uma trilha. A trilha então começará a registrar AWS KMS os eventos. No entanto, ele não pode recuperar AWS KMS eventos que ocorreram enquanto a exclusão era efetiva.

Quando você exclui AWS KMS eventos usando o console ou a API, a operação de CloudTrail `PutEventSelectors` API resultante também é registrada nos seus CloudTrail registros. Se AWS KMS os eventos não aparecerem nos seus CloudTrail registros, procure um `PutEventSelectors` evento com o `ExcludeManagementEventSources` atributo definido como`kms.amazonaws.com`.

Exemplos de entradas de AWS KMS registro

AWS KMS grava entradas no seu CloudTrail registro quando você chama uma AWS KMS operação e quando um AWS serviço chama uma operação em seu nome. AWS KMS também grava uma entrada quando chama uma operação para você. Por exemplo, ele grava uma entrada quando exclui uma chave do KMS que você agendou para exclusão.

Os tópicos a seguir mostram exemplos de entradas de CloudTrail registro para AWS KMS operações.

Para obter exemplos de entradas de CloudTrail registro de solicitações AWS KMS do AWS Nitro Enclaves, consulte. Solicitações de monitoramento para Nitro enclaves

Tópicos

- CancelKeyDeletion
- ConnectCustomKeyStore
- CreateAlias
- CreateCustomKeyStore
- CreateGrant
- CreateKey
- Decrypt
- DeleteAlias
- DeleteCustomKeyStore
- DeleteExpiredKeyMaterial
- DeleteImportedKeyMaterial
- DeleteKey
- DescribeCustomKeyStores
- DescribeKey
- DisableKey
- DisableKeyRotation
- DisconnectCustomKeyStore
- EnableKey
- EnableKeyRotation
- Encrypt
- GenerateDataKey
- GenerateDataKeyPair
- GenerateDataKeyPairWithoutPlaintext

- GenerateDataKeyWithoutPlaintext
- GenerateMac
- GenerateRandom
- GetKeyPolicy
- GetKeyRotationStatus
- GetParametersForImport
- ImportKeyMaterial
- ListAliases
- ListGrants
- ListKeyRotations
- PutKeyPolicy
- ReEncrypt
- ReplicateKey
- RetireGrant
- RevokeGrant
- RotateKey
- RotateKeyOnDemand
- ScheduleKeyDeletion
- Sign
- SynchronizeMultiRegionKey
- TagResource
- UntagResource
- UpdateAlias
- UpdateCustomKeyStore
- UpdateKeyDescription
- UpdatePrimaryRegion
- VerifyMac
- Verificar

- Exemplo 1 do Amazon EC2
- Exemplo 2 do Amazon EC2

CancelKeyDeletion

O exemplo a seguir mostra uma entrada de log do AWS CloudTrail gerada pela chamada da operação CancelKeyDeletion. Para obter informações sobre como excluir AWS KMS keys, consulte Excluir 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

O exemplo a seguir mostra uma entrada de log do AWS CloudTrail gerada pela chamada da operação `ConnectCustomKeyStore`. Para obter informações sobre conexão de um armazenamento de chaves personalizado, consulte Conectar e desconectar um armazenamento de chaves do 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

O exemplo a seguir mostra uma entrada de AWS CloudTrail registro para a CreateAliasoperação. O elemento `resources` inclui campos para o alias e recursos de chaves do KMS. Para obter informações sobre como criar aliases no AWS KMS, consulte Criar um alias.

CloudTrail as entradas de registro dessa operação registradas em ou após dezembro de 2022 incluem o ARN da chave KMS afetada no `responseElements.keyId` valor, mesmo que essa operação não retorne o ARN da chave.

```
{
    "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

O exemplo a seguir mostra uma entrada de log do AWS CloudTrail gerada pela chamada da operação `CreateCustomKeyStore` em um armazenamento de chaves do AWS CloudHSM. Para obter informações sobre a criação de armazenamentos de chaves personalizados, consulte Criar um armazenamento de chaves do 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

O exemplo a seguir mostra uma entrada de AWS CloudTrail registro para a CreateGrantoperação. Para obter informações sobre como criar concessões no AWS KMS, consulte Concessões no AWS KMS.

CloudTrail as entradas de registro dessa operação registradas em ou após dezembro de 2022 incluem o ARN da chave KMS afetada no `responseElements.keyId` valor, mesmo que essa operação não retorne o ARN da chave.

```
{
  "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

Esses exemplos mostram entradas de AWS CloudTrail registro da CreateKeyoperação.

Uma entrada de `CreateKey` registro pode resultar de uma `CreateKey` solicitação ou da `CreateKey` operação de uma ReplicateKeysolicitação.

O exemplo a seguir mostra uma entrada de CloudTrail registro para uma CreateKeyoperação que cria uma chave KMS de criptografia simétrica. Para obter mais informações sobre como criar chaves do KMS, consulte Criar chaves.

```
{
    "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"
}
```

O exemplo a seguir mostra o CloudTrail log de uma `CreateKey` operação que cria uma chave KMS de criptografia simétrica em um armazenamento de AWS CloudHSMchaves.

```
{
    "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"
}
```

O exemplo a seguir mostra o CloudTrail log de uma `CreateKey` operação que cria uma chave KMS de criptografia simétrica em um armazenamento de chaves externo.

```
{
    "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

Esses exemplos mostram entradas de log do AWS CloudTrail para a operação Decrypt.

A entrada de CloudTrail registro de uma `Decrypt` operação sempre inclui o `encryptionAlgorithm` in the, `requestParameters` mesmo que o algoritmo de criptografia não tenha sido especificado na solicitação. O texto cifrado na solicitação e o texto sem formatação na resposta são omitidos.

Tópicos

- Descriptografar com uma chave de criptografia simétrica padrão
- Descriptografar falhas com uma chave de criptografia simétrica padrão
- Descriptografar com uma chave do KMS em um armazenamento de chaves do AWS CloudHSM
- Descriptografar com uma chave do KMS em um armazenamento de chaves externas
- Descriptografar falhas com uma chave do KMS em um armazenamento de chaves externas

Descriptografar com uma chave de criptografia simétrica padrão

Veja a seguir um exemplo de entrada de CloudTrail registro para uma `Decrypt` operação com uma chave de criptografia simétrica padrão.


```
{
    "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"
```

```
}
```

Descriptografar falhas com uma chave de criptografia simétrica padrão

O exemplo de entrada de CloudTrail registro a seguir registra uma `Decrypt` operação com falha com uma chave KMS de criptografia simétrica padrão. A exceção (`errorCode`) e a mensagem de erro (`errorMessage`) foram incluídas para ajudar a resolver o erro.

Nesse caso, a chave do KMS de criptografia simétrica especificada na solicitação `Decrypt` não era a chave do KMS de criptografia simétrica usada para criptografar os dados.

```
{
    "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"
}
```

Descriptografar com uma chave do KMS em um armazenamento de chaves do AWS CloudHSM

O exemplo de entrada de CloudTrail registro a seguir `Decrypt` registra uma operação com uma chave KMS em um armazenamento de AWS CloudHSM chaves. Todas as entradas de log para operações criptográficas com uma chave do KMS em um armazenamento de chaves personalizado incluem um campo `additionalEventData` com o `customKeyStoreId`. `additionalEventData` não é especificado na solicitação.

```
{
    "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"
}
```

Descriptografar com uma chave do KMS em um armazenamento de chaves externas

O exemplo de entrada de CloudTrail registro a seguir `Decrypt` registra uma operação com uma chave KMS em um armazenamento de chaves externo. Além de `customKeyStoreId`, o campo `additionalEventData` inclui o ID da chave externa (`XksKeyId`). `additionalEventData` não é especificado na solicitação.

```
{
    "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"
}
```

Descriptografar falhas com uma chave do KMS em um armazenamento de chaves externas

O exemplo de entrada de CloudTrail registro a seguir registra uma falha na solicitação de uma `Decrypt` operação com uma chave KMS em um armazenamento de chaves externo. CloudWatch registra as solicitações que falham, além das solicitações bem-sucedidas. Ao registrar uma falha, a entrada do CloudTrail registro inclui a exceção (ErrorCode) e a mensagem de erro que a acompanha (ErrorMessage).

Se a solicitação com falha atingir seu proxy de armazenamento de chaves externas, como neste exemplo, você poderá usar o valor `requestId` para associar a solicitação com falha a uma

solicitação correspondente que seu proxy de armazenamento de chaves externas registra, se o proxy os fornecer.

Para obter ajuda com solicitações `Decrypt` em armazenamentos de chaves externas, consulte Erros de descriptografia.


```
{
    "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

O exemplo a seguir mostra uma entrada de AWS CloudTrail registro para a DeleteAliasoperação. Para obter informações sobre como excluir aliases, consulte Excluir um alias.

CloudTrail as entradas de registro dessa operação registradas em ou após dezembro de 2022 incluem o ARN da chave KMS afetada no `responseElements.keyId` valor, mesmo que essa operação não retorne o ARN da chave.

```
{
    "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

O exemplo a seguir mostra uma entrada de log do AWS CloudTrail gerada pela chamada da operação `DeleteCustomKeyStore`. Para obter informações sobre a criação de armazenamentos de chaves personalizados, consulte Excluir um armazenamento de chaves do 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

Ao importar material de chave para uma AWS KMS key (chave KMS), você pode definir uma data e hora de expiração para esse material de chave. AWS KMSregistra uma entrada em seu CloudTrail registro quando você importa o material da chave (com as configurações de expiração) e quando AWS KMS exclui o material da chave expirada. Para obter informações sobre como criar uma chave do KMS com o material de chave importado, consulte Importação de material chave para AWS KMS chaves.

O exemplo a seguir mostra uma entrada de log do AWS CloudTrail gerada quando o AWS KMS exclui o material de chave expirado.


```
{
    "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 você importar material de chave em uma chave KMS, poderá excluir o material de chave importado a qualquer momento usando a DeleteImportedKeyMaterialoperação. Quando você exclui o material de chave importado de uma chave do KMS, o estado da chave da chave do KMS é alterado para `PendingImport`, e a chave do KMS não pode ser usada em operações de criptografia. Para obter detalhes, consulte Excluir o material de chave importada.

O exemplo a seguir mostra uma entrada de log do AWS CloudTrail gerada para a operação `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

Estes exemplos mostram uma entrada de log do AWS CloudTrail gerada quando uma chave do KMS é excluída. Para excluir uma chave KMS, você usa a ScheduleKeyDeletionoperação. Depois que o período de espera especificado expirar, AWS KMS exclui a chave KMS e registra uma entrada como a seguinte em seu registro para CloudTrail registrar esse evento.

CloudTrail as entradas de registro dessa operação registradas em ou após dezembro de 2022 incluem o ARN da chave KMS afetada no `responseElements.keyId` valor, mesmo que essa operação não retorne o ARN da chave.

Para obter um exemplo da entrada de CloudTrail registro da `ScheduleKeyDeletion` operação, consulteScheduleKeyDeletion. Para informações sobre como excluir chaves do KMS, consulteExcluir AWS KMS keys.

O exemplo de entrada de CloudTrail registro a seguir registra uma `DeleteKey` operação de uma chave KMS com material de chave inserido. 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"
}
```

A entrada de CloudTrail registro a seguir registra uma `DeleteKey` operação de uma chave KMS em um armazenamento de chaves AWS CloudHSM personalizado.

```
{
    "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

O exemplo a seguir mostra uma entrada de log do AWS CloudTrail gerada pela chamada da operação `DescribeCustomKeyStores`. Para obter informações sobre visualização de armazenamentos de chaves personalizados, consulte Visualizar um armazenamento de chaves do 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

O exemplo a seguir mostra uma entrada de AWS CloudTrail registro para a DescribeKeyoperação. AWS KMSregistra uma entrada como a seguinte quando você chama a `DescribeKey` operação ou visualiza as chaves KMS no AWS KMS console. Essa chamada é o resultado da visualização de uma chave no console de gerenciamento do 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

O exemplo a seguir mostra uma entrada de AWS CloudTrail registro para a DisableKeyoperação. Para obter informações sobre como habilitar e desabilitar AWS KMS keys no AWS KMS, consulte Habilitar e desabilitar chaves.

CloudTrail as entradas de registro dessa operação registradas em ou após dezembro de 2022 incluem o ARN da chave KMS afetada no `responseElements.keyId` valor, mesmo que essa operação não retorne o ARN da chave.

```
{
    "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

O exemplo a seguir mostra uma entrada de log do AWS CloudTrail gerada pela chamada da operação DisableKeyRotation. Para obter informações sobre alternância automática de chaves, consulte Girando 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

O exemplo a seguir mostra uma entrada de log do AWS CloudTrail gerada pela chamada da operação `DisconnectCustomKeyStore`. Para obter informações sobre desconexão de um armazenamento de chaves personalizado, consulte Conectar e desconectar um armazenamento de chaves do 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

O exemplo a seguir mostra uma entrada de AWS CloudTrail registro para a EnableKeyoperação. Para obter informações sobre como habilitar e desabilitar AWS KMS keys no AWS KMS, consulte Habilitar e desabilitar chaves.

CloudTrail as entradas de registro dessa operação registradas em ou após dezembro de 2022 incluem o ARN da chave KMS afetada no `responseElements.keyId` valor, mesmo que essa operação não retorne o ARN da chave.


```
{
    "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

O exemplo a seguir mostra uma entrada de AWS CloudTrail registro de uma chamada para a EnableKeyRotationoperação. Para obter um exemplo da entrada de CloudTrail registro que é gravada quando a chave é girada, consulteRotateKey. Para obter informações sobre a alternância de AWS KMS keys, consulte Girando AWS KMS keys.

> **Note**
>
> rotation-periodÉ um parâmetro de solicitação opcional. Se você não especificar um período de rotação ao ativar a rotação automática de chaves, o valor padrão será 365 dias.

CloudTrail as entradas de registro dessa operação registradas em ou após dezembro de 2022 incluem o ARN da chave KMS afetada no `responseElements.keyId` valor, mesmo que essa operação não retorne o ARN da chave.

```
{
    "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",
        "rotationPeriodInDays": 180
    },
    "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"
}
```


Encrypt

O exemplo a seguir mostra uma entrada de log do AWS CloudTrail da operação 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

O exemplo a seguir mostra uma entrada de AWS CloudTrail registro para a GenerateDataKeyoperação.


```
{
```

```
    "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

O exemplo a seguir mostra uma entrada de AWS CloudTrail registro para a GenerateDataKeyPairoperação. Este exemplo registra uma operação que gera um par de chaves RSA criptografado com uma AWS KMS key de criptografia simétrica.


```
{
```

```
    "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

O exemplo a seguir mostra uma entrada de AWS CloudTrail registro para a GenerateDataKeyPairWithoutPlaintextoperação. Este exemplo registra uma operação que gera um par de chaves RSA criptografado com uma AWS KMS key de criptografia simétrica.

```
{
    "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

O exemplo a seguir mostra uma entrada de AWS CloudTrail registro para a GenerateDataKeyWithoutPlaintextoperação.

```
{
    "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

O exemplo a seguir mostra uma entrada de AWS CloudTrail registro para a GenerateMacoperação.

```
{
    "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

O exemplo a seguir mostra uma entrada de AWS CloudTrail registro para a GenerateRandomoperação. Como esta operação não usa uma AWS KMS key, o campo `resources` permanece vazio.


```
{
    "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

O exemplo a seguir mostra uma entrada de AWS CloudTrail registro para a GetKeyPolicyoperação. Para obter informações sobre como visualizar a política de chaves de uma chave do KMS, consulte Visualizar uma política de chaves.

```
{
    "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

O exemplo a seguir mostra uma entrada de AWS CloudTrail registro para a GetKeyRotationStatusoperação. Para obter informações sobre a rotação automática e sob demanda do material chave para uma chave KMS, consulte. Girando 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": "2024-02-20T19:16:45Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GetKeyRotationStatus",
    "awsRegion": "us-east-1",
    "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"
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES256-GCM-SHA384",
        "clientProvidedHostHeader": "kms.us-east-1.amazonaws.com"
    }
}
```

GetParametersForImport

O exemplo a seguir mostra uma entrada de AWS CloudTrail registro gerada quando você usa a GetParametersForImportoperação. Essa operação retorna a chave pública e o token de importação usados ao importar material de chave em uma chave do KMS. A mesma CloudTrail entrada é registrada quando você usa a `GetParametersForImport` operação ou usa o AWS KMS console para baixar a chave pública e o token de importação.

```
{
    "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

O exemplo a seguir mostra uma entrada de AWS CloudTrail registro gerada quando você usa a ImportKeyMaterialoperação. A mesma CloudTrail entrada é registrada quando você usa a `ImportKeyMaterial` operação ou usa o AWS KMS console para importar material chave para umAWS KMS key.

CloudTrail as entradas de registro dessa operação registradas em ou após dezembro de 2022 incluem o ARN da chave KMS afetada no `responseElements.keyId` valor, mesmo que essa operação não retorne o ARN da chave.

```
{
    "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

O exemplo a seguir mostra uma entrada de AWS CloudTrail registro para a ListAliasesoperação. Como essa operação não usa uma AWS KMS key ou um alias específico, o campo `resources` está vazio. Para obter informações sobre como visualizar aliases no AWS KMS, consulte Visualizar aliases.


```
{
    "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

O exemplo a seguir mostra uma entrada de AWS CloudTrail registro para a ListGrantoperação. Para obter informações sobre concessões no AWS KMS, consulte Concessões no 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"
}
```


ListKeyRotations

O exemplo a seguir mostra uma entrada de AWS CloudTrail registro para a ListKeyRotationsoperação. Para obter informações sobre a rotação automática e sob demanda do material chave para uma chave KMS, consulte. Girando 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": "2024-02-20T19:16:45Z",
```

```
    "eventSource": "kms.amazonaws.com",
    "eventName": "ListKeyRotations",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "responseElements": null,
    "requestID": "99c88d32-f2db-455e-8a9a-23855258a452",
    "eventID": "8ce0e74b-b9c7-45a2-96ef-83136d38068e",
    "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",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES256-GCM-SHA384",
        "clientProvidedHostHeader": "kms.us-east-1.amazonaws.com"
    }
}
```

PutKeyPolicy

O exemplo a seguir mostra uma entrada de log do AWS CloudTrail gerada pela chamada da operação PutKeyPolicy. Para obter informações sobre como atualizar uma política de chaves, consulte Alterar uma política de chaves.

```
{
    "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

O exemplo a seguir mostra uma entrada de AWS CloudTrail registro para a ReEncryptoperação. O campo `resources` nessa entrada de log especifica duas AWS KMS keys: a chave do KMS de origem e a chave do KMS de destino, nessa ordem.

```
{
    "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

O exemplo a seguir mostra uma entrada de log do AWS CloudTrail gerada pela chamada da operação ReplicateKey. Uma `ReplicateKey` solicitação resulta em uma `ReplicateKey` operação e em uma CreateKeyoperação.

Para informações sobre como replicar chaves de várias regiões, consulte Criar chaves de réplica de várias regiões.

```
{
    "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

O exemplo a seguir mostra uma entrada de log do AWS CloudTrail gerada pela chamada da operação RetireGrant. Para obter informações sobre a retirada de concessões, consulte Retirar e revogar concessões.

```
{
    "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

O exemplo a seguir mostra uma entrada de log do AWS CloudTrail gerada pela chamada da operação RevokeGrant. Para obter informações sobre a revogação de concessões, consulte Retirar e revogar concessões.

```
{
    "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

Esses exemplos mostram as entradas de AWS CloudTrail registro das operações que giram. AWS KMS keys Para informações sobre como alternar chaves do KMS, consulte Girando AWS KMS keys.

O exemplo a seguir mostra uma entrada de CloudTrail registro para a operação que gira uma chave KMS de criptografia simétrica na qual a rotação automática de chaves está ativada. Para obter informações sobre como ativar a rotação automática, consulteComo habilitar e desabilitar a rotação de chaves automática.

Para obter um exemplo da entrada de CloudTrail registro que registra a `EnableKeyRotation` operação, consulteEnableKeyRotation.


```
{
    "eventVersion": "1.08",
    "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": null,
    "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": {
        "rotationType": "AUTOMATIC",
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "eventCategory": "Management"
}
```

O exemplo a seguir mostra uma entrada de CloudTrail registro para uma RotateKeyOnDemandoperação. Para obter informações sobre a rotação de chaves KMS de criptografia simétrica sob demanda, consulte. Como realizar a rotação de chaves sob demanda

Para obter um exemplo da entrada de CloudTrail registro que registra a `RotateKeyOnDemand` operação, consulteRotateKeyOnDemand.

```
{
    "eventVersion": "1.08",
    "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": null,
    "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": {
        "rotationType": "ON_DEMAND",
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "eventCategory": "Management"
}
```

RotateKeyOnDemand

O exemplo a seguir mostra uma entrada de AWS CloudTrail registro para a RotateKeyOnDemandoperação. Para obter um exemplo da entrada de CloudTrail registro que é gravada quando a chave é girada, consulteRotateKey. Para obter mais informações sobre a rotação sob demanda do material de chaves para uma chave KMS, consulte. Como realizar a rotação de chaves sob demanda

```
{
    "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": "2024-02-20T17:41:57Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "RotateKeyOnDemand",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "responseElements": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
```

```
    },
    "requestID": "9e1dee86-eb84-42fd-8f25-e3fc7dbb32c8",
    "eventID": "00a09fbc-20d6-4a58-9b92-7da85984ab77",
    "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",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES256-GCM-SHA384",
        "clientProvidedHostHeader": "kms.us-east-1.amazonaws.com"
    }
}
```

ScheduleKeyDeletion

Esses exemplos mostram entradas de AWS CloudTrail registro da ScheduleKeyDeletionoperação.

Para obter um exemplo da entrada de CloudTrail registro que é gravada quando a chave é excluída, consulteDeleteKey. Para obter informações sobre como excluir AWS KMS keys, consulte Excluir AWS KMS keys.

O exemplo a seguir registra uma solicitação `ScheduleKeyDeletion` para uma chave do KMS de região única.

```
{
    "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"
}
```

O exemplo a seguir registra uma solicitação `ScheduleKeyDeletion` para uma chave do KMS de várias regiões.

Como AWS KMS não excluirá uma chave de várias regiões até que todas as chaves de réplica sejam excluídas, no campo `responseElements`, `keyState` é `PendingReplicaDeletion` e o campo `deletionDate` é omitido.

```
{
    "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"
}
```


O exemplo a seguir registra uma solicitação `ScheduleKeyDeletion` para uma chave do KMS em um armazenamento de chaves personalizado do 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

Esses exemplos mostram entradas de log do AWS CloudTrail referentes à operação Sign.

O exemplo a seguir mostra uma entrada de CloudTrail registro para uma operação de assinatura que usa uma chave RSA KMS assimétrica para gerar uma assinatura digital para um arquivo.

```
{
    "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

O exemplo a seguir mostra uma entrada de log do AWS CloudTrail gerada quando o AWS KMS sincroniza uma chave de várias regiões. A sincronização envolve chamadas entre regiões para copiar as propriedades compartilhadas de uma chave primária de várias regiões para suas chaves de réplica. O AWS KMS sincroniza chaves de várias regiões periodicamente para garantir que todas elas tenham o mesmo material de chave.

O `resources` elemento da entrada de CloudTrail registro inclui o ARN da chave primária multirregional, incluindo sua. Região da AWS As chaves de réplica de várias regiões relacionadas e suas regiões não estão listadas nessa entrada de log.

CloudTrail as entradas de registro dessa operação registradas em ou após dezembro de 2022 incluem o ARN da chave KMS afetada no `responseElements.keyId` valor, mesmo que essa operação não retorne o ARN da chave.

```
{
    "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

O exemplo a seguir mostra uma entrada de AWS CloudTrail registro de uma chamada para a TagResourceoperação para adicionar uma tag com uma chave de tag de `Department` e um valor de tag de`IT`.

Para obter um exemplo de uma entrada de `UntagResource` CloudTrail registro que é gravada quando a chave é girada, consulteUntagResource. Para informações sobre marcação de AWS KMS keys, consulte Marcar chaves com tags.

```
{
    "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

O exemplo a seguir mostra uma entrada de AWS CloudTrail registro de uma chamada para a UntagResourceoperação para excluir uma tag com uma chave de tag de`Dept`.

CloudTrail as entradas de registro dessa operação registradas em ou após dezembro de 2022 incluem o ARN da chave KMS afetada no `responseElements.keyId` valor, mesmo que essa operação não retorne o ARN da chave.

Para obter um exemplo de uma entrada de `TagResource` CloudTrail registro, consulteTagResource. Para informações sobre marcação de AWS KMS keys, consulte Marcar chaves com tags.

```
{
    "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

O exemplo a seguir mostra uma entrada de AWS CloudTrail registro para a UpdateAliasoperação. O elemento `resources` inclui campos para o alias e recursos de chaves do KMS. Para obter informações sobre como criar aliases no AWS KMS, consulte Criar um alias.

CloudTrail as entradas de registro dessa operação registradas em ou após dezembro de 2022 incluem o ARN da chave KMS afetada no `responseElements.keyId` valor, mesmo que essa operação não retorne o ARN da chave.

```
{
    "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

O exemplo a seguir mostra uma entrada de log do AWS CloudTrail gerada pela chamada da operação `UpdateCustomKeyStore` para atualizar o ID do cluster de um armazenamento de chaves personalizado. Para obter informações sobre edição de armazenamentos de chaves personalizados, consulte Editar as configurações do armazenamento de chaves do 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

O exemplo a seguir mostra uma entrada de log do AWS CloudTrail gerada pela chamada da operação 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

O exemplo a seguir mostra as entradas de AWS CloudTrail registro que são geradas ao chamar a UpdatePrimaryRegionoperação em uma chave multirregional.

A `UpdatePrimaryRegion` operação grava duas entradas de CloudTrail registro: uma na região com a chave primária multirregional que é convertida em uma chave de réplica e outra na região com uma chave de réplica multirregional que é convertida em uma chave primária.

CloudTrail as entradas de registro dessa operação registradas em ou após dezembro de 2022 incluem o ARN da chave KMS afetada no `responseElements.keyId` valor, mesmo que essa operação não retorne o ARN da chave.

O exemplo a seguir mostra uma entrada de CloudTrail registro na região `UpdatePrimaryRegion` em que a chave multirregional mudou de uma chave primária para uma chave de réplica (us-west-2). O campo `primaryRegion`mostra a região que agora hospeda a chave primária (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"
}
```

O exemplo a seguir representa a entrada de CloudTrail registro da região `UpdatePrimaryRegion` em que a chave multirregional mudou de uma chave de réplica para uma chave primária (ap-northeast-1). Essa entrada de log não identifica a região primária anterior.

```
{
    "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

O exemplo a seguir mostra uma entrada de AWS CloudTrail registro para a VerifyMacoperação.

```
{
    "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"
}
```

Verificar

Esses exemplos mostram entradas de log do AWS CloudTrail referentes à operação Verify.

O exemplo a seguir mostra uma entrada de CloudTrail registro para uma operação de verificação que usa uma chave RSA KMS assimétrica para verificar uma assinatura digital.

```
{
    "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"
}
```

Exemplo 1 do Amazon EC2

O exemplo a seguir registra uma entidade principal do IAM criando um volume criptografado ao usar a chave de volume padrão no console de gerenciamento do Amazon EC2.

O exemplo a seguir mostra uma entrada de CloudTrail registro na qual a usuária Alice cria um volume criptografado com uma chave de volume padrão no console de gerenciamento do Amazon EC2. O registro do arquivo de log do EC2 inclui um campo `volumeId` com um valor de `"vol-13439757"`. O registro do AWS KMS contém um campo `encryptionContext` com um valor de `"aws:ebs:id": "vol-13439757"`. Da mesma forma, o `principalId` e o `accountId` entre os dois registros coincidem. Os registros refletem o fato de que a criação de um volume criptografado gera uma chave de dados que é usada para criptografar o conteúdo do 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"
    }
  ]
}
```

Exemplo 2 do Amazon EC2

No exemplo a seguir, uma entidade principal do IAM que executa uma instância do Amazon EC2 realiza a criação e a montagem de um volume de dados que é criptografado em uma chave do KMS. Essa ação gera vários registros de CloudTrail log.

Quando o volume é criado, o Amazon EC2, agindo em nome do cliente, obtém uma chave de dados criptografada do AWS KMS (`GenerateDataKeyWithoutPlaintext`). Depois, ele cria uma concessão (`CreateGrant`) que permite descriptografar a chave de dados. Quando o volume é montado, o Amazon EC2 chama o AWS KMS para descriptografar a chave de dados (`Decrypt`).

O`instanceId` da instância do Amazon EC2,`"i-81e2f56c"`, aparece no evento `RunInstances`. O mesmo ID de instância qualifica o `granteePrincipal` da concessão que é criada (`"111122223333:aws:ec2-infrastructure:i-81e2f56c"`) e a função assumida que é o principal na chamada de `Decrypt`(`"arn:aws:sts::111122223333:assumed-role/aws:ec2-infrastructure/i-81e2f56c"`).

O ARN da chave da chave do KMS que protege o volume de dados, `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`, aparece nas três chamadas do 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"
    }
  ]
}
```


Monitoramento com a Amazon CloudWatch

Você pode monitorar seu AWS KMS keys uso da Amazon CloudWatch, um AWS serviço que coleta e processa dados brutos AWS KMS em métricas legíveis e quase em tempo real. Esses dados são registrados por um período de duas semanas, para que você possa acessar informações históricas

e obter um melhor entendimento do uso das suas chaves do KMS e das suas alterações ao longo do tempo.

Você pode usar CloudWatch a Amazon para alertá-lo sobre eventos importantes, como os seguintes.

- O material da chave importada em uma chave do KMS está próximo da data de validade.
- Uma chave do KMS com exclusão pendente ainda está sendo usada.
- O material de chave em uma chave do KMS foi alternado automaticamente.
- Uma chave do KMS foi excluída.

Você também pode criar um CloudWatch alarme da Amazon que o alerta quando sua taxa de solicitação atingir uma determinada porcentagem do valor da cota. Para obter detalhes, consulte Gerenciar suas taxas de solicitação de AWS KMS API usando Service Quotas e Amazon CloudWatch no Blog de AWS Segurança.

Tópicos

- AWS KMS métricas e dimensões
- Visualizando AWS KMS métricas
- Criação de CloudWatch alarmes para monitorar chaves KMS

AWS KMS métricas e dimensões

AWS KMS predefine CloudWatch as métricas da Amazon para facilitar o monitoramento de dados críticos e a criação de alarmes. Você pode visualizar as AWS KMS métricas usando a AWS Management Console e a CloudWatch API da Amazon.

Esta seção lista cada AWS KMS métrica e as dimensões de cada métrica e fornece algumas orientações básicas para criar CloudWatch alarmes com base nessas métricas e dimensões.

> **Note**
>
> Nome do grupo de dimensões:
> Para visualizar uma métrica no CloudWatch console da Amazon, na seção Métricas, selecione o nome do grupo de dimensões. Em seguida, é possível filtrar pelo nome da métrica. O tópico inclui o nome da métrica e o nome do grupo de dimensões para cada métrica do AWS KMS .

Tópicos

- SecondsUntilKeyMaterialExpiration
- ExternalKeyStoreThrottle
- XksProxyCertificateDaysToExpire
- XksProxyCredentialAge
- XksProxyErrors
- XksExternalKeyManagerStates
- XksProxyLatency

SecondsUntilKeyMaterialExpiration

O número de segundos restantes até que o material de chave importado em uma chave do KMS expire. Essa métrica só é válida para chaves do KMS com material de chave importado (uma origem de material de chave de `EXTERNAL`) e data de validade.

Use essa métrica para acompanhar o tempo restante até a expiração do material de chave importado. Quando esse tempo estiver abaixo de um limite definido, convém reimportar o material de chave com uma nova data de validade. A métrica `SecondsUntilKeyMaterialExpiration` é específica para uma chave do KMS. Você não pode usar essa métrica para monitorar várias chaves do KMS ou chaves do KMS que você possa vir a criar futuramente. Para obter ajuda na criação de um CloudWatch alarme para monitorar essa métrica, consulteCriação de um CloudWatch alarme para expiração do material chave importado.

A estatística mais útil para essa métrica é `Minimum`, que informa o menor tempo restante para todos os pontos de dados no período estatístico especificado. A única unidade válida para essa métrica é `Seconds`.

Nome do grupo de dimensões: métricas por chave

Dimensões do **`SecondsUntilKeyMaterialExpiration`**

Dimensão	Descrição; relacionado a AWS
KeyId	Valor para cada chave do KMS.

ExternalKeyStoreThrottle

O número de solicitações de operações criptográficas em chaves KMS em cada armazenamento de chaves externo que acelera AWS KMS (responde com a). `ThrottlingException` Essa métrica se aplica apenas aos armazenamentos de chaves externas.

A `ExternalKeyStoreThrottle` métrica se aplica somente às chaves KMS em um armazenamento de chaves externo e somente às solicitações de operações criptográficas e da DescribeKeyoperação. AWS KMS limita essas solicitações quando a taxa de solicitação excede a cota de solicitações de armazenamento de chaves personalizadas para seu armazenamento de chaves externo. Essa métrica não inclui o controle de utilização por seu proxy de armazenamento de chaves externas ou gerenciador de chaves externas.

Use essa métrica para revisar e ajustar o valor da cota de solicitação de armazenamento de chaves personalizado. Se essa métrica indicar que AWS KMS está frequentemente limitando suas solicitações dessas chaves KMS, considere solicitar um aumento no valor da cota de solicitação do armazenamento de chaves personalizadas. Para obter ajuda, consulte Requesting a quota increase (Solicitar um aumento de cota) no Guia do usuário do Service Quotas.

Se você estiver recebendo erros `KMSInvalidStateException` com muita frequência com uma mensagem que explica que a solicitação foi rejeitada “due to a very high request rate” (devido a uma taxa de solicitação muito alta) ou que a solicitação foi rejeitada “because the external key store proxy did not respond in time” (porque o proxy de armazenamento de chaves externas não respondeu a tempo), isso pode indicar que o gerenciador de chaves externas ou o proxy de armazenamento de chaves externas não consegue acompanhar a taxa de solicitação atual. Se possível, reduza a taxa de solicitação. Considere também solicitar uma redução no valor da cota de solicitação de armazenamento de chaves personalizado. Diminuir esse valor da cota pode aumentar a limitação (e o valor da `ExternalKeyStoreThrottle` métrica), mas indica que AWS KMS está rejeitando solicitações em excesso rapidamente antes de serem enviadas ao proxy externo do armazenamento de chaves ou ao gerenciador de chaves externo. Para solicitar uma redução de cota, acesse o AWS Support Center e crie um caso.

Nome do grupo de dimensões: métrica de controle de utilização de armazenamento de chaves

Dimensão	Descrição
CustomKey StoreId	Valor para cada armazenamento de chaves externas.

Dimensão	Descrição
KmsOperation	Valor para cada operação de AWS KMS API. Essa métrica se aplica somente às operações de criptografia e à operação `DescribeKey` em chaves do KMS em um armazenamento de chaves externas.
KeySpec	Valor para cada tipo de chave do KMS. A única especificação de chave compatível com chaves do KMS em um armazenamento de chaves externas é SYMMETRIC_DEFAULT.

XksProxyCertificateDaysToExpire

O número de dias até o certificado TLS do endpoint do proxy de armazenamento de chaves externas (`XksProxyUriEndpoint`) expirar. Essa métrica se aplica apenas aos armazenamentos de chaves externas.

Use essa métrica para criar um CloudWatch alarme que o notifique sobre a próxima expiração do seu certificado TLS. Quando o certificado expira, AWS KMS não é possível se comunicar com o proxy externo do armazenamento de chaves. Todos os dados protegidos por chaves do KMS em seu armazenamento de chaves externas ficarão inacessíveis até você renovar o certificado.

Um alarme do certificado evita que a expiração do certificado impeça você de acessar os recursos criptografados. Defina o alarme para dar tempo para a sua organização renovar o certificado antes que ele expire.

Nome do grupo de dimensões: métricas de certificado do proxy XKS

Dimensão	Descrição
CustomKeyStoreId	Valor para cada armazenamento de chaves externas.
CertificateName	Nome (CN) da entidade no certificado TLS.

XksProxyCredentialAge

O número de dias desde que a credencial de autenticação do proxy (`XksProxyAuthenticationCredential`) atual do armazenamento de chaves externas foi associada ao armazenamento de chaves externas. Essa contagem começa quando você insere a credencial de autenticação como parte da criação ou atualização do armazenamento de chaves externas. Essa métrica se aplica apenas aos armazenamentos de chaves externas.

Esse valor foi criado para lembrar você sobre a idade da credencial de autenticação. No entanto, como começamos a contagem quando você associa a credencial ao armazenamento de chaves externas, não quando você cria sua credencial de autenticação em seu proxy de armazenamento de chaves externas, isso pode não ser um indicador preciso da idade da credencial no proxy.

Use essa métrica para criar um CloudWatch alarme que lembre você de alternar sua credencial de autenticação de proxy do armazenamento de chaves externo.

Nome do grupo de dimensões: métricas por armazenamento de chaves

Dimensão	Descrição
CustomKeyStoreId	Valor para cada armazenamento de chaves externas.

XksProxyErrors

O número de exceções relacionadas às AWS KMS solicitações ao proxy externo do armazenamento de chaves. Essa contagem inclui exceções às quais o proxy externo do armazenamento de chaves retorna AWS KMS e erros de tempo limite que ocorrem quando o proxy do armazenamento de chaves externo não responde AWS KMS dentro do intervalo de tempo limite de 250 milissegundos. Essa métrica se aplica apenas aos armazenamentos de chaves externas.

Use essa métrica para rastrear a taxa de erro das chaves do KMS no armazenamento de chaves externas. Ela revela os erros mais frequentes para que você possa priorizar seus esforços de engenharia. Por exemplo, chaves do KMS que estão gerando altas taxas de erros sem nova tentativa podem indicar um problema com a configuração do armazenamento de chaves externas. Para visualizar a configuração do armazenamento de chaves externas, consulte Visualizar um armazenamento de chaves externas. Para editar suas configurações de armazenamento de chaves externas, consulte Editar propriedades do armazenamento de chaves externas.

Nome do grupo de dimensões: métricas de erro do proxy XKS

Dimensão	Descrição
CustomKeyStoreId	Valor para cada armazenamento de chaves externas.
KmsOperation	Valor de cada operação de AWS KMS API que gerou uma solicitação para o proxy XKS.
XksOperation	Valor para cada operação de API do proxy de armazenamento de chaves externas.
KeySpec	Valor para cada tipo de chave do KMS. A única especificação de chave compatível com chaves do KMS em um armazenamento de chaves externas é SYMMETRIC_DEFAULT.
ErrorType	Valores: • Erros com nova tentativa: provavelmente são transitórios, como erros de redes. • Erros sem nova tentativa: provavelmente indicam um problema com a configuração do armazenamento de chaves personalizado ou com os componentes externos. • N/A: solicitação bem-sucedida; sem erros
ExceptionName	Valores: • Nome da exceção • Nenhum: solicitação bem-sucedida; sem erros

XksExternalKeyManagerStates

Uma contagem do número de instâncias do gerenciador de chaves externas em cada um dos seguintes estados de integridade: `Active`, `Degraded` e `Unavailable`. As informações dessa métrica vêm do proxy de armazenamento de chaves externas associado a cada armazenamento de chaves externas. Essa métrica se aplica apenas aos armazenamentos de chaves externas.

Veja a seguir os estados de integridade das instâncias externas do gerenciador de chaves associadas a um armazenamento de chaves externas. Cada proxy de armazenamento de chaves externas pode usar indicadores diferentes para medir o estado de integridade do gerenciador de chaves externas. Para obter detalhes, consulte a documentação do proxy de armazenamento de chaves externas.

- `Active`: o gerenciador de chaves externas está íntegro.
- `Degraded`: o gerenciador de chaves externas não está íntegro, mas ainda pode atender ao tráfego
- `Unavailable`: o gerenciador de chaves externas não pode atender ao tráfego.

Use essa métrica para criar um CloudWatch alarme que alerta você sobre instâncias do gerenciador de chaves externo degradadas e indisponíveis. Para determinar quais instâncias externas do gerenciador de chaves estão em cada estado, consulte seus logs de proxy do armazenamento de chaves externas.

Nome do grupo de dimensões: métrica do gerenciados de chaves externas XKS

Dimensão	Descrição
CustomKeyStoreId	Valor para cada armazenamento de chaves externas.
XksExternalKeyManagerState	Valor para cada estado de integridade.

XksProxyLatency

O número de milissegundos necessários para que um proxy de armazenamento de chaves externas responda a uma solicitação do AWS KMS . Se a solicitação atingiu o tempo limite, o valor registrado é o limite de tempo limite de 250 milissegundos. Essa métrica se aplica apenas aos armazenamentos de chaves externas.

Use essas métrica para avaliar a performance do proxy de armazenamento de chaves externas e do gerenciador de chaves externas. Por exemplo, se o proxy estiver frequentemente atingindo o tempo limite nas operações de criptografia e descriptografia, consulte o administrador do proxy externo.

Respostas lentas também podem indicar que seu gerenciador de chaves externo não consegue lidar com o tráfego de solicitações atual. AWS KMS recomenda que seu gerenciador de chaves externo seja capaz de lidar com até 1800 solicitações de operações criptográficas por segundo. Se o gerenciador de chaves externas não conseguir lidar com a taxa de 1800 solicitações por segundo, considere solicitar uma redução na cota de solicitações de chaves do KMS em um armazenamento de chaves personalizado. As solicitações de operações de criptografia que usam as chaves do KMS em seu armazenamento de chaves externas se anteciparão à falha com uma exceção de controle de utilização, em vez de serem processadas e posteriormente rejeitadas pelo proxy de armazenamento de chaves externas ou pelo gerenciador de chaves externas.

Nome do grupo de dimensões: métricas de latência do proxy XKS

Dimensão	Descrição
CustomKeyStoreId	Valor para cada armazenamento de chaves externas.
KmsOperation	Valor de cada operação de AWS KMS API que gerou uma solicitação para o proxy XKS.
XksOperation	Valor para cada operação de API do proxy de armazenamento de chaves externas.
KeySpec	Valor para cada tipo de chave do KMS. A única especificação de chave compatível com chaves do KMS em um armazenamento de chaves externas é SYMMETRIC_DEFAULT.

Visualizando AWS KMS métricas

Você pode visualizar as AWS KMS métricas usando a AWS Management Console e a CloudWatch API da Amazon.

Para visualizar métricas usando o CloudWatch console

1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. Se necessário, altere a região. Na barra de navegação, selecione a região em que os seus recursos da AWS residem.
3. No painel de navegação, escolha Métricas, Todas as métricas.

4. Na guia Browse (Procurar), pesquise por KMS e escolha KMS.
5. Escolha o nome do grupo de dimensões da métrica que você deseja visualizar.

   Por exemplo, para a métrica SecondsUntilKeyMaterialExpiration, escolha Per-Key Metrics (Métricas por chave).
6. Para um gráfico do valor da métrica, escolha o nome da métrica e Add to graph (Adicionar ao gráfico). Para converter o gráfico de linhas em um valor, escolha Line (Linha) e, em seguida, escolha Number (Número).

Para visualizar métricas usando a CloudWatch API da Amazon

Para visualizar AWS KMS métricas usando a CloudWatch API, envie uma ListMetricssolicitação com Namespace set toAWS/KMS. O exemplo a seguir mostra como fazer isso com a 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": "ExternalKeyStoreThrottle",
            "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"
                }
            ]
        }
    ]
}
```

Criação de CloudWatch alarmes para monitorar chaves KMS

Você pode criar um CloudWatch alarme da Amazon com base em uma AWS KMS métrica. O alarme envia uma mensagem de e-mail quando um valor de métrica exceder um limite especificado na configuração do alarme. O alarme pode enviar a mensagem de e-mail para um tópico do Amazon Simple Notification Service (Amazon SNS) ou uma política do Amazon EC2 Auto Scaling. Para obter informações detalhadas sobre CloudWatch alarmes, consulte Usando CloudWatch alarmes da Amazon no Guia do usuário da Amazon CloudWatch

Criar um alarme para material de chave importado prestes a expirar

Você pode usar a `SecondsUntilKeyMaterialExpiration`métrica para criar um CloudWatch alarme que o notifique quando o material de chave importado em uma chave KMS está prestes a expirar.

Ao importar o material de chave para uma chave do KMS, é possível especificar opcionalmente uma data e hora quando o material de chave expira. Quando o material da chave expira, ele é AWS KMS excluído e a chave KMS fica inutilizável. Para usar a chave do KMS novamente, você deve reimportar o material de chave.

Para obter instruções, consulte Criação de um CloudWatch alarme para expiração do material chave importado.

Criar um alarme para o uso de chaves do KMS que estejam com exclusão pendente

Ao programar a exclusão de uma chave do KMS, o AWS KMS impõe um período de espera antes de excluir a chave do KMS. É possível usar o período de espera para garantir que não precisa mais da chave do KMS agora ou no futuro. Você também pode configurar um CloudWatch alarme para avisá-lo se uma pessoa ou aplicativo tentar usar a chave KMS em uma operação criptográfica durante o

período de espera. Se você receber uma notificação de um alarme desse tipo, poderá cancelar a exclusão da chave do KMS.

Para obter instruções, consulte Criar um alarme que detecte o uso de uma chave do KMS com exclusão pendente.

Criar um alarme para monitorar um armazenamento de chaves externas

Você pode criar CloudWatch alarmes com base nas métricas para armazenamentos de chaves externos e chaves KMS em armazenamentos de chaves externos.

Por exemplo, recomendamos que você defina um CloudWatch alarme para notificá-lo quando o certificado TLS do seu armazenamento de chaves externo estiver prestes a expirar (XksProxyCertificateDaysToExpire), quando você e quando o proxy do armazenamento de chaves externo relatar que suas instâncias externas do gerenciador de chaves estão em um estado degradado ou indisponível (). XksProxyHsmStates

Para obter instruções, consulte Monitorar um armazenamento de chaves externas.

Monitoramento com a Amazon EventBridge

Você pode usar a Amazon EventBridge (antiga Amazon CloudWatch Events) para alertá-lo sobre os seguintes eventos importantes no ciclo de vida de suas chaves KMS.

- O material de chave em uma chave do KMS foi alternado automaticamente.
- O material de chave importado em uma chave do KMS expirada.
- Uma chave do KMS que havia sido agendada para exclusão foi excluída.

AWS KMSse integra à Amazon EventBridge para notificá-lo sobre eventos importantes que afetam suas chaves KMS. Cada evento é representado em JSON (JavaScriptObject Notation) e inclui o nome do evento, a data e a hora em que o evento ocorreu e os afetados. Você pode coletar esses eventos e estabelecer regras que os roteiam a um ou mais destinos, como funções do AWS Lambda, tópicos do Amazon SNS, filas do Amazon SQS, transmissões no Amazon Kinesis Data Streams no destinos integrados.

Para obter mais informações sobre o uso EventBridge com outros tipos de eventos, incluindo aqueles emitidos AWS CloudTrail quando ele registra uma solicitação de API de leitura/gravação, consulte o Guia do usuário da Amazon EventBridge .

Os tópicos a seguir descrevem os EventBridge eventos AWS KMS gerados.

Alternância de CMKs do KMS

O AWS KMS é compatível com alternância automática do material de chave em chaves do KMS com criptografia simétrica. A alternância anual do material de chave é opcional para chaves gerenciadas pelo cliente. O material de chave para Chaves gerenciadas pela AWS é alternado automaticamente a cada ano.

Sempre que AWS KMS gira o material da chave, ele envia um `KMS CMK Rotation` evento para EventBridge. AWS KMSgera esse evento com base no melhor esforço.

A seguir há um exemplo deste 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"
  }
}
```

Expiração do material de chave importado do KMS

Ao importar o material de chave em uma chave do KMS, é possível especificar opcionalmente em que hora o material de chave expira. Quando o material chave expira, AWS KMS exclui o material chave e envia um `KMS Imported Key Material Expiration` evento correspondente para. EventBridge AWS KMSgera esse evento com base no melhor esforço.

A seguir há um exemplo deste 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"
  }
}
```

Exclusão da CMK do KMS

Ao programar a exclusão de uma chave do KMS, o AWS KMS impõe um período de espera antes de excluir a chave do KMS. Após o término do período de espera, AWS KMS exclui a chave KMS e envia um `KMS CMK Deletion` evento para. EventBridge AWS KMSgarante esse EventBridge evento. Devido a novas tentativas, ele pode gerar vários eventos dentro de alguns segundos que excluem a mesma chave do KMS.

A seguir há um exemplo deste 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"
  }
}
```

Criando AWS KMS recursos com AWS CloudFormation

AWS Key Management Service é integrado com AWS CloudFormation, um serviço que ajuda você a modelar e configurar seus AWS recursos para que você possa gastar menos tempo criando e

gerenciando seus recursos e infraestrutura. Você cria um modelo que descreve chaves e aliases do KMS, e o AWS CloudFormation provisiona e configura esses recursos para você. Para obter informações sobre AWS KMS suporte para CloudFormation, consulte a referência do tipo de recurso KMS no Guia do AWS CloudFormation usuário.

Ao usar AWS CloudFormation, você pode reutilizar seu modelo para configurar seus AWS KMS recursos de forma consistente e repetida. Descreva seus recursos uma vez e, em seguida, provisione os mesmos recursos repetidamente em várias Contas da AWS regiões.

Para provisionar e configurar recursos AWS KMS e outros AWS serviços, você deve entender AWS CloudFormation os modelos. Os modelos são arquivos de texto formatados em JSON ou YAML. Esses modelos descrevem os recursos que você deseja provisionar em suas AWS CloudFormation pilhas. Se você não estiver familiarizado com JSON ou YAML, você pode usar o AWS CloudFormation Designer para ajudá-lo a começar a usar modelos. AWS CloudFormation Para obter mais informações, consulte O que é o Designer AWS CloudFormation ? no Manual do usuário do AWS CloudFormation .

Regiões

AWS KMS CloudFormation os recursos são suportados em todas as regiões nas quais AWS CloudFormation há suporte.

AWS KMS recursos em AWS CloudFormation modelos

AWS KMS suporta os seguintes AWS CloudFormation recursos.

- O `AWS::KMS::Key`recurso especifica uma chave KMS em. AWS Key Management ServiceÉ possível utilizar esse recurso para criar chaves do KMS de criptografia simétrica, chaves do KMS assimétricas para criptografia ou assinatura e chaves do KMS HMAC simétricas. Você pode usar `AWS::KMS::Key` para criar chaves primárias multirregionais de todos os tipos compatíveis. Para replicar uma chave de réplica de várias regiões, use o recurso `AWS::KMS::ReplicaKey`.
- O `AWS::KMS::Alias` cria um alias e o associa a uma chave do KMS. A chave do KMS pode ser definida no modelo ou criada por outro mecanismo.
- O `AWS::KMS::ReplicaKey` cria uma chave de réplica de várias regiões. Para criar uma chave primária de várias regiões, use o recurso `AWS::KMS::Key`. Você não pode usar esse recurso para replicar chaves de várias regiões com material de chave importado. Para obter detalhes sobre chaves de várias regiões, consulteChaves multirregionais em AWS KMS.

> **Important**
>
> Se você alterar o valor da propriedade `KeyUsage`, `KeySpec` ou `MultiRegion` de uma chave do KMS existente, esta será programada para exclusão, e uma nova chave do KMS será criada com o valor especificado.
> Enquanto é programada para exclusão, a chave do KMS existente torna-se inutilizável.
> Se você não cancelar a exclusão programada da chave KMS existente fora do AWS CloudFormation, todos os dados criptografados sob a chave KMS existente se tornarão irrecuperáveis quando a chave KMS for excluída.

As chaves KMS que o modelo cria são recursos reais em seu Conta da AWS. Os diretores autorizados podem usar e gerenciar as chaves KMS que o modelo cria, usando o modelo, o AWS KMS console ou as AWS KMS APIs. Quando você exclui uma chave do KMS do modelo, ela é programada para exclusão usando um período de espera especificado antecipadamente.

Por exemplo, você pode usar um AWS CloudFormation modelo para criar uma chave KMS de teste com uma política de chave, especificação de chave, uso de chaves, aliases e tags de sua preferência. Você pode executá-lo em seu conjunto de teste, rever seus resultados e usar o modelo para programar a chave de teste para exclusão. Mais tarde, você pode executar o modelo novamente para criar uma chave de teste com as mesmas propriedades.

Ou você pode usar um AWS CloudFormation modelo para definir uma configuração de chave KMS específica que satisfaça suas regras de negócios e padrões de segurança. Em seguida, você pode usar esse modelo sempre que precisar para criar uma chave do KMS. Você não precisa se preocupar com chaves mal configuradas. Se a sua configuração preferencial for alterada, você poderá usar o modelo para atualizar suas chaves do KMS. Por exemplo, o modelo facilita a ativação programática da alternância automática de chaves em todas as chaves do KMS definidas por ele.

Para obter mais informações sobre AWS KMS recursos, incluindo exemplos, consulte a referência do tipo de recurso KMS no Guia do AWS CloudFormation usuário.

Saiba mais sobre AWS CloudFormation

Para saber mais sobre isso AWS CloudFormation, consulte os seguintes recursos:

- AWS CloudFormation
- AWS CloudFormation Guia do usuário
- AWS CloudFormation API Reference

- Guia do Usuário da Interface de Linha de Comando AWS CloudFormation

Excluir AWS KMS keys

Excluir uma AWS KMS key é um processo destrutivo e potencialmente perigoso. Essa ação exclui o material de chave e todos os metadados associados à chave do KMS e é irreversível. Depois que uma chave do KMS é excluída, não é mais possível descriptografar os dados que foram criptografados com ela, o que significa que os dados são irrecuperáveis. (As únicas exceções são chaves de réplica multirregionais e chaves assimétricas e as chaves do KMS de HMAC com material de chave importado.) Esse risco é significativo para chaves do KMS assimétricas usadas para criptografia, nas quais, sem aviso ou erro, os usuários podem continuar gerando textos cifrados com a chave pública que não podem ser descriptografados após que a chave privada for excluída do AWS KMS.

Só exclua uma chave do KMS quando você tiver certeza de que não vai mais precisar dela. Caso não tenha certeza, desabilite a chave do KMS em vez de excluí-la. Você poderá reabilitar a chave do KMS desabilitada e cancelar a exclusão agendada de uma chave do KMS, mas não poderá recuperar a chave do KMS excluída.

Apenas é possível agendar a exclusão de uma chave gerenciada pelo cliente. Não é possível excluir Chaves gerenciadas pela AWS ou Chaves pertencentes à AWS.

Antes de excluir uma chave do KMS, é recomendável saber como muitos textos cifrados foram criptografados com ela. O AWS KMS não armazena essas informações nem qualquer um dos textos cifrados. Para obter essas informações, você deve determinar o uso anterior de uma chave do KMS. Para obter ajuda, acesse Determinar a utilização anterior de uma chave do KMS.

O AWS KMS nunca exclui suas chaves do KMS, a menos que você as programe explicitamente para exclusão e o período de espera obrigatório expire.

No entanto, você pode optar por excluir uma chave do KMS devido a um ou mais dos seguintes motivos:

- Para concluir o ciclo de vida das chaves do KMS que não são mais necessárias
- Para evitar a sobrecarga de gerenciamento e os custos associados à manutenção de chaves do KMS não usadas
- Para reduzir o número de chaves do KMS que contam para a sua cota de recursos de chaves do KMS

> **Note**
>
> Se você fechar a sua Conta da AWS, as suas chaves do KMS se tornarão inacessíveis, e você não será mais cobrado por elas.

O AWS KMS registra uma entrada no log do AWS CloudTrail quando você programa a exclusão da chave do KMS e quando a chave do KMS é realmente excluída.

Para obter informações sobre como excluir chaves primárias e réplicas de várias regiões, consulte Excluir chaves de várias regiões.

Tópicos

- Sobre o período de espera
- Excluir chaves do KMS assimétricas
- Excluir chaves de várias Regiões
- Excluir chaves do KMS com material de chave importado
- Controlar o acesso à exclusão de chaves
- Programar e cancelar a exclusão de chaves
- Criar um alarme que detecte o uso de uma chave do KMS com exclusão pendente
- Determinar a utilização anterior de uma chave do KMS

Sobre o período de espera

Como é destrutivo e potencialmente perigoso excluir uma chave do KMS, o AWS KMS exige que você defina um período de espera de 7 a 30 dias. O período de espera padrão é de 30 dias.

No entanto, o período de espera real pode ser até 24 horas mais longo do que o programado. Para obter a data e a hora reais em que a chave KMS será excluída, use a DescribeKeyoperação. Ou, no console do AWS KMS, na página de detalhes da chave do KMS, na seção General configuration (Configuração geral), consulte a seçãoScheduled deletion date (Data de exclusão programada). Certifique-se de anotar o fuso horário.

Durante o período de espera, o status da chave do KMS e o status da chave é Pending deletion (Exclusão pendente).

- Uma chave do KMS com exclusão pendente não pode ser usada em nenhuma operação criptográfica.
- O AWS KMS não alterna o material de chave de chaves do KMS com exclusão pendente.

Após o término do período de espera, o AWS KMS excluirá a chave do KMS, seus aliases e todos os metadados do AWS KMS relacionados.

Programar a exclusão de uma chave do KMS pode não afetar imediatamente as chaves de dados criptografadas pela chave do KMS. Para obter detalhes, consulte Como as chaves do KMS inutilizáveis afetam as chaves de dados.

Use o período de espera para garantir que não vai precisar da chave do KMS agora nem no futuro. Você pode configurar um CloudWatch alarme da Amazon para avisá-lo se uma pessoa ou aplicativo tentar usar a chave KMS durante o período de espera. Para recuperar a chave do KMS, basta cancelar a exclusão de chaves antes do término do período de espera. Após o término do período de espera, não será possível cancelar a exclusão da chave, e o AWS KMS excluirá a chave do KMS.

Excluir chaves do KMS assimétricas

Usuários autorizados podem excluir chaves do KMS simétricas ou assimétricas. O procedimento para programar a exclusão dessas chaves do KMS é o mesmo para os dois tipos de chaves. Entretanto, como a chave pública de uma chave KMS assimétrica pode ser baixada e usada fora do AWS KMS, a operação apresenta riscos adicionais significativos, especialmente para chaves do KMS assimétricas usadas para criptografia (o uso da chave é `ENCRYPT_DECRYPT`).

- Ao programar a exclusão de uma chave do KMS, o estado dessa chave é alterado para Pending deletion (Exclusão pendente), e a chave do KMS não pode ser usada em operações de criptografia. No entanto, a programação de exclusão não tem efeito em chaves públicas fora do AWS KMS. Os usuários que têm a chave pública podem continuar a usá-la para criptografar mensagens. Eles não recebem nenhuma notificação sobre a alteração do estado da chave. A menos que a exclusão seja cancelada, o texto cifrado criado com a chave pública não pode ser descriptografado.
- Alarmes, logs e outras estratégias que detectam a tentativa de uso da chave do KMS com exclusão pendente não podem detectar o uso da chave pública fora do AWS KMS.
- Quando a chave do KMS é excluída, todas as ações do AWS KMS que envolvem essa chave falham. No entanto, os usuários que têm a chave pública podem continuar a usá-la para criptografar mensagens. Esses textos cifrados não podem ser descriptografados.

Se você precisar excluir uma chave KMS assimétrica com um uso de chave de`ENCRYPT_DECRYPT`, use suas entradas de CloudTrail registro para determinar se a chave pública foi baixada e compartilhada. Se for o caso, verifique se a chave pública não está sendo usada fora do AWS KMS. Depois, considere desabilitar a chave do KMS em vez de excluí-la.

O risco de excluir uma chave do KMS assimétrica é reduzido para chaves do KMS assimétricas com material de chave importado. Para obter detalhes, consulte Excluir uma chave do KMS com material de chave importado.

Excluir chaves de várias Regiões

Usuários autorizados podem programar a exclusão de chaves primárias e réplicas de várias regiões. No entanto, o AWS KMS não excluirá uma chave primária de várias regiões com chaves de réplica. Além disso, desde que sua chave primária exista, você pode recriar uma chave de réplica de várias regiões excluída. Para obter detalhes, consulte Excluir chaves de várias regiões.

Excluir chaves do KMS com material de chave importado

Os usuários autorizados podem programar a exclusão de chaves do KMS com material de chave importado. Essa ação exclui permanentemente a chave do KMS, seu material de chave e todos os metadados associados à chave do KMS.

Não é possível criar uma nova chave do KMS de criptografia simétrica que possa descriptografar os textos cifrados de uma chave de criptografia simétrica excluída com material de chave importado, mesmo que você tenha uma cópia desse material. No entanto, se você tiver o material de chave, poderá efetivamente recriar uma chave do KMS assimétrica ou uma chave do HMAC do KMS com material de chave importado. Para obter detalhes, consulte Excluir uma chave do KMS com material de chave importado.

Controlar o acesso à exclusão de chaves

Se você usar políticas do IAM para conceder permissões do AWS KMS, as identidades do IAM que têm acesso de administrador da AWS (`"Action": "*"`) ou acesso total do AWS KMS (`"Action": "kms:*"`) já têm permissão para agendar e cancelar a exclusão de chaves do KMS. Para permitir que os administradores de chaves programem e cancelem a exclusão de chaves na política de chaves, use o console do AWS KMS ou a API do AWS KMS.

Normalmente, apenas os administradores de chaves têm permissão para programar ou cancelar a exclusão da chave. Porém, você pode conceder essas permissões a outras identidades do IAM adicionando a permissão`kms:ScheduleKeyDeletion` e `kms:CancelKeyDeletion`

à política de chaves ou a uma política do IAM. Você também pode usar a chave de `kms:ScheduleKeyDeletionPendingWindowInDays`condição para restringir ainda mais os valores que os principais podem especificar no `PendingWindowInDays` parâmetro de uma ScheduleKeyDeletionsolicitação.

Permitir que os administradores de chaves programem e cancelem a exclusão de chaves (console)

Para conceder aos administradores de chaves permissão para agendar e cancelar a exclusão de chaves.

1. Faça login no AWS Management Console e abra o console do AWS Key Management Service (AWS KMS) em https://console.aws.amazon.com/kms.
2. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.
3. No painel de navegação, escolha Customer managed keys (Chaves gerenciadas pelo cliente).
4. Escolha o alias ou o ID de chave da chave do KMS cujas permissões você quer alterar.
5. Selecione a guia Key policy (Política de chaves).
6. A próxima etapa difere a visualização padrão da visualização de política de sua política de chaves. A visualização padrão estará disponível somente se você estiver usando a política de chaves padrão do console. Senão, apenas a visualização da política estará disponível.

   Quando a visualização padrão está disponível, o botão Switch to policy view (Alternar para visualização de política) ou Switch to default view (Alternar para visualização padrão) é exibido na guia Key policy (Política de chaves).

   - Na visualização padrão:
     - Em Key deletion (Exclusão de chaves), escolha Allow key administrators to delete this key (Permitir que administradores de chaves excluam esta chave).
   - Na visualização de política:
     a. Selecione a opção Editar.
     b. Na declaração de política para administradores de chave, adicione as permissões `kms:ScheduleKeyDeletion` e `kms:CancelKeyDeletion` ao 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. Escolha Salvar alterações.

Conceder aos administradores de chaves permissão para agendar e cancelar a exclusão de chaves (AWS CLI)

Você pode usar o AWS Command Line Interface para adicionar permissões para programar e cancelar a exclusão de chaves.

Para adicionar permissão para programar e cancelar a exclusão de chaves

1. Use o comando `aws kms get-key-policy` para recuperar a política de chaves existente e, em seguida, salve o documento de política em um arquivo.
2. Abra o documento de política no editor de texto de sua preferência. Na declaração de política para administradores de chave, adicione as permissões `kms:ScheduleKeyDeletion` e `kms:CancelKeyDeletion`. O exemplo a seguir mostra uma declaração de política com essas duas permissões:

```
{
  "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. Use o comando `aws kms put-key-policy` para aplicar a política de chaves à chave do KMS.

Programar e cancelar a exclusão de chaves

Os procedimentos a seguir descrevem como programar e cancelar a exclusão de AWS KMS keys (chaves do KMS) de região única no AWS KMS usando o AWS Management Console, a AWS CLI e o AWS SDK for Java.

Para obter informações sobre como programar a exclusão de chaves de várias regiões, consulteExcluir chaves de várias regiões.

> **Warning**
>
> Excluir uma chave do KMS é um processo destrutivo e potencialmente perigoso. Prossiga somente quando você tiver certeza de que não vai precisar mais usar a chave do KMS futuramente. Caso não tenha certeza, desabilite a chave do KMS em vez de excluí-la.

Para excluir uma chave do KMS, é preciso ter a respectiva permissão. Para obter informações sobre como conceder essas permissões aos administradores de chaves, consulte Controlar o acesso à exclusão de chaves. Também é possível usar a chave de condição `kms:ScheduleKeyDeletionPendingWindowInDays` para restringir ainda mais o período de espera, como impor um período mínimo de espera.

O AWS KMS registra uma entrada no log do AWS CloudTrail quando você programa a exclusão da chave do KMS e quando a chave do KMS é realmente excluída.

Programar e cancelar a exclusão de chaves (console)

No AWS Management Console, você pode programar e cancelar a exclusão de várias chaves do KMS ao mesmo tempo.

Para programar a exclusão de chaves

1. Faça login no AWS Management Console e abra o console do AWS Key Management Service (AWS KMS) em https://console.aws.amazon.com/kms.
2. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.
3. No painel de navegação, escolha Customer managed keys (Chaves gerenciadas pelo cliente).

   Não é possível agendar a exclusão de Chaves gerenciadas pela AWS ou Chaves pertencentes à AWS.
4. Marque a caixa de seleção ao lado da chave do KMS que você deseja excluir.
5. Escolha Key actions (Ações de chave), Schedule key deletion (Programar exclusão da chave).
6. Leia e considere o aviso e as informações sobre o cancelamento e a exclusão durante o período de espera. Se você decidir cancelar a exclusão, no final da página, selecione Cancel (Cancelar).
7. Para Waiting period (in days) (Período de espera (em dias)), digite um número de dias entre 7 e 30.
8. Revise as chaves do KMS que você está excluindo.
9. Marque a caixa de seleção ao lado de Confirm you want to schedule this key for deletion in ***<number of days>*** days. (Confirme se você deseja agendar essa chave para exclusão em <número de dias> dias).
10. Escolha Schedule deletion.

O status da chave muda para Pending deletion (Exclusão pendente).

Para cancelar a exclusão de chaves

1. Abra o console do AWS KMS em https://console.aws.amazon.com/kms.
2. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.
3. No painel de navegação, escolha Customer managed keys (Chaves gerenciadas pelo cliente).

4. Marque a caixa de seleção ao lado da chave do KMS que você deseja recuperar.
5. Escolha Key actions (Ações de chave), Cancel key deletion (Cancelar exclusão da chave).

O status da chave muda de Pending deletion (Exclusão pendente) para Disabled (Desabilitada). Para usar a chave, você deve habilitá-la.

Programar e cancelar a exclusão de chaves (AWS CLI)

Use o comando `aws kms schedule-key-deletion` para agendar a exclusão de chaves de uma chave gerenciada pelo cliente, conforme mostrado no exemplo a seguir.

Não é possível agendar a exclusão de uma Chave gerenciada pela AWS ou Chave pertencente à AWS.

```
$ aws kms schedule-key-deletion --key-id 1234abcd-12ab-34cd-56ef-1234567890ab --
pending-window-in-days 10
```

Quando usada com êxito, a AWS CLI retorna o resultado como a saída mostrada no exemplo a seguir:

```
{
    "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "DeletionDate": 1598304792.0,
    "KeyState": "PendingDeletion",
    "PendingWindowInDays": 10
}
```

Use o comando `aws kms cancel-key-deletion` para cancelar a exclusão de chaves da AWS CLI, conforme mostrado no exemplo a seguir.

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

Quando usada com êxito, a AWS CLI retorna o resultado como a saída mostrada no exemplo a seguir:

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

```
}
```

O status da chave do KMS muda de Pending Deletion (Exclusão pendente) para Disabled (Desabilitada). Para usar a chave, você deve habilitá-la.

Programar e cancelar a exclusão de chaves (AWS SDK for Java)

O exemplo a seguir demonstra como agendar a exclusão de uma chave gerenciada pelo cliente com o AWS SDK for Java. Esse exemplo requer que você tenha instanciado anteriormente um `AWSKMSClient` como `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);
```

O exemplo a seguir demonstra como cancelar uma chave para exclusão com o AWS SDK for Java. Esse exemplo requer que você tenha instanciado anteriormente um `AWSKMSClient` como `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);
```

O status da chave do KMS muda de Pending Deletion (Exclusão pendente) para Disabled (Desabilitada). Para usar a chave, você deve habilitá-la.

Criar um alarme que detecte o uso de uma chave do KMS com exclusão pendente

Você pode combinar os recursos do AWS CloudTrail Amazon CloudWatch Logs e do Amazon Simple Notification Service (Amazon SNS) para criar um alarme da CloudWatch Amazon que notifica você

quando alguém em sua conta tenta usar uma chave KMS que está pendente de exclusão. Se você receber essa notificação, convém cancelar a exclusão da chave do KMS e reconsiderar sua decisão de excluí-la.

Os procedimentos a seguir criam um alarme que notifica você sempre que a mensagem de erro *Key ARN* `is pending deletion` "" for gravada em seus arquivos de CloudTrail log. Essa mensagem de erro indica que uma pessoa ou aplicação tentou usar a chave do KMS em uma operação criptográfica. Como a notificação está vinculada à mensagem de erro, ela não é acionada quando você usa operações da API que são permitidas em chaves do KMS com exclusão pendente, como `ListKeys`, `CancelKeyDeletion` e `PutKeyPolicy`. Para ver uma lista das operações de API do AWS KMS que geram essa mensagem de erro, consulte Principais estados das AWS KMS chaves.

O e-mail de notificação recebido não indicará a chave do KMS ou a operação criptográfica. É possível encontrar essas informações em seu log do CloudTrail. Em vez disso, o e-mail informa que o estado do alarme mudou de OK para Alarme. Para obter mais informações sobre CloudWatch alarmes e mudanças de estado, consulte Usando CloudWatch alarmes da Amazon no Guia CloudWatch do usuário da Amazon.

> **Warning**
>
> Esse CloudWatch alarme da Amazon não pode detectar o uso da chave pública de uma chave KMS assimétrica fora do. AWS KMS Para obter detalhes sobre os riscos especiais de exclusão de chaves do KMS assimétricas usadas para a criptografia de chave pública, incluindo a criação de textos cifrados que não podem ser descriptografados, consulte Excluir chaves do KMS assimétricas.

Tópicos

- Requisitos para um CloudWatch alarme
- Criando o CloudWatch alarme

Requisitos para um CloudWatch alarme

Antes de criar um CloudWatch alarme, você deve criar uma AWS CloudTrail trilha e configurá-la CloudTrail para entregar arquivos de CloudTrail log ao Amazon CloudWatch Logs. Você também precisa de um tópico do Amazon SNS para a notificação do alarme.

- Crie uma trilha do CloudTrail.

  CloudTrail é ativado automaticamente Conta da AWS quando você cria a conta. No entanto, para obter um registro contínuo de eventos em sua conta, incluindo eventos do AWS KMS, crie uma trilha.

- Configure CloudTrail para entregar seus arquivos de log CloudWatch Logs.

  Configure a entrega de seus arquivos de CloudTrail log para o CloudWatch Logs. Isso permite que o CloudWatch Logs monitore os registros de solicitações de AWS KMS API que tentam usar uma chave KMS que está pendente de exclusão.

- Crie um tópico do Amazon SNS.

  Quando seu alarme é acionado, ele notifica você enviando uma mensagem de e-mail para um endereço de e-mail em um tópico do Amazon Simple Notification Service (Amazon SNS).

Criando o CloudWatch alarme

Neste procedimento, você cria um filtro métrico de grupo de CloudWatch registros que localiza instâncias da exceção de exclusão pendente. Em seguida, você cria um CloudWatch alarme com base na métrica do grupo de registros. Para obter informações sobre filtros métricos de grupos de registros, consulte Criação de métricas a partir de eventos de log usando filtros no Guia do usuário do Amazon CloudWatch Logs.

1. Crie um filtro CloudWatch métrico que analise os CloudTrail registros.

   Siga as instruções em Criar um filtro de métrica para um grupo de logs usando os seguintes valores obrigatórios. Para outros campos, aceite os valores padrão e forneça os nomes conforme solicitado.

Campo	Valor
Padrão de filtro	`{ $.eventSource = kms* && $.errorMessage = "* is pending deletion."}`
Valor da métrica	1

2. Crie um CloudWatch alarme com base no filtro métrico que você criou na Etapa 1.

Siga as instruções em Criação de um CloudWatch alarme com base em um filtro métrico de grupo de registros usando os seguintes valores obrigatórios. Para outros campos, aceite os valores padrão e forneça os nomes conforme solicitado.

Campo	Valor
Filtro de métrica	O nome do filtro de métrica que você criou na Etapa 1.
Tipo de limite	Estático
Condições	Sempre que o *nome da métrica* for maior que 1
Pontos de dados para o alarme	1 de 1
Tratamento de dados ausentes	Treat missing data as good (not breaching threshold) (Tratar dados ausentes como bons [sem violar o limite])

Depois de concluir esse procedimento, você receberá uma notificação sempre que o novo CloudWatch alarme entrar no `ALARM` estado. Se você receber uma notificação desse alarme, talvez isso signifique que uma chave do KMS programada para exclusão ainda seja necessária para criptografar ou descriptografar dados. Nesse caso, cancele a exclusão da chave do KMS e reconsidere sua decisão de excluí-la.

Determinar a utilização anterior de uma chave do KMS

Antes de excluir uma chave do KMS, convém saber como muitos textos cifrados foram criptografados com ela. O AWS KMS não armazena essas informações nem qualquer um dos textos cifrados. Saber como uma chave do KMS foi utilizada no passado pode ajudar você a decidir se ela será ou não necessária no futuro. Este tópico sugere várias estratégias que podem ajudar você a determinar o uso anterior de uma chave do KMS.

> **Warning**
>
> Essas estratégias para determinar o uso passado e atual têm efeito somente para usuários da AWS e operações do AWS KMS. Elas não podem detectar o uso da chave pública de uma chave do KMS assimétrica fora do AWS KMS. Para obter detalhes sobre os riscos especiais de exclusão de chaves do KMS assimétricas usadas para a criptografia de chave pública, incluindo a criação de textos cifrados que não podem ser descriptografados, consulte Excluir chaves do KMS assimétricas.

Tópicos

- Examinar as permissões da chave do KMS para determinar o escopo da utilização em potencial
- Examinar os logs do AWS CloudTrail para determinar a utilização real

Examinar as permissões da chave do KMS para determinar o escopo da utilização em potencial

Determinar quem ou o quê tem acesso no momento a uma chave do KMS pode ajudar a determinar o quão amplamente ela foi usada e se ainda é necessária. Para saber como determinar quem ou o quê tem acesso no momento a uma chave do KMS, acesse Determinar acesso a AWS KMS keys.

Examinar os logs do AWS CloudTrail para determinar a utilização real

Talvez seja possível usar o histórico de uso de uma chave do KMS para ajudar a determinar se você tem textos cifrados em uma chave do KMS específica.

Toda a atividade da API do AWS KMS é registrada em arquivos de log do AWS CloudTrail. Se você criou uma CloudTrail trilha na região em que sua chave KMS está localizada, você pode examinar seus arquivos de CloudTrail log para ver um histórico de todas as atividades de AWS KMS API de uma chave KMS específica. Se você não tiver uma trilha, ainda poderá ver eventos recentes no Histórico de eventos do CloudTrail . Para obter detalhes sobre como AWS KMS usar CloudTrail, consulteRegistrando chamadas de AWS KMS API com AWS CloudTrail.

Os exemplos a seguir mostram entradas de CloudTrail registro que são geradas quando uma chave KMS é usada para proteger um objeto armazenado no Amazon Simple Storage Service (Amazon S3). Neste exemplo, o objeto é carregado no Amazon S3 usando Proteção de dados usando criptografia no lado do servidor com chaves do KMS (SSE-KMS). Ao carregar um objeto

no Amazon S3 com SSE-KMS, você especifica a chave do KMS a ser usada para proteger esse objeto. O Amazon S3 usa a AWS KMS GenerateDataKeyoperação para solicitar uma chave de dados exclusiva para o objeto, e esse evento de solicitação é registrado CloudTrail com uma entrada semelhante à seguinte:

```
{
  "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"
}
```

Mais tarde, quando você baixar esse objeto do Amazon S3, o Amazon S3 enviará uma solicitação `Decrypt` ao AWS KMS para descriptografar a chave de dados do objeto usando a chave do KMS especificada. Ao fazer isso, seus arquivos de CloudTrail log incluem uma entrada semelhante à seguinte:

```
{
  "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"
}
```

Todas as atividades de API do AWS KMS são registradas pelo CloudTrail. Ao avaliar essas entradas de log, talvez você possa determinar a utilização anterior de uma chave do KMS específica, e isso pode ajudar a determinar se você deseja ou não excluí-la.

Para ver mais exemplos de como a atividade da AWS KMS API aparece em seus arquivos de CloudTrail log, acesseRegistrando chamadas de AWS KMS API com AWS CloudTrail. Para obter mais informações sobre, CloudTrail acesse o Guia AWS CloudTrail do usuário.

Principais estados das AWS KMS chaves

E AWS KMS key sempre tem um estado chave. As operações na chave do KMS e em seu ambiente podem alterar esse estado de chave, de forma transitória ou até que outra operação altere seu estado de chave.

A tabela nesta seção mostra como os estados principais afetam as chamadas para operações de AWS KMS API. Como resultado de seu estado de chave, espera-se que uma operação em uma chave do KMS tenha êxito (#), apresente falhas (X) ou tenha êxito somente em certas condições (?). O resultado muitas vezes é diferente para chaves do KMS com material de chave importado.

Essa tabela inclui apenas as operações de API que usam uma chave do KMS existente. Outras operações, como CreateKeye ListKeys, são omitidas.

Tópicos

- Estados de chave e tipos de chaves do KMS

- Tabela de estados de chave

Estados de chave e tipos de chaves do KMS

O tipo da chave do KMS determina os estados de chave que ela pode ter.

- Todas as chaves do KMS podem estar nos estados `Enabled`, `Disabled` e `PendingDeletion`.
- A maioria das chaves do KMS é criada no estado `Enabled`. Chaves com material de chave importado são criadas no estado `PendingImport`.
- O estado `PendingImport` aplica-se somente a chaves do KMS com material de chave importado.
- O estado `Unavailable` aplica-se somente a uma chave do KMS em um armazenamento de chaves personalizado. Uma chave KMS em um armazenamento de AWS CloudHSM chaves ocorre `Unavailable` quando o armazenamento de chaves personalizado é intencionalmente desconectado de seu cluster. AWS CloudHSM Uma chave do KMS em um armazenamento de chaves externas está `Unavailable` quando o armazenamento de chaves personalizado foi desconectado do proxy de armazenamento de chaves externas intencionalmente. É possível visualizar e gerenciar chaves do KMS indisponíveis, mas não é possível usá-las em operações de criptografia.

  O estado da chave de uma chave do KMS em um armazenamento de chaves personalizado não é afetado pelas alterações em sua chave de reserva. Uma chave KMS em um armazenamento de AWS CloudHSM chaves não é afetada pelas alterações no material de chaves associado no AWS CloudHSM cluster. Uma chave do KMS em um armazenamento de chaves externas não é afetada por alterações em sua chave externa em um gerenciador de chaves externas. Se a chave de reserva estiver desabilitada ou excluída, o estado da chave do KMS não será alterado, mas as operações de criptografia que usam a chave do KMS apresentarão falha.
- Os estados de chave `Creating`, `Updating` e`PendingReplicaDeletion` aplicam-se somente a chaves de várias regiões.
  - Uma chave de réplica de várias regiões está no estado de chave `Creating` enquanto ela está sendo criada. Esse processo ainda pode estar em andamento quando a ReplicateKeyoperação for concluída. Quando o processo de replicação estiver concluído, a chave de réplica estará no estado `Enabled` ou `PendingImport`.
  - Chaves de várias regiões estão no estado de chave `Updating` transitório enquanto a região primária está sendo atualizada. Esse processo ainda pode estar em andamento quando a UpdatePrimaryRegionoperação for concluída. Quando o processo de atualização estiver concluído, as chaves primária e de réplica retomarão o estado de chave `Enabled`.

- Quando você programar a exclusão de uma chave primária de várias regiões contendo chaves de réplica, essa chave primária estará no estado `PendingReplicaDeletion` até que todas as suas chaves de réplica sejam excluídas. Seu estado de chave muda para `PendingDeletion`. Para obter detalhes, consulte Excluir chaves de várias regiões.

Tabela de estados de chave

A tabela a seguir mostra como o estado de uma chave do KMS afeta operações do AWS KMS .

Descrições de notas de rodapé numeradas ([n]) estão no final deste tópico.

> **Note**
>
> Talvez seja necessário rolar horizontalmente ou verticalmente para ver todos os dados nessa tabela.

API	Habilitado	Desabilitado	Exclusão pendente Exclusão pendente de réplica	Importação pendente	Unavailable (Indisponível)	Criando	Atualizando
CancelKeyDeletion	✗ [4]	✗ [4]	✓	✗ [4]	✗ [4], [13]	✗ [4]	✗ [4]
CreateAlias	✓	✓	✗ [3]	✓	✓	✓	✓
CreateGrant	✓	✗ [1]	✗ [2] ou [3]	✗ [5]	✓	✗ [14]	✓

API	Habilitado	Desabilitado	Exclusão pendente Exclusão pendente de réplica	Importação pendente	Unavailable (Indisponível)	Criando	Atualizando
Decrypt	✓	⊗ [1]	⊗ [2] ou [3]	⊗ [5]	⊗ [11]	⊗ [14]	✓
DeleteAlias	✓	✓	✓	✓	✓	✓	✓
DeleteImportedKeyMaterial	✓ [9]	✓ [9]	✓ [9]	✓ (sem efeito)	N/D	⊗ [14]	⊗ [15]
DescribeKey	✓	✓	✓	✓	✓	✓	✓
DisableKey	✓	✓	⊗ [3]	⊗ [5]	✓ [12]	⊗ [14]	⊗ [15]
DisableKeyRotation	? [7]	⊗ [1] ou [7]	⊗ [3] ou [7]	⊗ [6]	⊗ [7]	⊗ [14]	? [7]
EnableKey	✓	✓	⊗ [3]	⊗ [5]	✓ [12]	⊗ [14]	⊗ [15]

API	Habilitado	Desabilitado	Exclusão pendente Exclusão pendente de réplica	Importação pendente	Unavailable (Indisponível)	Criando	Atualizando
EnableKeyRotation	 [7]	 [1] ou [7]	 [3] ou [7]	 [6]	 [7]	 [14]	 [7]
Encrypt		 [1]	 [2] ou [3]	 [5]	 [11]	 [14]	
GenerateDataKey		 [1]	 [2] ou [3]	 [5]	 [11]	 [14]	
GenerateDataKeyPair		 [1]	 [2] ou [3]	 [5]	 [11]	 [14]	
GenerateDataKeyPairWithoutPlaintext		 [1]	 [2] ou [3]	 [5]	 [11]	 [14]	
GenerateDataKeyWithoutPlaintext		 [1]	 [2] ou [3]	 [5]	 [11]	 [14]	

API	Habilitado	Desabilitado	Exclusão pendente Exclusão pendente de réplica	Importação pendente	Unavailable (Indisponível)	Criando	Atualizando
GenerateMac	✓	⊗ [1]	⊗ [2] ou [3]	N/D	N/D	⊗ [14]	✓
GetKeyPolicy	✓	✓	✓	✓	✓	✓	✓
GetKeyRotationStatus	? [7]	? [7]	? [7]	⊗ [6]	⊗ [7]	? [7]	? [7]
GetParametersForImport	? [9]	? [9]	⊗ [8] ou [9]	✓	⊗ [9]	⊗ [14]	⊗ [15]
GetPublicKey	✓	⊗ [1]	⊗ [2] ou [3]	N/D	N/D	⊗ [14]	✓
ImportKeyMaterial	? [9]	? [9]	⊗ [8] ou [9]	✓	⊗ [9]	⊗ [14]	✓
ListAliases	✓	✓	✓	✓	✓	✓	✓
ListGrants	✓	✓	✓	✓	✓	✓	✓

API	Habilitado	Desabilitado	Exclusão pendente Exclusão pendente de réplica	Importação pendente	Unavailable (Indisponível)	Criando	Atualizando
ListKeyPolicies	✓	✓	✓	✓	✓	✓	✓
ListKeyRotations	? [7]	? [7]	? [7]	⊗ [6]	⊗ [7]	? [7]	? [7]
ListResourceTags	✓	✓	✓	✓	✓	✓	✓
PutKeyPolicy	✓	✓	✓	✓	✓	✓	✓
ReEncrypt	✓	⊗ [1]	⊗ [2] ou [3]	⊗ [5]	⊗ [11]	⊗ [14]	✓
ReplicateKey	✓	⊗ [1]	⊗ [2] ou [3]	⊗ [5]	N/D	⊗ [14]	⊗ [15]
RetireGrant	✓	✓	✓	✓	✓	✓	✓
RevokeGrant	✓	✓	✓	✓	✓	✓	✓

API	Habilitado	Desabilitado	Exclusão pendente Exclusão pendente de réplica	Importação pendente	Unavailable (Indisponível)	Criando	Atualizando
RotateKeyOnDemand	 [7]	 [1] ou [7]	 [3] ou [7]	 [6]	 [7]	 [14]	 [7]
ScheduleKeyDeletion			 [3]				 [15]
Sign		 [1]	 [2] ou [3]	N/D	N/D	 [14]	
TagResource			 [3]				
UntagResource			 [3]				
UpdateAlias			 [10]				
UpdateKeyDescription			 [3]				

API	Habilitado	Desabilitado	Exclusão pendente Exclusão pendente de réplica	Importação pendente	Unavailable (Indisponível)	Criando	Atualizando
UpdatePrimaryRegion	✓	⊗ [1]	⊗ [2] ou [3]	⊗ [5]	N/D	⊗ [14]	✓
Verificar	✓	⊗ [1]	⊗ [2] ou [3]	N/D	N/D	⊗ [14]	✓
VerifyMac	✓	⊗ [1]	⊗ [2] ou [3]	N/D	N/D	⊗ [14]	✓

Detalhes da tabela

- [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 a chave do KMS tiver material de chave importado ou estiver em um armazenamento de chaves personalizado: `UnsupportedOperationException`.

- [8] Se a chave do KMS tiver material de chave importado: `KMSInvalidStateException`
- [9] Se a chave do KMS não puder ter ou não tiver material de chave importado: `UnsupportedOperationException`.
- [10] Se a exclusão da chave do KMS de origem está pendente, o comando foi bem-sucedido. Se a exclusão da chave do KMS de destino está pendente, o comando falha com o erro: `KMSInvalidStateException : <key ARN> is pending deletion.`
- [11] `KMSInvalidStateException: <key ARN> is unavailable.` Não é possível executar essa operação em uma chave do KMS indisponível.
- [12] A operação é bem-sucedida, mas o estado da chave do KMS não muda até que ela se torne disponível.
- [13] Enquanto a exclusão de uma chave do KMS em um armazenamento de chaves personalizado estiver pendente, seu estado de chave permanecerá `PendingDeletion`, mesmo que a chave do KMS se torne indisponível. Isso permite que você cancele a exclusão da chave do KMS a qualquer momento durante o período de espera.
- [14] `KMSInvalidStateException: <key ARN> is creating.` AWS KMS lança essa exceção enquanto replica uma chave multirregional (). `ReplicateKey`
- [15] `KMSInvalidStateException: <key ARN> is updating.` AWS KMS lança essa exceção enquanto atualiza a região primária de uma chave multirregional ()`UpdatePrimaryRegion`.

Autenticação e controle de acesso para o AWS KMS

Para usar AWS KMS, você deve ter credenciais que a AWS possa usar para autenticar suas solicitações. As credenciais devem incluir permissões para acessar recursos da AWS: AWS KMS keys e aliases. Nenhuma entidade principal da AWS tem permissão para uma chave do KMS, a menos que essa permissão seja fornecida explicitamente e nunca seja negada. Não há permissão implícita ou automática para usar ou gerenciar uma chave do KMS.

A principal maneira de gerenciar o acesso aos seus recursos do AWS KMS é por meio de políticas. Políticas são documentos que descrevem quais entidades principais podem acessar recursos específicos. As políticas anexadas a uma identidade do IAM são chamadas de políticas baseadas em identidade (ou políticas do IAM), e as políticas anexadas a outros tipos de recurso são conhecidas como políticas baseadas em recursos. As políticas de recursos do AWS KMS para chaves do KMS são chamadas de políticas de chaves. Todas as chaves do KMS têm uma política de chaves.

Para controlar o acesso aos seus aliases do AWS KMS, use políticas do IAM. Para permitir que as entidades criem aliases, você deve fornecer a permissão para o alias em uma política do IAM e permissão para a chave em uma política de chaves. Para obter detalhes, consulte Controlar o acesso a aliases.

Para controlar o acesso às suas chaves do KMS, você pode usar os seguintes mecanismos de política.

- Política de chaves: cada chave do KMS tem uma política de chave. Esse é o mecanismo principal para controlar o acesso a uma chave do KMS. Você pode usar apenas a política de chaves para controlar o acesso, ou seja, o escopo completo de acesso à chave do KMS é definido em um único documento (a política de chaves). Para mais informações sobre como usar políticas de chaves, consulte Políticas de chaves.
- Políticas do IAM: você pode usar políticas do IAM combinadas com a política de chaves e concessões para controlar o acesso a uma chave do KMS. Com esse controle de acesso, você pode gerenciar todas as permissões para suas identidades do IAM no IAM. Para usar uma política do IAM para permitir o acesso a uma chave do KMS, a política de chaves deve explicitamente permitir isso. Para mais informações sobre como usar políticas do IAM, consulte Políticas do IAM.
- Concessões: você pode usar concessões combinadas com a política de chaves e políticas do IAM para permitir o acesso a uma chave do KMS. Controlar o acesso dessa maneira possibilita permitir o acesso à chave do KMS na política de chaves e permitir que as identidades deleguem o

acesso para outras pessoas. Para obter mais informações sobre como usar concessões, consulte Concessões no AWS KMS.

As chaves do KMS pertencem à conta da AWS na qual foram criadas. No entanto, nenhuma identidade ou entidade principal, incluindo o usuário raiz da conta da AWS, tem permissão para usar ou gerenciar uma chave do KMS, a menos que essa permissão seja explicitamente fornecida em uma política de chave, política do IAM ou concessão. A identidade do IAM que cria uma chave do KMS não é considerada a proprietária da chave e não recebe permissão automática para usar ou gerenciar a chave do KMS criada. Como qualquer outra identidade, o criador da chave precisa obter permissão por meio de uma política de chaves, política do IAM ou concessão. No entanto, as identidades que têm a permissão `kms:CreateKey` podem definir a política de chave inicial e conceder a si mesmas permissões para usar ou gerenciar a chave.

Os tópicos a seguir fornecem detalhes sobre como é possível usar o AWS Identity and Access Management (IAM) e permissões do AWS KMS para ajudar a proteger seus recursos controlando quem pode acessá-los.

Tópicos

- Conceitos em controle de acesso do AWS KMS
- Políticas-chave em AWS KMS
- Usando políticas do IAM com AWS KMS
- Concessões no AWS KMS
- Conectar-se ao AWS KMS por meio de um endpoint da VPC
- Chaves de condição para AWS KMS
- ABAC para AWS KMS
- Permitir que usuários de outras contas usem uma chave do KMS
- Usar perfis vinculados ao serviço do AWS KMS
- Usar TLS pós-quântico híbrido com o AWS KMS
- Determinar acesso a AWS KMS keys
- AWS KMS permissões
- Testar suas permissões

Conceitos em controle de acesso do AWS KMS

Aprenda os conceitos usados nas discussões sobre controle de acesso em AWS KMS.

Tópicos

- Autenticação
- Autorização
- Autenticando com identidades
- Como gerenciar acesso usando políticas
- Atributos AWS KMS

Autenticação

A autenticação é o processo de verificação da identidade. Para enviar uma solicitação ao AWS KMS, você deve fazer login na AWS usando suas credenciais da AWS.

Autorização

A autorização fornece permissões para enviar solicitações para criar, gerenciar ou usar recursos do AWS KMS. Por exemplo, você deve ter autorização para usar uma chave do KMS em uma operação criptográfica.

Para controlar o acesso aos recursos do AWS KMS, use políticas de chaves, políticas do IAM e concessões. Cada chave do KMS deve ter uma política de chaves. Se a política de chaves permitir, também é possível usar concessões e políticas do IAM para conceder às entidades principais acesso à chave do KMS. Para detalhar a autorização, você pode usar chaves de condição que permitem ou negam acesso somente quando uma solicitação ou recurso atende às condições especificadas. Também é possível permitir o acesso às entidades principais em que confia em outras Contas da AWS.

Autenticando com identidades

A autenticação é a forma como você faz login na AWS usando suas credenciais de identidade. É necessário ser autenticado (fazer login na AWS) como o usuário raiz da Usuário raiz da conta da AWS, como usuário do IAM ou assumindo um perfil do IAM.

É possível fazer login na AWS como uma identidade federada usando credenciais fornecidas por uma fonte de identidades. AWS IAM Identity Center Os usuários do IAM Identity Center, a

autenticação única da empresa e as suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como uma identidade federada, o administrador já configurou anteriormente a federação de identidades utilizando perfis do IAM. Quando você acessa a AWS usando a federação, está indiretamente assumindo um perfil.

É possível fazer login no AWS Management Console ou no de acesso da AWS dependendo do tipo de usuário que você é. Para obter mais informações sobre como fazer login na AWS, consulte Conta da AWS Como fazer login na sua no Início de Sessão da AWS Guia do usuário.

Se você acessar a AWS programaticamente, a AWS fornecerá um kit de desenvolvimento de software (SDK) e uma interface de linha de comandos (CLI) para você assinar criptograficamente as solicitações usando as suas credenciais. Se você não utilizar as ferramentas da AWS, deverá assinar as solicitações por conta própria. Para obter mais informações sobre como usar o método recomendado para assinar solicitações por conta própria, consulte Assinar solicitações de API da AWS no Guia do usuário do IAM.

Independentemente do método de autenticação usado, também pode ser exigido que você forneça mais informações de segurança. Por exemplo, a AWS recomenda o uso da autenticação multifator (MFA) para aumentar a segurança de sua conta. Para saber mais, consulte Autenticação multifator no Guia do usuário do AWS IAM Identity Center e Usar a autenticação multifator (MFA) naAWS no Guia do usuário do IAM.

Usuário raiz da Conta da AWS

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos os atributos e Serviços da AWS na conta. Essa identidade, denominada usuário raiz da Conta da AWS, e é acessada por login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não utilizar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele puder executar. Para obter a lista completa das tarefas que exigem login como usuário raiz, consulte Tarefas que exigem credenciais de usuário raiz no Guia do usuário do IAM.

Identidade federada

Como prática recomendada, exija que os usuários, inclusive os que precisam de acesso de administrador, usem a federação com um provedor de identidades para acessar Serviços da AWS usando credenciais temporárias.

Identidade federada é um usuário de seu diretório de usuários corporativos, um provedor de identidades da web AWS Directory Service, o , o diretório do Centro de Identidade ou qualquer

usuário que acesse os Serviços da AWS usando credenciais fornecidas por meio de uma fonte de identidade. Quando as identidades federadas acessam Contas da AWS, elas assumem perfis que fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos usar o .AWS IAM Identity Center É possível criar usuários e grupos no Centro de Identidade do IAM ou se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todas as suas Contas da AWS e aplicações. Para obter mais informações sobre o IAM Identity Center, consulte "O que é o IAM Identity Center?" no Guia do usuário do AWS IAM Identity Center.

Usuários e grupos do IAM

Um usuário do IAM é uma identidade dentro da Conta da AWS que tem permissões específicas para uma única pessoa ou aplicação. Sempre que possível, recomendamos contar com credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de utilização específicos que exijam credenciais de longo prazo com usuários do IAM, recomendamos alternar as chaves de acesso. Para obter mais informações, consulte Alterne as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo no Guia do usuário do IAM.

Um grupo do IAM é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível utilizar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, é possível ter um grupo chamado IAMAdmins e atribuir a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Quando criar um usuário do IAM (em vez de um perfil) no Guia do usuário do IAM.

Perfis do IAM

Um perfil do IAM é uma identidade dentro da Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. É possível assumir temporariamente um perfil do IAM no AWS Management Console alternando perfis. É possível assumir um perfil chamando uma operação de API da AWS CLI ou da AWS, ou usando um

URL personalizado. Para obter mais informações sobre métodos para o uso de perfis, consulte Usar perfis do IAM no Guia do usuário do IAM.

Perfis do IAM com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, é possível criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter mais informações sobre perfis para federação, consulte Criar uma função para um provedor de identidade de terceiros no Guia do usuário do IAM. Se você usar o IAM Identity Center, deverá configurar um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o Centro de identidade do IAM correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de permissões no Guia do usuário do AWS IAM Identity Center.
- Permissões temporárias para usuários do IAM: um usuário ou um perfil do IAM pode assumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas: é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, alguns Serviços da AWS permitem que você anexe uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Como os perfis do IAM diferem das políticas baseadas em recurso no Guia do usuário do IAM.
- Acesso entre serviços: alguns Serviços da AWS usam atributos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicações no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões do principal de chamada, usando um perfil de serviço ou uma função vinculada ao serviço.
  - Encaminhamento de sessões de acesso (FAS): qualquer pessoa que utilizar uma função ou usuário do IAM para realizar ações na AWS é considerada uma entidade principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O recurso FAS utiliza as permissões da entidade principal que chama um AWS service (Serviço da AWS), combinadas às permissões do AWS service (Serviço da AWS) solicitante, para realizar solicitações para serviços downstream. As solicitações de FAS só são feitas quando um serviço recebe uma solicitação que exige interações com outros Serviços da AWS ou com recursos para serem concluídas. Nesse caso, você precisa ter permissões para executar ambas as ações.

Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.

- Perfil de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do usuário do IAM.
- Perfil vinculado a serviço: um perfil vinculado a serviço é um tipo de perfil de serviço vinculado a um AWS service (Serviço da AWS). O serviço pode assumir o perfil de executar uma ação em seu nome. Os perfis vinculados ao serviço aparecem em sua Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para perfis vinculados ao serviço.

- Aplicações em execução no Amazon EC2: é possível usar um perfil do IAM para gerenciar credenciais temporárias para aplicações em execução em uma instância do EC2 e fazer solicitações da AWS CLI ou da AWS API. É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir um perfil da AWS a uma instância do EC2 e disponibilizá-la para todas as suas aplicações, crie um perfil de instância que esteja anexado a ela. Um perfil de instância contém o perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Usar um perfil do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Para saber se deseja usar os perfis do IAM, consulte Quando criar uma função do IAM (em vez de um usuário) no Guia do usuário do IAM.

Como gerenciar acesso usando políticas

Você controla o acesso na AWS criando políticas e anexando-as a identidades ou recursos da AWS. Uma política é um objeto na AWS que, quando associado a uma identidade ou recurso, define suas permissões. A AWS avalia essas políticas quando uma entidade principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas são armazenadas na AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão geral das políticas JSON no Guia do usuário do IAM.

Os administradores podem usar AWS as políticas JSON da para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e funções não têm permissões. Para conceder aos usuários permissões para executar ações nos recursos de que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM a perfis, e os usuários podem assumir os perfis.

As políticas do IAM definem permissões para uma ação independente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de perfis do AWS Management Console, da AWS CLI ou da API da AWS.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e funções podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criar políticas do IAM no Guia do usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda mais como políticas embutidas ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas independentes que podem ser anexadas a vários usuários, grupos e perfis na Conta da AWS. As políticas gerenciadas incluem políticas gerenciadas pela AWS e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

Políticas baseadas em recurso

Uma política de chaves do AWS KMS corresponde a uma política baseada em recursos que controla o acesso a uma chave do KMS. Cada chave do KMS deve ter uma política de chaves. É possível usar outro mecanismo de autorização para permitir o acesso à chave do KMS, mas somente se a política de chaves permitir. (É possível usar uma política do IAM para negar o acesso para uma chave do KMS, mesmo que a política de chaves não permita isso explicitamente.)

Políticas baseadas em recursos são documentos de política JSON que você vincula a um recurso, como uma chave do KMS, para controlar o acesso ao recurso específico. A política baseada em recursos define as ações que uma entidade principal especificada pode executar nesse recurso e sob quais condições. Você não especifica o recurso em uma política baseada em recursos, mas deve especificar uma entidade principal, como contas, usuários, perfis, usuários federados ou

Serviços da AWS. As políticas baseadas em recursos são políticas em linha localizadas no serviço que gerencia o recurso. Não é possível usar as políticas gerenciadas pela AWS do IAM, como a política gerenciada `AWSKeyManagementServicePowerUser`, em uma política baseada em recursos.

Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

Amazon S3, AWS WAF e Amazon VPC são exemplos de serviços compatíveis com ACLs. Para saber mais sobre ACLs, consulte Visão geral da lista de controle de acesso (ACL) no Guia do desenvolvedor do Amazon Simple Storage Service.

O AWS KMS não é compatível com ACLs.

Outros tipos de política

A AWS aceita tipos de política menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões: um limite de permissões é um atributo avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do usuário do IAM.
- Políticas de controle de serviço (SCPs): SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (UO) no AWS Organizations. O AWS Organizations é um serviço para agrupar e gerenciar centralmente várias Contas da AWS pertencentes à sua empresa. Se você habilitar todos os atributos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as contas. O SCP limita as permissões para entidades em contas-membro, incluindo cada .Usuário raiz da conta da AWS Para obter mais informações sobre o Organizações e SCPs, consulte How SCPs work (Como os SCPs funcionam) noAWS Organizations Guia do usuário do .

- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em recurso. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia do usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como a AWS determina se deve permitir uma solicitação quando há vários tipos de política envolvidos, consulte Lógica da avaliaçãode políticas no Guia do usuário do IAM.

Atributos AWS KMS

No AWS KMS, o recurso principal é AWS KMS key. O AWS KMS também oferece suporte a um alias, um recurso independente que fornece um nome amigável para uma chave do KMS. Algumas operações do AWS KMS permitem usar um alias para identificar uma chave do KMS.

Cada instância de uma chave do KMS ou um alias tem um Amazon Resource Name (ARN) exclusivo com um formato padrão. Em recursos do AWS KMS, o nome do serviço da AWS é `kms`.

- AWS KMS key

  Formato do ARN:

  ```
  arn:AWS partition name:AWS service name:Região da AWS:Conta da AWS ID:key/key ID
  ```

  Exemplo de ARN:

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

- Alias

  Formato do ARN:

```
arn:AWS partition name:AWS service name:Região da AWS:Conta da AWS
ID:alias/alias name
```

Exemplo de ARN:

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

O AWS KMS fornece um conjunto de operações de API para trabalhar com os seus recursos do AWS KMS. Para mais informações sobre como identificar chaves do KMS nas operações de API do AWS Management Console e do AWS KMS, consulte Identificadores-chave () KeyId. Para uma lista de operações do AWS KMS, consulte a Referência de APIs do AWS Key Management Service.

Políticas-chave em AWS KMS

Uma política fundamental é uma política de recursos para um AWS KMS key. Políticas de chaves são a principal maneira de controlar o acesso a chaves do KMS. Cada chave do KMS deve ter exatamente uma política de chaves. As instruções na política de chaves determinam quem tem permissão para usar a chave do KMS e como eles podem usá-la. Você também pode usar políticas do IAM e concessões para controlar o acesso à chave do KMS, mas cada chave do KMS deve ter uma política de chaves.

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 nunca negada, em uma política de chaves, política do IAM ou concessão.

A menos que a política de chaves permita isto explicitamente, você não pode usar políticas do IAM para autorizar o acesso a uma chave do KMS. Sem permissão da política de chaves, as políticas do IAM que autorizam permissões não têm efeito. (Você pode usar uma política do IAM para negar uma permissão para uma chave KMS sem permissão de uma política de chaves.) A política de chaves padrão habilita as políticas do IAM. Para habilitar políticas do IAM em sua política de chaves, adicione a declaração de política descrita em Permitir acesso à Conta da AWS e habilita políticas do IAM.

Ao contrário das políticas do IAM, que são globais, as políticas de chaves são regionais. Uma política de chaves controla o acesso somente a uma chave do KMS na mesma região. Ela não tem efeito sobre as chaves do KMS em outras regiões.

Tópicos

- Criação de uma política de chave
- Política de chaves padrão
- Visualizar uma política de chaves
- Alterar uma política de chaves
- Permissões para AWS serviços nas principais políticas

Criação de uma política de chave

Você pode criar e gerenciar políticas de chaves no AWS KMS console usando operações de AWS KMS API, como CreateKey, ReplicateKey, e PutKeyPolicy, ou usando um AWS CloudFormation modelo.

Quando você cria uma chave KMS no AWS KMS console, o console orienta você pelas etapas de criação de uma política de chaves com base na política de chaves padrão do console. Ao usar as APIs `CreateKey` ou `ReplicateKey`, se você não especificar uma política de chaves, essas APIs aplicam a política de chaves padrão para chaves criadas programaticamente. Ao usar a API `PutKeyPolicy`, você precisa especificar uma política de chaves.

Cada documento de política pode ter uma ou mais declarações de política. O exemplo a seguir mostra um documento válido de política de chaves com uma instrução de política.

```
{
  "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"
        }
      }
    }
  ]
```

```
}
```

Tópicos

- Formato de política de chaves
- Elementos em uma política de chaves
- Política de chaves de exemplo

Formato de política de chaves

Um documento de política de chaves deve estar de acordo com as seguintes regras:

- Até 32 kilobytes (32.768 bytes)
- O elemento `Sid` em uma instrução de política de chaves pode incluir espaços. (É proibido usar espaços no elemento `Sid` de um documento de política do IAM.)

Um documento de política de chaves pode incluir apenas os seguintes caracteres:

- Caracteres ASCII imprimíveis
- Caracteres imprimíveis no conjunto de caracteres Basic Latin e Latin-1 Supplement
- Os caracteres especiais de tabulação (`\u0009`), alimentação de linha (`\u000A`) e retorno de carro (`\u000D`)

Elementos em uma política de chaves

Um documento de política de chaves deve ter os elementos a seguir:

Version (Versão)

Especifica a versão do documento de política de chaves. Define a versão como `2012-10-17` (a versão mais recente).

Statement

Inclui as instruções da política. Um documento de política de chaves deve ter pelo menos uma instrução.

Cada instrução de política de chaves pode consistir em até seis elementos. Os elementos `Effect`, `Principal`, `Action` e `Resource` são obrigatórios.

Sid

(Opcional) O identificador de instrução (`Sid`) é uma string arbitrária que você pode usar para descrever a instrução. O `Sid` em uma política de chaves pode incluir espaços. (Você não pode incluir espaços no elemento `Sid` de uma política do IAM.)

Efeito

(Obrigatório) Determina se as permissões devem ser permitidas ou negadas na instrução de política. Os valores válidos são `Allow` ou `Deny`. Se você não permitir explicitamente o acesso a uma chave do KMS, esse acesso será implicitamente negado. Também é possível negar explicitamente o acesso a uma chave do KMS. Você poderia fazer isso para garantir que um usuário não possa acessá-la, mesmo quando uma política diferente permite o acesso.

Entidade principal

(Obrigatório) A entidade principal é a identidade que recebe a especificação de permissões na instrução de política. Você pode especificar usuários do IAM Contas da AWS, funções do IAM e alguns AWS serviços como principais em uma política de chaves. Grupos de usuários do IAM não são uma entidade principal válida em nenhum tipo de política.

Um valor de asterisco, como `"AWS": "*"` representa todas as identidades da AWS em todas as contas.

> **Important**
>
> Não defina a entidade principal como um asterisco (*) em qualquer instrução de política de chave que permita permissões, a menos que você utilize condições para limitar a política de chave. Um asterisco dá a cada identidade em cada Conta da AWS permissão para usar a chave KMS, a menos que outra declaração de política a negue explicitamente. Usuários de outros usuários Contas da AWS podem usar sua chave KMS sempre que tiverem permissões correspondentes em suas próprias contas.

> **Note**
>
> As práticas recomendadas do IAM não encorajam o uso de usuários do IAM com credenciais de longo prazo. Sempre que possível, use os perfis do IAM, por fornecerem credenciais temporárias. Para obter detalhes, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

Quando a entidade em uma declaração de política de chaves é uma entidade principal da Conta da AWS no formato `arn:aws:iam::111122223333:root"`, a declaração da política não dá permissão a nenhuma entidade principal do IAM. Em vez disso, ele dá Conta da AWS permissão para usar políticas do IAM para delegar as permissões especificadas na política de chaves. (Uma entidade principal no formato `arn:aws:iam::111122223333:root"` não representa o usuário raiz de conta da AWS, apesar do uso de “root” no identificador da conta. No entanto, a entidade principal da conta representa a conta e seus administradores, incluindo o usuário raiz da conta.)

Quando o principal é outro Conta da AWS ou seus diretores, as permissões são efetivas somente quando a conta é ativada na região com a chave e a política de chaves do KMS. Para obter informações sobre regiões não habilitadas por padrão (“regiões de adesão”), consulte Gerenciar Regiões da AWS em Referência geral da AWS.

Para permitir que outra Conta da AWS pessoa ou seus principais usem uma chave KMS, você deve fornecer permissão em uma política de chaves e em uma política do IAM na outra conta. Para obter detalhes, consulte Permitir que usuários de outras contas usem uma chave do KMS.

Ação

(Obrigatório) Especifica as operações de API que serão permitidas ou negadas. Por exemplo, a `kms:Encrypt` ação corresponde à operação AWS KMS Criptografar. Você pode listar mais de uma ação em uma declaração de política. Para ter mais informações, consulte Referência de permissões.

Recurso

(Obrigatório) Em uma política de chaves, o valor do elemento Recurso é `"*"`, o que significa “esta chave do KMS”. O asterisco (`"*"`) identifica a chave do KMS à qual a política de chaves está associada.

> **Note**
>
> Se o elemento `Resource` necessário estiver ausente de uma declaração de política de chave, a declaração de política não terá efeito. Uma declaração de política de chaves sem um elemento `Resource` não se aplica a nenhuma chave do KMS. Quando uma declaração de política chave não tem seu `Resource` elemento, o AWS KMS console relata corretamente um erro, mas as PutKeyPolicyAPIs CreateKeye são bem-sucedidas, mesmo que a declaração de política seja ineficaz.

Condição

(Opcional) As condições especificam os requisitos que devem ser atendidos para que a política de chaves entre em vigor. Com condições, AWS pode avaliar o contexto de uma solicitação de API para determinar se a declaração de política se aplica ou não.

Para especificar condições, você usa chaves de condição predefinidas. AWS KMS suporta chaves de condição AWS globais e chaves de AWS KMS condição. Para oferecer suporte ao controle de acesso baseado em atributos (ABAC), AWS KMS fornece chaves de condição que controlam o acesso a uma chave KMS com base em tags e aliases. Para obter detalhes, consulte ABAC para AWS KMS.

O formato de uma condição é:

```
"Condition": {"condition operator": {"condition key": "condition value"}}
```

como:

```
"Condition": {"StringEquals": {"kms:CallerAccount": "111122223333"}}
```

Para obter mais informações sobre a sintaxe da AWS política, consulte Referência de política AWS do IAM no Guia do usuário do IAM.

Política de chaves de exemplo

O exemplo a seguir mostra uma política de chaves completa para uma chave do KMS de criptografia simétrica. Você pode usá-lo para referência ao ler sobre os principais conceitos de política neste capítulo. Esta política de chaves combina as declarações da política de exemplo da seção anterior de política de chaves padrão em uma política de chaves única que faz o seguinte:

- Permite Conta da AWS, por exemplo, 111122223333, acesso total à chave KMS. Há permissão para que a conta e seus administradores, incluindo o usuário raiz da conta (para emergências), usem políticas do IAM na conta para conceder acesso à chave do KMS.
- Permite que o perfil do IAM `ExampleAdminRole` administre a chave do KMS.
- Permite que o perfil do IAM `ExampleUserRole` use a chave do 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",
                "kms:RotateKeyOnDemand"
            ],
            "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"
                }
            }
        }
    ]
}
```

Política de chaves padrão

Ao criar uma chave do KMS, é possível especificar a política de chaves da nova chave do KMS. 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 no AWS KMS console ou usa a AWS KMS API.

Política de chaves padrão ao criar uma chave do KMS de forma programática

Quando você cria uma chave KMS programaticamente com a AWS KMS API (inclusive usando AWS os SDKs AWS Command Line Interfaceou AWS Tools for PowerShell) e não especifica uma política de chaves, AWS KMS aplica uma política de chaves padrão muito simples. Essa política de chaves padrão tem uma declaração de política que dá ao Conta da AWS proprietário da chave KMS permissão para usar políticas do IAM para permitir acesso a todas as AWS KMS operações na chave

KMS. Para obter mais informações sobre essa declaração de política, consulte Permitir acesso à Conta da AWS e habilita políticas do IAM.

Política de chaves padrão quando você cria uma chave KMS com o AWS Management Console

Quando você cria uma chave KMS com o AWS Management Console, a política de chaves começa com a declaração de política que permite o acesso Conta da AWS e ativa as políticas do IAM. Em seguida, o console adiciona uma declaração de administradores de chaves, uma declaração de usuários-chave e (para a maioria dos tipos de chaves) uma declaração que permite que os diretores usem a chave KMS com outros serviços. AWS Você pode usar os recursos do AWS KMS console para especificar os usuários do IAM, os IAMRoles e Contas da AWS quem são os principais administradores e aqueles que são os principais usuários (ou ambos).

Permissões

- Permitir acesso à Conta da AWS e habilita políticas do IAM
- Permite que administradores de chaves administrem a chave do KMS
- Permite que os usuários de chaves usem a chave do KMS
  - Permite que usuários de chaves usem uma chave do KMS para operações de criptografia
  - Permite que os usuários de chaves usem a chave do KMS com serviços da AWS

Permitir acesso à Conta da AWS e habilita políticas do IAM

A declaração de política de chave padrão a seguir é fundamental.

- Ele dá ao Conta da AWS proprietário da chave KMS acesso total à chave KMS.

  Diferentemente AWS de outras políticas de recursos, uma política de AWS KMS chaves não dá permissão automática à conta ou a nenhuma de suas identidades. Para dar permissão aos administradores de conta, a política de chaves deve incluir uma declaração explícita que forneça essa permissão, como esta.
- Ele permite que a conta use políticas do IAM para permitir acesso à chave do KMS, além da política de chaves.

  Sem essa permissão, as políticas do IAM que permitem o acesso à chave são ineficazes, embora as políticas do IAM que negam acesso à chave ainda sejam efetivas.
- Ela reduz o risco de a chave se tornar não gerenciável, dando permissão de controle de acesso aos administradores da conta, incluindo o usuário raiz da conta, que não pode ser excluído.

A declaração de política de chaves a seguir é toda a política de chaves padrão para chaves do KMS criadas programaticamente. É a primeira declaração de política na política de chaves padrão para chaves KMS criadas no AWS KMS console.

```
{
  "Sid": "Enable IAM User Permissions",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:root"
   },
  "Action": "kms:*",
  "Resource": "*"
}
```

Permite que políticas do IAM permitam o acesso à chave do KMS.

A declaração de política de chaves mostrada acima dá ao Conta da AWS proprietário da chave permissão para usar políticas do IAM, bem como políticas de chave, para permitir todas as ações (`kms:*`) na chave KMS.

A entidade principal nesta declaração de política de chave é a entidade principal da conta, que é representada por um ARN neste formato: `arn:aws:iam::account-id:root`. O principal da conta representa a AWS conta e seus administradores.

Quando a entidade principal em uma instrução de política de chave é a entidade principal da conta, a instrução de política não concede permissões para o uso da chave do KMS a nenhuma entidade principal do IAM. Em vez disso, ela permite que a conta use políticas do IAM para delegar as permissões especificadas na política de chaves. Essa declaração de política de chaves padrão permite que a conta use políticas do IAM para delegar permissão para todas as ações (`kms:*`) na chave do KMS.

reduz o risco de a chave do KMS perder a capacidade de gerenciamento.

Ao contrário AWS de outras políticas de recursos, uma política de AWS KMS chaves não dá permissão automática à conta ou a qualquer um de seus diretores. Para dar permissão a qualquer entidade principal, incluindo a entidade principal da conta, você deve usar uma declaração de política chave que forneça a permissão explicitamente. Você não precisa dar à entidade principal da conta, ou a qualquer entidade principal, acesso à chave do KMS. No entanto, dar acesso à entidade principal da conta ajuda você a evitar que a chave se torne não gerenciável.

Por exemplo, suponha que você crie uma política de chaves que dê acesso a apenas um usuário à chave do KMS. Se você excluir esse usuário, a chave se tornará não gerenciável e você deverá contatar o suporte da AWS para recuperar o acesso à chave do KMS.

A declaração de política de chaves mostrada acima dá permissão para controlar a chave do principal da conta, que representa o Conta da AWS e seus administradores, incluindo o usuário raiz da conta. O usuário raiz da conta é a única entidade principal que não pode ser excluída, a menos que você exclua a Conta da AWS. As práticas recomendadas do IAM desencorajam agir em nome do usuário raiz da conta, exceto em caso de emergência. No entanto, talvez seja necessário atuar como usuário raiz da conta se você excluir todos os outros usuários e funções com acesso à chave do KMS.

Permite que administradores de chaves administrem a chave do KMS

A política de chaves padrão criada pelo console permite que você escolha usuários e funções do IAM na conta e os torne administradores de chaves. Essa declaração é chamada de declaração de administradores de chaves. Os administradores de chaves têm permissões para gerenciar a chave do KMS, mas não têm permissões para usar essa chave em operações de criptografia. Você pode adicionar usuários e funções do IAM à lista de administradores de chaves ao criar a chave do KMS na visualização padrão ou na visualização de políticas.

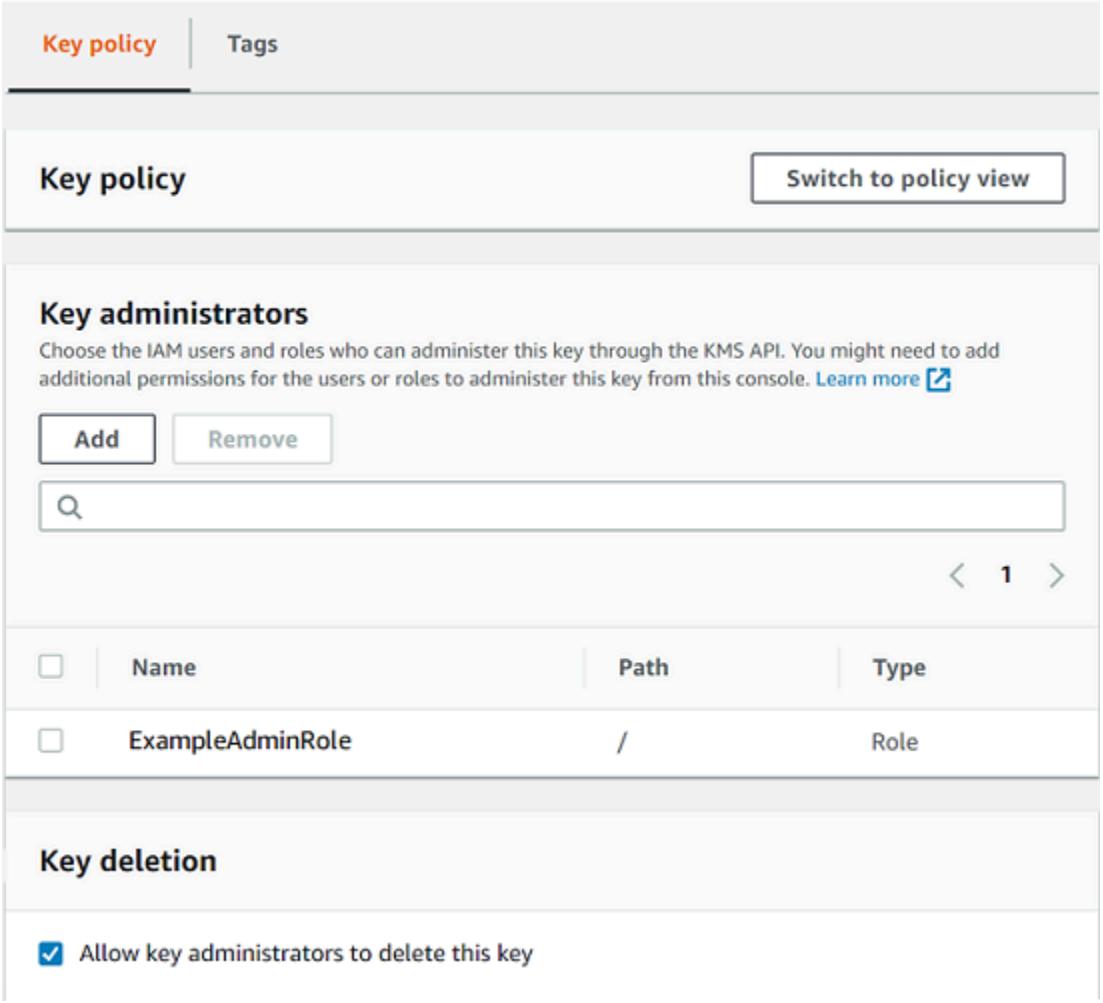
Warning

Como os administradores de chaves têm permissão para alterar a política de chaves e criar concessões, eles podem conceder a si mesmos e a outras pessoas AWS KMS permissões não especificadas nessa política.
As entidades principais que têm permissão para gerenciar etiquetas e aliases também podem controlar o acesso a uma chave do KMS. Para obter detalhes, consulte ABAC para AWS KMS.

Note

As práticas recomendadas do IAM não encorajam o uso de usuários do IAM com credenciais de longo prazo. Sempre que possível, use os perfis do IAM, por fornecerem credenciais temporárias. Para obter detalhes, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

O exemplo a seguir mostra a declaração de administradores de chaves na visualização padrão do console do AWS KMS .



A seguir é apresentado um exemplo que mostra a declaração de administradores de chaves na visualização padrão do console do AWS KMS . Essa instrução de administradores de chaves serve para uma chave do KMS de criptografia simétrica e região única.

```
{
  "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": "*"
}
```

A instrução padrão de administradores de chaves para a chave mais comum do KMS, uma chave do KMS de criptografia simétrica de região única, possibilita as permissões a seguir. Para obter informações detalhadas sobre cada permissão, consulte a AWS KMS permissões.

Quando você usa o AWS KMS console para criar uma chave KMS, o console adiciona os usuários e as funções que você especifica ao `Principal` elemento na instrução dos administradores de chaves.

Muitas dessas permissões contêm o caractere curinga (*), que permite todas as permissões que começam com o verbo especificado. Como resultado, ao AWS KMS adicionar novas operações de API, os administradores de chaves podem usá-las automaticamente. Não é necessário atualizar suas políticas de chaves para incluir as novas operações. Se você preferir limitar seus administradores de chaves a um conjunto fixo de operações de API, poderá alterar sua política de chaves.

`kms:Create*`

Permite `kms:CreateAlias` e `kms:CreateGrant`. (A permissão `kms:CreateKey` é válida somente em uma política do IAM.)

`kms:Describe*`

Permite `kms:DescribeKey`. A permissão `kms:DescribeKey` é necessária para visualizar a página de detalhes de chaves de uma chave do KMS no AWS Management Console.

`kms:Enable*`

Permite `kms:EnableKey`. Para chaves do KMS de criptografia simétrica, ela também permite `kms:EnableKeyRotation`.

`kms:List*`

Permite `kms:ListGrants`, `kms:ListKeyPolicies` e `kms:ListResourceTags`. (As permissões `kms:ListAliases` e `kms:ListKeys`, que são necessárias para exibir chaves do KMS no AWS Management Console, são válidas somente em políticas do IAM.)

`kms:Put*`

Permite `kms:PutKeyPolicy`. Essa permissão permite que os administradores de chaves alterem a política de chaves dessa chave do KMS.

`kms:Update*`

Permite `kms:UpdateAlias` e `kms:UpdateKeyDescription`. Para chaves de várias regiões, ele permite `kms:UpdatePrimaryRegion` nesta chave do KMS.

`kms:Revoke*`

Permite `kms:RevokeGrant`, o que permite que os administradores de chaves excluam uma concessão mesmo que eles não sejam uma entidade principal prestes a se retirar na concessão.

`kms:Disable*`

Permite `kms:DisableKey`. Para chaves do KMS de criptografia simétrica, ela também permite `kms:DisableKeyRotation`.

`kms:Get*`

Permite `kms:GetKeyPolicy` e `kms:GetKeyRotationStatus`. Para chaves do KMS com material de chave importado, ela permite `kms:GetParametersForImport`. Para chaves do KMS assimétricas, ela permite `kms:GetPublicKey`. A permissão `kms:GetKeyPolicy` é necessária para visualizar a política da chave de uma chave do KMS no AWS Management Console.

`kms:Delete*`

Permite `kms:DeleteAlias`. Para chaves com material de chave importado, ela permite `kms:DeleteImportedKeyMaterial`. A permissão `kms:Delete*` não permite que os administradores de chaves excluam a chave do KMS (`ScheduleKeyDeletion`).

`kms:TagResource`

Permite `kms:TagResource`, que, por sua vez, permite que os administradores de chaves adicionem tags à chave do KMS. Como as tags também podem ser usadas para controlar o acesso à chave do KMS, essa permissão pode permitir que os administradores concedam ou neguem acesso à chave do KMS. Para obter detalhes, consulte ABAC para AWS KMS.

`kms:UntagResource`

Permite `kms:UntagResource`, que, por sua vez, permite que os administradores de chaves excluam tags da chave do KMS. Como as tags podem ser usadas para controlar o acesso à chave, essa permissão pode permitir que os administradores concedam ou neguem acesso à chave do KMS. Para obter detalhes, consulte ABAC para AWS KMS.

`kms:ScheduleKeyDeletion`

Permite `kms:ScheduleKeyDeletion`, que, por sua vez, permite que os administradores de chaves excluam esta chave do KMS. Para excluir essa permissão, desmarque a opção Allow key administrators to delete this key(Permitir que os administradores de chaves excluam essa chave).

`kms:CancelKeyDeletion`

Permite `kms:CancelKeyDeletion`, que, por sua vez, permite que os administradores de chaves cancelem a exclusão desta chave do KMS. Para excluir essa permissão, desmarque a opção Allow key administrators to delete this key(Permitir que os administradores de chaves excluam essa chave).

AWS KMS adiciona as seguintes permissões à declaração padrão dos administradores de chaves quando você cria chaves para fins especiais.

`kms:ImportKeyMaterial`

A permissão `kms:ImportKeyMaterial` permite que os administradores de chaves importem material de chave para a chave do KMS. Essa permissão está incluída na política de chaves somente quando você cria uma chave do KMS sem material de chave.

`kms:ReplicateKey`

A `kms:ReplicateKey`permissão permite que os administradores de chaves criem uma réplica de uma chave primária multirregional em uma região diferente. AWS Essa permissão é incluída na política de chaves somente quando você cria uma chave primária ou de réplica de várias regiões.

`kms:UpdatePrimaryRegion`

A permissão `kms:UpdatePrimaryRegion` permite que os administradores de chaves alterem uma chave de réplica de várias regiões para uma chave primária de várias regiões. Essa

permissão é incluída na política de chaves somente quando você cria uma chave primária ou de réplica de várias regiões.

Permite que os usuários de chaves usem a chave do KMS

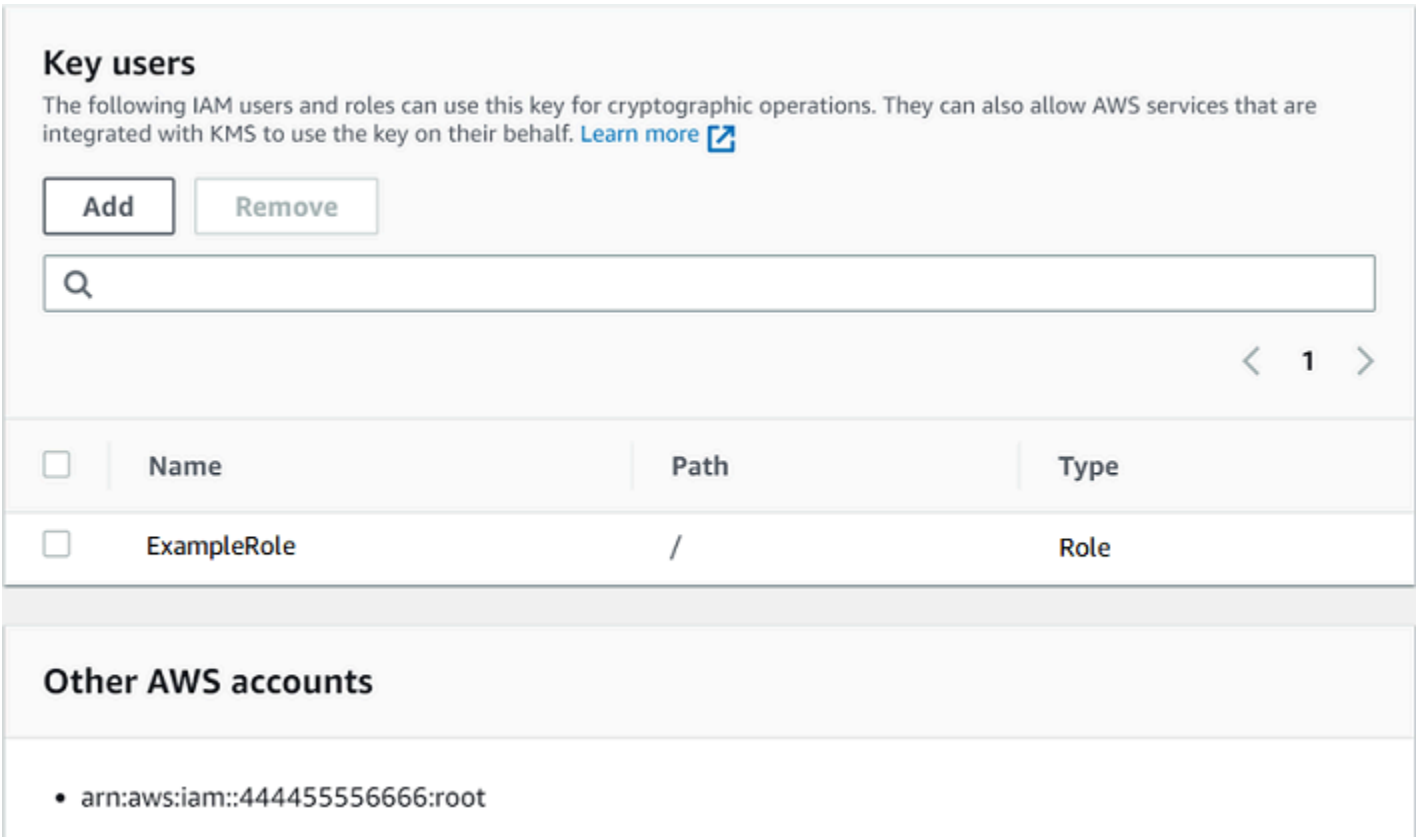
A política de chaves padrão que o console cria para chaves KMS permite que você escolha usuários do IAM e funções do IAM na conta, e externas Contas da AWS, e os torne usuários-chave.

O console adiciona duas instruções de política à política de chaves para usuários de chaves.

- Use a chave do KMS diretamente – A primeira instrução de política de chaves dá aos usuários de chave permissão para usar a chave do KMS diretamente para todas as operações de criptografia com suporte para esse tipo de chave do KMS.
- Use a chave KMS com AWS serviços — A segunda declaração de política dá permissão aos principais usuários para permitir que os AWS serviços integrados usem a chave KMS em seu nome AWS KMS para proteger recursos, como buckets do Amazon S3 e tabelas do Amazon DynamoDB.

Você pode adicionar usuários do IAM, funções do IAM e outros Contas da AWS à lista de usuários principais ao criar a chave do KMS. Você também pode editar a lista com a visualização padrão do console para políticas de chaves, conforme mostrado na imagem a seguir. A visualização padrão para políticas de chaves está na página de detalhes de chaves. Para obter mais informações sobre como permitir que usuários de outras Contas da AWS pessoas usem a chave KMS, consultePermitir que usuários de outras contas usem uma chave do KMS.

> **Note**
>
> As práticas recomendadas do IAM não encorajam o uso de usuários do IAM com credenciais de longo prazo. Sempre que possível, use os perfis do IAM, por fornecerem credenciais temporárias. Para obter detalhes, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.



As declarações de usuários de chaves padrão para uma chave simétrica de região única possibilita as permissões a seguir. Para obter informações detalhadas sobre cada permissão, consulte a AWS KMS permissões.

Quando você usa o AWS KMS console para criar uma chave KMS, o console adiciona os usuários e as funções que você especifica ao `Principal` elemento em cada declaração de usuários da chave.

```
{
  "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}}
}
```

Permite que usuários de chaves usem uma chave do KMS para operações de criptografia

Os usuários de chaves têm permissão para usar a chave do KMS diretamente em todas as operações de criptografia com suporte na chave do KMS. Eles também podem usar a DescribeKeyoperação para obter informações detalhadas sobre a chave KMS no AWS KMS console ou usando as operações da AWS KMS API.

Por padrão, o AWS KMS console adiciona declarações de usuários-chave, como as dos exemplos a seguir, à política de chaves padrão. Como elas são compatíveis com diferentes operações de API, as ações nas instruções de política para chaves do KMS de criptografia simétrica, chaves do KMS de Hash-based message authentication code (HMAC – Código de autenticação de mensagem por hash), chaves do KMS assimétricas para criptografia de chave pública e chaves do KMS assimétricas para assinatura e verificação são ligeiramente diferentes.

Chaves do KMS de criptografia simétrica

O console adiciona a seguinte instrução à política de chaves para chaves do KMS de criptografia simétrica.

```
{
  "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": "*"
}
```

Chaves do KMS de HMAC

O console adiciona a seguinte instrução à política de chaves para chaves do KMS de 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": "*"
}
```

Chaves do KMS assimétricas para criptografia de chave pública

O console adiciona a seguinte instrução à política de chaves para chaves do KMS assimétricas com um uso de chave de Encrypt and decrypt (Criptografar e descriptografar).

```
{
  "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": "*"
}
```

Chaves do KMS assimétricas para assinatura e verificação

O console adiciona a seguinte instrução à política de chaves para chaves do KMS assimétricas com um uso de chave de Sign and verify (Assinar e verificar).

```
{
  "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": "*"
}
```

As ações nessas declarações concedem aos usuários de chaves as permissões a seguir.

kms:Encrypt

Permite que os usuários de chaves criptografem dados com essa chave do KMS.

kms:Decrypt

Permite que os usuários de chaves descriptografem dados com essa chave do KMS.

kms:DescribeKey

Permite que os usuários de chaves obtenham informações detalhadas sobre essa chave do KMS, incluindo seus identificadores, data de criação e estado de chave. Também permite que os principais usuários exibam detalhes sobre a chave KMS no AWS KMS console.

kms:GenerateDataKey*

Permite que os usuários de chaves solicitem uma chave de dados simétrica ou um par de chaves de dados assimétricas para operações criptográficas no lado do cliente. O console usa o caractere curinga * para representar a permissão para as seguintes operações

de API: GenerateDataKeyGenerateDataKeyWithoutPlaintext, GenerateDataKeyPair, e. GenerateDataKeyPairWithoutPlaintext Essas permissões são válidas somente nas chaves do KMS simétricas que criptografam as chaves de dados.

kms: GenerateMac

Permite que os usuários de chaves usem uma chave do KMS de HMAC para gerar uma etiqueta de HMAC.

kms: GetPublicKey

Permite que os usuários de chaves baixem a chave pública da chave do KMS assimétrica. As partes com quem você compartilha essa chave pública podem criptografar dados fora do AWS KMS. No entanto, esses textos cifrados só podem ser descriptografados chamando a operação Decrypt no AWS KMS.

km: * ReEncrypt

Permite que os usuários de chaves criptografem novamente os dados que foram originalmente criptografados com essa chave do KMS ou permite que eles usem essa chave do KMS para criptografar novamente dados já criptografados. A ReEncryptoperação requer acesso às chaves KMS de origem e destino. Para fazer isso, é possível conceder a permissão `kms:ReEncryptFrom` na chave do KMS de origem e a permissão `kms:ReEncryptTo` na chave do KMS de destino. No entanto, para simplificar, o console permite `kms:ReEncrypt*` (com o caractere curinga `*`) nas duas chaves do KMS.

kms:Sign

Permite que os usuários de chaves assinem mensagens com essa chave do KMS.

kms:Verify

Permite que os usuários de chaves verifiquem assinaturas com essa chave do KMS.

kms: VerifyMac

Permite que os usuários de chaves usem uma chave do KMS de HMAC para verificar uma etiqueta de HMAC.

Permite que os usuários de chaves usem a chave do KMS com serviços da AWS

A política de chaves padrão no console também dá aos principais usuários as permissões de que precisam para proteger seus dados em AWS serviços que usam concessões. AWS os serviços geralmente usam concessões para obter permissão específica e limitada para usar uma chave KMS.

Essa declaração de política de chaves permite que o usuário da chave crie, visualize e revogue concessões na chave KMS, mas somente quando a solicitação de operação de concessão vem de um AWS serviço integrado com o. AWS KMS A condição kms: GrantIsFor AWSResource policy não permite que o usuário chame essas operações de concessão diretamente. Quando o usuário da chave permite, um AWS serviço pode criar uma concessão em nome do usuário que permite que o serviço use a chave KMS para proteger os dados do usuário.

Os usuários de chaves precisam dessas permissões de concessão para usar a chave do KMS com os serviços integrados, mas essas permissões não são suficientes. Os usuários de chaves também precisam de permissão para usar os serviços integrados. Para obter detalhes sobre como dar aos usuários acesso a um AWS serviço que se integra ao AWS KMS, consulte a documentação do serviço integrado.

```
{
  "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}}
}
```

Por exemplo, os usuários de chaves podem usar essas permissões na chave do KMS das maneiras indicadas a seguir.

- Use essa chave do KMS com o Amazon Elastic Block Store (Amazon EBS) e com o Amazon Elastic Compute Cloud (Amazon EC2) para anexar um volume do EBS criptografado a uma instância do EC2. O usuário de chaves concede implicitamente permissão ao Amazon EC2 para usar a chave do KMS com o objetivo de associar o volume criptografado à instância. Para ter mais informações, consulte Como o Amazon Elastic Block Store (Amazon EBS) usa o AWS KMS.
- Use essa chave do KMS com o Amazon Redshift para executar um cluster criptografado. O usuário de chaves concede implicitamente permissão ao Amazon Redshift para usar a chave do KMS para executar o cluster criptografado e criar snapshots criptografados. Para ter mais informações, consulte Como o Amazon Redshift usa o AWS KMS.

- Use essa chave do KMS com outros serviços da AWS integrados ao AWS KMS que usem concessões para criar, gerenciar ou usar recursos criptografados com esses serviços.

Apolítica de chaves padrão permite que os usuários de chaves deleguem suas permissões de concessão para todos os serviços integrados que usam concessões. No entanto, você pode criar uma política de chaves personalizada que restrinja a permissão a AWS serviços específicos. Para obter mais informações, consulte a kms: ViaService chave de condição.

Visualizar uma política de chaves

Você pode visualizar a política de chaves de uma chave gerenciada pelo AWS KMS cliente ou Chave gerenciada pela AWSem sua conta usando a operação AWS Management Console ou a GetKeyPolicyoperação na AWS KMS API. Não é possível usar essas técnicas para visualizar a política de chaves de uma chave do KMS em outra Conta da AWS.

Para saber mais sobre as políticas de chaves do AWS KMS, consulte Políticas-chave em AWS KMS. Para saber como determinar quais usuários e funções têm acesso a uma chave do KMS, consulte the section called “Determinar o acesso”.

Tópicos

- Visualizar uma política de chaves (console)
- Visualizar uma política de chaves (API do AWS KMS)

Visualizar uma política de chaves (console)

Os usuários autorizados podem visualizar a política de chaves de uma Chave gerenciada pela AWS ou de uma chave gerenciada pelo cliente na guia Key policy (Política de chaves) do AWS Management Console.

Para visualizar a política de chaves de uma chave KMS noAWS Management Console, você deve ter as permissões kms: ListAliases, kms: DescribeKey e kms:. GetKeyPolicy

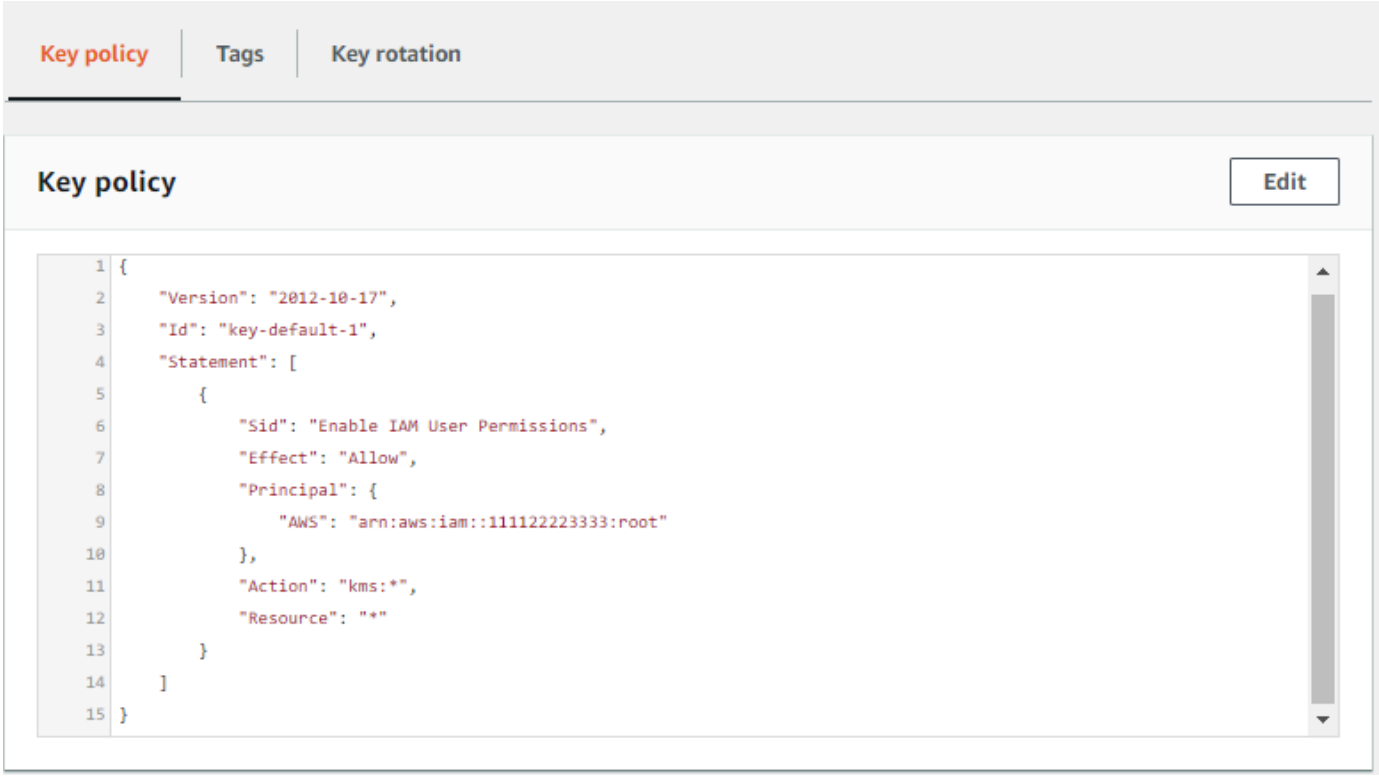
1. Faça login no AWS Management Console e abra o console do AWS Key Management Service (AWS KMS) em https://console.aws.amazon.com/kms.
2. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.
3. Para visualizar as chaves na sua conta que a AWS cria e gerencia para você, no painel de navegação, escolha AWS managed keys (Chaves gerenciadas pela AWS). Para exibir as

chaves em sua conta que você cria e gerencia, no painel de navegação, escolha Customer managed keys (Chaves gerenciadas de cliente).

4. Na lista de chaves do KMS, escolha o alias ou o ID de chave da chaves do KMS que você deseja examinar.
5. Selecione a guia Key policy (Política de chaves).

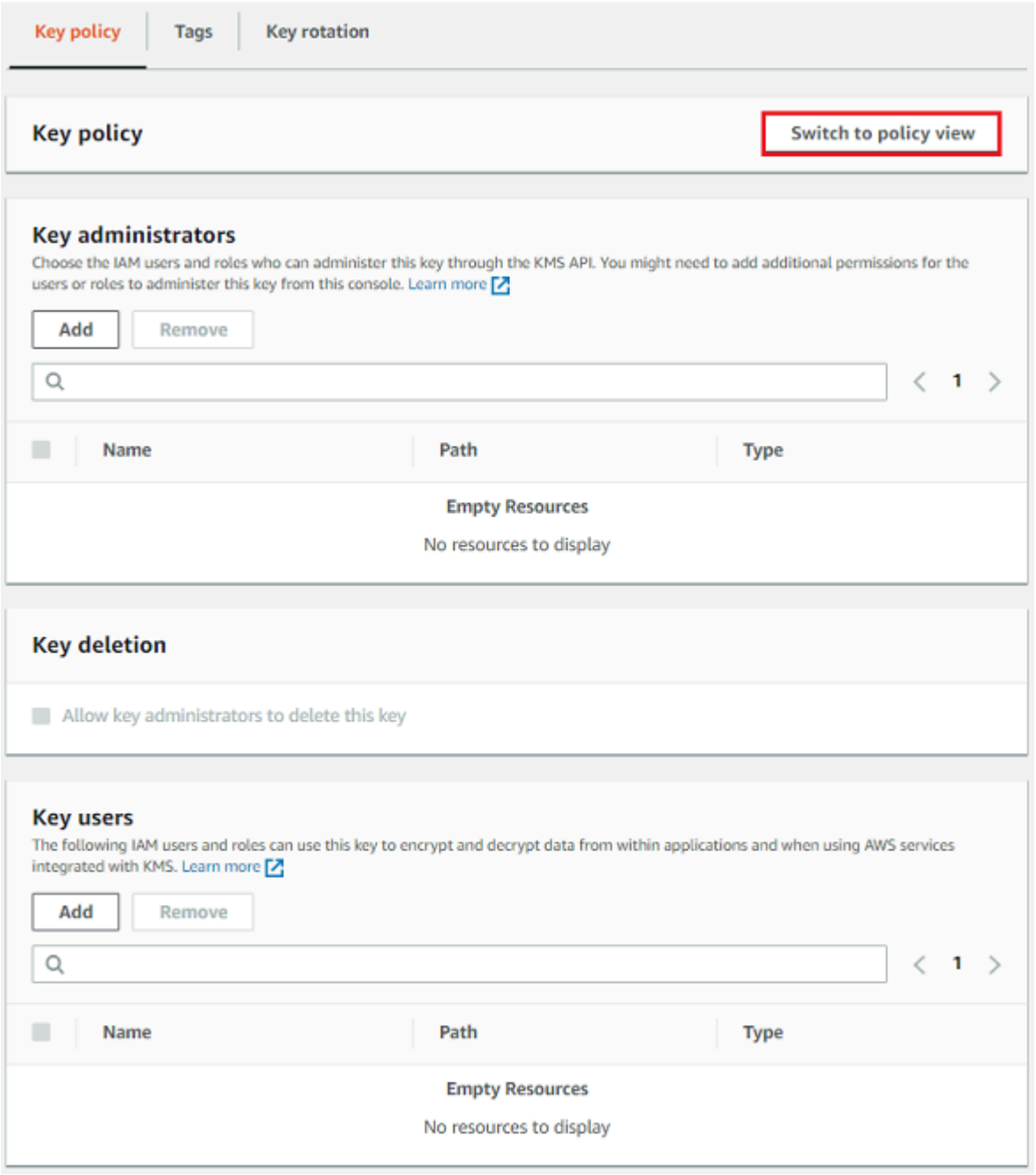
   Na seção Key policy (Política de chaves), você pode ver o documento da política de chaves. Essa é a visualização da política. Nas instruções da política de chaves, é possível ver as entidades principais que receberam acesso à chave do KMS pela política de chaves e ver as ações que elas podem executar.

   O exemplo a seguir mostra a visualização da política de chaves padrão.



   Ou, se você criou a chave do KMS no AWS Management Console, verá a visualização padrão com seções para Key administrators (Administradores de chaves), Key deletion (Exclusão de chaves) e Key Users (Usuários de chaves). Para ver o documento da política de chaves, selecione Switch to policy view (Alternar para a visualização da políticas).

   O exemplo a seguir mostra a visualização padrão da política de chaves padrão.



Visualizar uma política de chaves (API do AWS KMS)

Para obter a política de chaves de uma chave KMS em suaConta da AWS, use a GetKeyPolicyoperação na AWS KMS API. Não é possível usar essa operação para visualizar uma política de chaves em uma conta diferente.

O exemplo a seguir usa o get-key-policycomando no AWS Command Line Interface (AWS CLI), mas você pode usar qualquer AWS SDK para fazer essa solicitação.

Observe que o parâmetro `PolicyName` será exigido mesmo se `default` for seu único valor válido. Além disso, esse comando solicita a saída em texto, em vez de em JSON, para facilitar a visualização.

Antes de executar esse comando, substitua o ID de chave de exemplo por um válido da sua conta.

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

A resposta deve ser semelhante à seguinte, que retorna a política de chaves padrão.

```
{
  "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" : "*"
  } ]
}
```

Alterar uma política de chaves

Você pode alterar a política de chaves de uma chave KMS na sua Conta da AWS usando a AWS Management Console ou a PutKeyPolicyoperação. Não é possível usar essas técnicas para alterar a política de chaves de uma chave do KMS em outra Conta da AWS.

Ao alterar a política de chaves, lembre-se das seguintes regras:

- É possível visualizar a política de chaves de uma Chave gerenciada pela AWS ou de uma chave gerenciada pelo cliente, mas só é possível alterar a política de chaves de uma chave gerenciada pelo cliente. As políticas de Chaves gerenciadas pela AWS são criadas e gerenciadas pelo serviço da AWS que criou a chave do KMS na sua conta. Não é possível visualizar ou alterar a política de chaves para uma Chave pertencente à AWS.
- Você pode adicionar ou remover usuários do IAM, funções do IAM e Contas da AWS na política de chaves e alterar as ações permitidas ou negadas para essas entidades principais. Para mais

informações sobre as maneiras de especificar principais e permissões em uma política de chaves, consulte Políticas de chaves.

- Não é possível adicionar grupos do IAM a uma política de chaves, mas é possível adicionar diversos usuários do IAM e perfis do IAM. Para ter mais informações, consulte Permitir que diversas entidades principais do IAM acessem uma chave do KMS.
- Se você adicionar Contas da AWS externas a uma política de chaves, será necessário também usar políticas do IAM nessas contas externas para conceder permissões a usuários, grupos ou funções do IAM nessas contas. Para ter mais informações, consulte Permitir que usuários de outras contas usem uma chave do KMS.
- O documento de política de chaves resultante não pode exceder 32 KB (32.768 bytes).

Tópicos

- Como alterar uma política de chaves
- Permitir que diversas entidades principais do IAM acessem uma chave do KMS

Como alterar uma política de chaves

Você pode alterar uma política de chaves de três maneiras diferentes, conforme explicado nas seções a seguir.

Tópicos

- Usar a visualização padrão do AWS Management Console
- Usar a visualização de política do AWS Management Console
- Uso da API AWS KMS

Usar a visualização padrão do AWS Management Console

Você pode usar o console para alterar uma política de chaves com uma interface gráfica chamada visualização padrão.

Se as seguintes etapas não correspondem à visualização no console, isso significa que essa política de chaves não foi criada pelo console. Ou significa que a política de chaves foi modificada e é incompatível com a visualização padrão do console. Nesse caso, siga as etapas em Usar a visualização de política do AWS Management Console ou Uso da API AWS KMS.

1. Visualize a política de chaves de uma chave gerenciada pelo cliente conforme descrito em Visualizar uma política de chaves (console). (Você não pode alterar a política de chave de Chaves gerenciadas pela AWS.)
2. Defina o que alterar.

   - Para adicionar ou remover administradores de chaves e permitir ou impedir que eles excluam a chave do KMS, use os controles na seção Key administrators (Administradores de chaves) da página. Os administradores de chaves gerenciam a chave do KMS, incluindo sua habilitação e desabilitação, a configuração da política de chaves e a habilitação da alternância de chaves.
   - Para adicionar ou remover usuários de chaves e permitir ou proibir que Contas da AWS externas usem a chave do KMS, use os controles na seção Key users (Usuários de chaves) da página. Usuários de chaves podem usar a chave do KMS em operações de criptografia, como criptografar, descriptografar, recriptografar e gerar chaves de dados.

Usar a visualização de política do AWS Management Console

Você pode usar o console para alterar um documento de política de chaves com a visualização de política do console.

1. Visualize a política de chaves de uma chave gerenciada pelo cliente conforme descrito em Visualizar uma política de chaves (console). (Você não pode alterar a política de chave de Chaves gerenciadas pela AWS.)
2. Na seção Key Policy (Política de chave), selecione Switch to policy view (Alternar para visualização de política).
3. Edite o documento de política de chaves e selecione Save changes (Salvar alterações).

Uso da API AWS KMS

Você pode usar a PutKeyPolicyoperação para alterar a política de chaves de uma chave KMS no seuConta da AWS. Não é possível usar essa API em uma chave do KMS em outra Conta da AWS.

1. Use a GetKeyPolicyoperação para obter o documento de política de chaves existente e, em seguida, salve o documento de política de chaves em um arquivo. Para obter o código de exemplo em várias linguagens de programação, consulte Obter uma política de chaves.
2. Abra o documento de política de chaves no editor de texto de sua preferência, edite-o e salve o arquivo.

3. Use a PutKeyPolicyoperação para aplicar o documento de política de chaves atualizado à chave KMS. Para obter o código de exemplo em várias linguagens de programação, consulte Definir uma política de chaves.

Para ver um exemplo de cópia de uma política de chaves de uma chave KMS para outra, consulte o GetKeyPolicy exemplo na Referência de AWS CLI Comandos.

Permitir que diversas entidades principais do IAM acessem uma chave do KMS

Grupos do IAM não são entidades principais válidas em uma política de chaves. Para permitir que diversos usuários e perfis acessem uma chave do KMS, siga um dos procedimentos a seguir:

- Use um perfil do IAM como entidade principal na política de chaves. Diversos usuários autorizados podem assumir o perfil, conforme necessário. Para obter detalhes, consulte Perfis do IAM no Guia do usuário do IAM.

  Embora você possa listar diversos usuários do IAM em uma política de chaves, essa prática não é recomendada porque requer que você atualize a política de chaves sempre que a lista de usuários autorizados for alterada. Além disso, as práticas recomendadas do IAM não encorajam o uso de usuários do IAM com credenciais de longo prazo. Para obter detalhes, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.
- Use uma política do IAM para conceder permissões a um grupo do IAM. Para fazer isso, certifique-se de que a política de chaves inclua a instrução que possibilita que as políticas do IAM concedam acesso à chave do KMS, crie uma política do IAM que conceda acesso à chave do KMS e, em seguida, vincule essa política a um grupo do IAM que contenha os usuários do IAM autorizados. Com essa abordagem, você não precisará alterar nenhuma política quando a lista de usuários autorizados for alterada. Basta adicionar ou remover esses usuários do grupo do IAM apropriado. Para obter detalhes, consulte Grupos de usuários do IAM no Guia do usuário do IAM.

Para obter mais informações sobre como as políticas de chaves do AWS KMS e as políticas do IAM funcionam juntas, consulte Solucionar problemas de acesso à chave.

Permissões para AWS serviços nas principais políticas

Muitos AWS serviços são usados AWS KMS keys para proteger os recursos que gerenciam. Quando um serviço usa Chaves pertencentes à AWS ou Chaves gerenciadas pela AWS, o serviço estabelece e mantém as políticas de chaves para essas chaves do KMS.

No entanto, ao usar uma chave gerenciada pelo cliente com um serviço da AWS , você é quem define e mantém a política de chaves. Essa política de chaves deve conceder ao serviço as permissões mínimas necessárias para proteger o recurso em seu nome. Recomendamos seguir o princípio de privilégio mínimo: conceda ao serviço apenas as permissões necessárias. Você pode fazer isso de forma eficaz aprendendo quais permissões o serviço precisa e usando chaves de condição globais da AWS e chaves de condição do AWS KMS para refinar as permissões.

Para encontrar as permissões que o serviço exige em uma chave gerenciada pelo cliente, consulte a documentação de criptografia do serviço. Por exemplo, para obter as permissões exigidas pelo Amazon Elastic Block Store (Amazon EBS), consulte Permissões para usuários do IAM no Guia do usuário do Amazon EC2 para instâncias Linux ou no Guia do usuário do Amazon EC2 para instâncias Windows. Para obter as permissões exigidas pelo Secrets Manager, consulte Autorizar o uso da chave do KMS no Guia do usuário do AWS Secrets Manager .

Implementação de permissões de privilégio mínimo

Ao conceder permissão a um AWS serviço para usar uma chave KMS, certifique-se de que a permissão seja válida somente para os recursos que o serviço deve acessar em seu nome. Essa estratégia de privilégios mínimos ajuda a evitar o uso não autorizado de uma chave KMS quando as solicitações são passadas entre serviços. AWS

Para implementar uma estratégia de privilégios mínimos, recomendamos o uso de chaves de condição de contexto de AWS KMS criptografia e do ARN de origem global ou das chaves de condição da conta de origem.

Uso de chaves de condição de contexto de criptografia

A maneira mais eficaz de implementar permissões com menos privilégios ao usar AWS KMS recursos é incluir as chaves de kms:EncryptionContextKayscondição kms:EncryptionContext:context-keyou na política que permite que os diretores chamem operações AWS KMS criptográficas. Essas chaves de condição são particularmente eficazes porque associam a permissão ao contexto de criptografia que está vinculado ao texto cifrado quando o recurso é criptografado.

Use chaves de condições de contexto de criptografia somente quando a ação na declaração de política for CreateGrantuma operação criptográfica AWS KMS simétrica que usa um `EncryptionContext` parâmetro, como as operações como GenerateDataKeyou Decrypt. (Para ver uma lista das operações válidas, consulte kms:EncryptionContext:context-key ou kms:EncryptionContextKeys. Se você usar essas chaves de condição para permitir outras operações, como, por exemplo DescribeKey, a permissão será negada.

Defina o valor para o contexto de criptografia usado pelo serviço ao criptografar o recurso. Essas informações geralmente estão disponíveis no capítulo Segurança da documentação do serviço. Por exemplo, o contexto de criptografia do AWS Proton identifica o recurso AWS Proton e seu modelo associado. O contexto de criptografia do AWS Secrets Manager identifica o segredo e sua versão. O contexto de criptografia para Amazon Location identifica o rastreador ou a coleção.

O exemplo de declaração de política de chave a seguir permite que o Amazon Location Service crie concessões em nome de usuários autorizados. Essa declaração de política limita a permissão usando as chaves kms: ViaService, kms: CallerAccount e de `kms:EncryptionContext:`*`context-key`* condição para vincular a permissão a um recurso específico do rastreador.

```
{
  "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"
    }
  }
}
```

Uso de chaves de condição **`aws:SourceArn`** ou **`aws:SourceAccount`**

Quando a entidade principal em uma declaração de política chave é uma entidade principal de serviço da AWS, recomendamos usar as chaves de condição globais aws:SourceArn ou aws:SourceAccount, além da chave de condição `kms:EncryptionContext:`*`context-key`*. O ARN e os valores da conta são incluídos no contexto de autorização somente quando uma solicitação AWS KMS vem de outro AWS serviço. Essa combinação de condições implementa permissões de privilégio mínimo e evita um possível cenário de auxiliar confuso. Os diretores de serviços normalmente não são usados como diretores em uma política chave, mas alguns AWS serviços, como o AWS CloudTrail, exigem isso.

Para usar as chaves de condição globais `aws:SourceArn` ou `aws:SourceAccount`, defina o valor como o nome do recurso da Amazon (ARN) ou a conta do recurso que está sendo criptografado. Por exemplo, em uma declaração de política de chave que concede ao AWS CloudTrail permissão para criptografar uma trilha, defina o valor de `aws:SourceArn` como o ARN da trilha. Sempre que possível, use `aws:SourceArn`, que é mais específico. Defina o valor como o ARN ou um padrão de ARN com caracteres curinga. Se você não conhece o ARN do recurso, use `aws:SourceAccount` em vez disso.

> **Note**
>
> Se um ARN de recurso incluir caracteres que não são permitidos em uma política de AWS KMS chave, você não pode usar esse ARN de recurso no valor da chave de condição. `aws:SourceArn` Em vez disso, use a chave de condição `aws:SourceAccount`. Para obter detalhes sobre as regras de documento de política de chaves, consulte Formato de política de chaves.

No exemplo de política de chaves a seguir, a entidade principal que obtém as permissões é a entidade principal do serviço AWS CloudTrail , `cloudtrail.amazonaws.com`. Para implementar o privilégio mínimo, essa política usa as chaves de condição `aws:SourceArn` e `kms:EncryptionContext:`*`context-key`*. A declaração de política permite CloudTrail usar a chave KMS para gerar a chave de dados que ela usa para criptografar uma trilha. As condições `aws:SourceArn` e `kms:EncryptionContext:`*`context-key`* são avaliadas de forma independente. Qualquer solicitação para usar a chave do KMS para a operação especificada deve atender às duas condições.

Para restringir a permissão do serviço à trilha `finance` na conta de exemplo (111122223333) e na região `us-west-2`, esta declaração de política define a chave de condição `aws:SourceArn` como o ARN de uma trilha específica. A declaração de condição usa o ArnEqualsoperador para garantir que cada elemento no ARN seja avaliado de forma independente durante a correspondência. O exemplo também usa a chave de condição `kms:EncryptionContext:`*`context-key`* para limitar a permissão a trilhas em uma determinada conta e região.

Antes de usar essa política de chaves, substitua os valores de ID da conta, região e nome da trilha de exemplo por valores válidos da sua conta.

```
{
  "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/*"
          ]
        }
      }
    }
  ]
}
```

Usando políticas do IAM com AWS KMS

Você pode usar as políticas do IAM, junto com as principais políticas, concessões e políticas de VPC endpoint, para controlar o acesso à sua entrada. AWS KMS keys AWS KMS

> **Note**
>
> Para usar uma política do IAM para controlar o acesso a uma chave do KMS, a política de chaves da chave do KMS deve conceder à conta permissão para usar políticas do IAM. Especificamente, a política de chaves deve incluir a instrução de política que habilita políticas do IAM.
>
> Esta seção explica como usar as políticas do IAM para controlar o acesso às AWS KMS operações. Para obter informações mais gerais sobre permissões do IAM, consulte o Manual do usuário do IAM.

Todas chaves do KMS do KMS têm uma política de chaves. Políticas do IAM são opcionais. Para usar uma política do IAM para controlar o acesso a uma chave do KMS, a política de chaves da chave do KMS deve conceder à conta permissão para usar políticas do IAM. Especificamente, a política de chaves deve incluir a instrução de política que habilita políticas do IAM.

As políticas do IAM podem controlar o acesso a qualquer AWS KMS operação. Diferentemente das políticas de chaves, as políticas do IAM podem controlar o acesso a várias chaves do KMS e fornecer permissões para as operações de vários AWS serviços relacionados. Mas as políticas do IAM são particularmente úteis para controlar o acesso a operações CreateKey, como aquelas que não podem ser controladas por uma política de chaves porque não envolvem nenhuma chave KMS específica.

Se você acessar AWS KMS por meio de um endpoint da Amazon Virtual Private Cloud (Amazon VPC), você também pode usar uma política de endpoint de VPC para limitar o acesso aos seus AWS KMS recursos ao usar o endpoint. Por exemplo, ao usar o VPC endpoint, você pode permitir que apenas os principais acessem suas Conta da AWS chaves gerenciadas pelo cliente. Para obter detalhes, consulte Controlar o acesso a um endpoint da VPC.

Para ajuda sobre como escrever e formatar um documento de política JSON, consulte aReferência a políticas JSON do IAM, no Manual do usuário do IAM.

Tópicos

- Visão geral de políticas do IAM
- Práticas recomendadas para políticas do IAM
- Especificando chaves do KMS em instruções de políticas do IAM
- Permissões necessárias para usar o AWS KMS console
- AWS política gerenciada para usuários avançados
- Exemplos de política do IAM

Visão geral de políticas do IAM

Use as políticas do IAM das seguintes maneiras:

- Anexar uma política de permissões a uma função de federação ou a permissões entre contas – Você pode anexar uma política do IAM a uma função do IAM para permitir a federação de identidades, conceder permissões entre contas ou a aplicações em execução nas instâncias do

EC2. Para mais informações sobre os vários casos de uso das funções do IAM, consulte Funções do IAM no Manual do usuário do IAM.

- Vincular uma política de permissões a um usuário ou a um grupo: é possível vincular uma política que permite que um usuário ou um grupo de usuários chame operações do AWS KMS . No entanto, as práticas recomendadas do IAM recomendam usar identidades com credenciais temporárias, como perfis do IAM, sempre que possível.

O exemplo a seguir mostra uma política do IAM com AWS KMS permissões. Essa política permite que as identidades do IAM às quais está associada obtenham todas as chaves do KMS e aliases.

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

Como todas as políticas do IAM, essa política não tem um elemento `Principal`. Quando você vincula uma política do IAM a uma identidade do IAM, essa identidade obtém as permissões especificadas na política.

Para ver uma tabela mostrando todas as ações da AWS KMS API e os recursos aos quais elas se aplicam, consulte Referência de permissões o.

Práticas recomendadas para políticas do IAM

Proteger o acesso ao AWS KMS keys é fundamental para a segurança de todos os seus AWS recursos. As chaves KMS são usadas para proteger muitos dos recursos mais confidenciais do seu Conta da AWS. Aproveite o tempo para projetar as políticas de chave, as políticas do IAM, as concessões e políticas de endpoint da VPC que controlam o acesso às chaves do KMS.

Em instruções de políticas do IAM que controlam o acesso a chaves do KMS, use o princípio de menor privilégio. Conceda às entidades principais do IAM somente as permissões de que eles precisam somente nas chaves do KMS que elas devem usar ou gerenciar.

As práticas recomendadas a seguir se aplicam às políticas do IAM que controlam o acesso a AWS KMS chaves e aliases. Para obter uma orientação geral sobre as práticas recomendadas da política do IAM, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

Usar políticas de chaves

Sempre que possível, conceda permissões em políticas de chaves que afetem uma chave do KMS, em vez de em uma política do IAM que possa ser aplicada a muitas chaves do KMS, incluindo aquelas em outras Contas da AWS. Isso é particularmente importante para permissões confidenciais, como kms: PutKeyPolicy e kms:, ScheduleKeyDeletion mas também para operações criptográficas que determinam como seus dados são protegidos.

Limitar CreateKey a permissão

Dê permissão para criar chaves (kms: CreateKey) somente aos diretores que precisarem delas. Entidades principais que criam uma chave do KMS também definem sua política de chave, para que possam conceder a si mesmas e a outros permissão para usar e gerenciar as chaves do KMS criadas. Ao conceder essa permissão, considere limitá-la usando condições de política. Por exemplo, você pode usar a KeySpec condição kms: para limitar a permissão às chaves KMS de criptografia simétrica.

Especificar chaves do KMS em uma política do IAM

Como prática recomendada, especifique o ARN da chave de cada chave do KMS à qual a permissão se aplica no elemento `Resource` da instrução de política. Esta prática restringe a permissão a chaves do KMS necessárias para a entidade principal. Por exemplo, esse elemento `Resource` lista apenas as chaves do KMS que a entidade principal precisa usar.

```
"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"
]
```

Quando especificar chaves KMS for impraticável, use um `Resource` valor que limite o acesso às chaves KMS em uma região confiável, Conta da AWS como. `arn:aws:kms:region:account:key/*` Ou limite o acesso às chaves KMS em todas as regiões (*) de uma rede confiável Conta da AWS, como`arn:aws:kms:*:account:key/*`.

Não é possível usar um ID de chave, um nome do alias ou ARN de alias para representar uma chave do KMS no campo `Resource` de uma política do IAM. Se você especificar um ARN de

alias, a política se aplicará ao alias, e não à chave do KMS. Para obter informações gerais sobre políticas do IAM para aliases, consulte Controlar o acesso a aliases

Evite "Resource": "*" em uma política do política do IAM

Use caracteres curinga (*) com critério. Em uma política de chaves, o caractere curinga no elemento `Resource` representa a chave do KMS à qual a política de chaves está associada. Mas em uma política do IAM, um caractere curinga sozinho no `Resource` elemento (`"Resource": "*"`) aplica as permissões a todas as chaves do KMS em tudo o Contas da AWS que a conta do diretor tem permissão para usar. Isso pode incluir chaves KMS em outras Contas da AWS, bem como chaves KMS na conta do diretor.

Por exemplo, para usar uma chave KMS em outra Conta da AWS, um principal precisa da permissão da política de chaves da chave KMS na conta externa e de uma política do IAM em sua própria conta. Suponha que uma conta arbitrária concedeu permissão à sua Conta da AWS kms:Decrypt em suas . Em caso afirmativo, uma política do IAM na sua conta que dê acesso uma função com permissão `kms:Decrypt` em todas as chaves do KMS (`"Resource": "*"`) atenderá à parte do IAM do requisito. Como resultado, as entidades principais que podem assumir essa função agora podem descriptografar textos cifrados usando a chave do KMS na conta não confiável. As entradas de suas operações aparecem nos CloudTrail registros de ambas as contas.

Especificamente, evite usar `"Resource": "*"` em uma declaração de política que permita as operações de API a seguir. Essas operações podem ser chamadas em chaves KMS em outras Contas da AWS.

- DescribeKey
- GetKeyRotationStatus
- Operações criptográficas (criptografar, descriptografar,,,,, GenerateDataKey,, GenerateDataKeyPair, GenerateDataKeyWithoutPlaintextassinar GenerateDataKeyPairWithoutPlaintextGetPublicKey, ReEncryptverificar)
- CreateGrant, ListGrants, ListRetirableGrants, RetireGrant, RevokeGrant

Quando usar "Resource": "*"

Em uma política do IAM, use um caractere curinga no elemento `Resource` somente para permissões que o exijam. Somente as permissões a seguir exigem o elemento `"Resource": "*"`.

- kms: CreateKey

- kms: GenerateRandom
- kms: ListAliases
- kms: ListKeys
- Permissões para armazenamentos de chaves personalizadas, como kms: CreateCustomKeyStore e kms:. ConnectCustomKeyStore

> **Note**
>
> As permissões para operações de alias (kms: CreateAlias, kms:UpdateAlias, kms: DeleteAlias) devem ser anexadas ao alias e à chave KMS. É possível usar `"Resource": "*"` em uma política do IAM para representar os aliases e as chaves do KMS, ou especificar os aliases e as chaves do KMS no elemento `Resource`. Para ver exemplos, consulte Controlar o acesso a aliases.

Os exemplos deste tópico fornecem mais informações e orientações para criar políticas do IAM para chaves do KMS. Para obter orientações gerais sobre AWS KMS as melhores práticas, consulte as AWS Key Management Service Melhores Práticas (PDF). Para ver as melhores práticas do IAM para todos os AWS recursos, consulte as melhores práticas de segurança no IAM no Guia do usuário do IAM.

Especificando chaves do KMS em instruções de políticas do IAM

É possível usar uma política do IAM para permitir que uma entidade principal use ou gerencie chaves do KMS. Chaves do KMS são especificadas no elemento `Resource` da instrução de política.

- Para especificar uma chave do KMS em uma instrução de política do IAM, use seu ARN de chave. Não é possível usar um ID de chave, um nome de alias nem um ARN de alias para identificar uma chave do KMS em uma instrução de política do IAM.

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

  Para controlar o acesso a uma chave KMS com base em seus aliases, use as chaves de condição kms: RequestAlias ou kms:. ResourceAliases Para obter detalhes, consulte ABAC para AWS KMS.

Use um alias ARN como recurso somente em uma declaração de política que controle o acesso às operações de alias, CreateAliascomo UpdateAlias, ou. DeleteAlias Para obter detalhes, consulte Controlar o acesso a aliases.

- Para especificar várias chaves do KMS na conta e região, use caracteres curinga (*) nas posições de Região ou ID de recurso do ARN de chave.

  Por exemplo, para especificar todas as chaves do KMS na região Oeste dos EUA (Oregon) de uma conta, use "`Resource": "arn:aws:kms:us-west-2:111122223333:key/*`". Para especificar todas as chaves do KMS em todas as regiões da conta, use "`Resource": "arn:aws:kms:*:111122223333:key/*`".
- Para representar todas as chaves do KMS, use um caractere curinga sozinho ("`*`"). Use esse formato para operações que não usam nenhuma chave KMS específica, a saber CreateKeyGenerateRandom, ListAliases, e. ListKeys

Ao escrever suas instruções de política, é uma prática recomendada limitar as chaves do KMS àquelas que as entidades principais precisam usar, em vez de conceder acesso a todas as chaves do KMS.

Por exemplo, a declaração de política do IAM a seguir permite que o diretor chame as operações DescribeKeyGenerateDataKey,, Decrypt somente nas chaves KMS listadas no `Resource` elemento da declaração de política. Especificar chaves do KMS por ARN de chave, que é uma prática recomendada, garante que as permissões sejam limitadas apenas às chaves do KMS especificadas.

```
{
  "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"
    ]
  }
}
```

Para aplicar a permissão a todas as chaves KMS em um determinado local confiável Conta da AWS, você pode usar caracteres curinga (*) na região e nas posições de ID da chave. Por exemplo, a instrução de política a seguir permite que a entidade principal chame as operações especificadas em quaisquer chaves do KMS em duas contas confiáveis demonstrativas.

```
{
  "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/*"
    ]
  }
}
```

Também é possível usar um caractere curinga ("*") sozinho no elemento `Resource`. Como ela permite o acesso a todas as chaves do KMS que a conta tem permissão para usar, é recomendável principalmente para operações que não envolvam uma chaves do KMS específica e para instruções `Deny`. Você também pode usá-lo em declarações de política que permitam apenas operações somente leitura menos confidenciais. Para determinar se uma AWS KMS operação envolve uma chave KMS específica, procure o valor da chave KMS na coluna Recursos da tabela em. the section called “Referência de permissões”

Por exemplo, a instrução de política a seguir usa um efeito `Deny` para proibir as entidades principais de usar as operações especificadas em qualquer chave do KMS. Ela usa um caractere curinga no elemento `Resource` para representar todas as chaves do KMS.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Deny",
    "Action": [
      "kms:CreateKey",
      "kms:PutKeyPolicy",
      "kms:CreateGrant",
```

```
      "kms:ScheduleKeyDeletion"
    ],
    "Resource": "*"
  }
}
```

A instrução de política a seguir usa um caractere curinga isoladamente para representar todas as chaves do KMS. Porém, ela permite apenas operações menos confidenciais somente leitura e operações que não se aplicam a uma chave do KMS específica.

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

Permissões necessárias para usar o AWS KMS console

Para trabalhar com o AWS KMS console, os usuários devem ter um conjunto mínimo de permissões que lhes permita trabalhar com os AWS KMS recursos em seu Conta da AWS. Além dessas permissões do AWS KMS , os usuários precisam ter também permissões para listar usuários do IAM e perfis do IAM. Se você criar uma política do IAM que seja mais restritiva do que as permissões mínimas exigidas, o AWS KMS console não funcionará conforme o esperado para os usuários com essa política do IAM.

Para obter as permissões mínimas necessárias para conceder ao usuário acesso somente leitura ao console do AWS KMS , consulte Permitir que um usuário visualize as chaves KMS no console AWS KMS.

Para permitir que os usuários trabalhem com o AWS KMS console para criar e gerenciar chaves KMS, anexe a política AWSKeyManagementServicePowerUsergerenciada ao usuário, conforme descrito na seção a seguir.

Não é necessário habilitar permissões mínimas do console para usuários que estão trabalhando com a API do AWS KMS por meio de AWS SDKs, AWS Command Line Interface ou AWS Tools for PowerShell. No entanto, você precisa conceder permissão a esses usuários para usar a API. Para ter mais informações, consulte Referência de permissões.

AWS política gerenciada para usuários avançados

É possível usar a política gerenciada pela `AWSKeyManagementServicePowerUser` para conceder às entidades principais do IAM em sua conta as permissões de um usuário avançado. Usuários avançados podem criar chaves do KMS, usar e gerenciar as chaves do KMS que eles criam e visualizar todas as chaves do KMS e identidades do IAM. Entidades principais que têm a política gerenciada `AWSKeyManagementServicePowerUser` também podem obter permissões de outras origens, incluindo políticas de chave, outras políticas do IAM e concessões.

`AWSKeyManagementServicePowerUser`é uma política AWS gerenciada do IAM. Para obter mais informações sobre políticas AWS gerenciadas, consulte políticas AWS gerenciadas no Guia do usuário do IAM.

> **Note**
>
> As permissões nessa política que são específicas para uma chave do KMS, como `kms:TagResource` e`kms:GetKeyRotationStatus`, só são efetivas quando a política de chaves dessa chave do KMS permite explicitamente o uso de políticas do IAM Conta da AWS para controlar o acesso à chave. Para determinar se uma permissão é específica para uma chave do KMS, consulte AWS KMS permissões e procure um valor de KMS key (Chave do KMS) na coluna Resources (Recursos).
>
> Essa política concede a um usuário avançado permissões sobre qualquer chave do KMS com uma política de chave que permita a operação. Para permissões entre contas, como `kms:DescribeKey` e `kms:ListGrants`, isso pode incluir chaves do KMS em Contas da AWS não confiáveis. Para obter mais detalhes, consulte Práticas recomendadas para políticas do IAM e Permitir que usuários de outras contas usem uma chave do KMS. Para determinar se uma permissão é válida em chaves do KMS em outras contas, consulte AWS KMS permissões e procure por um valor Yes (Sim) na coluna Cross-account use (Uso entre contas).
>
> Para permitir que os diretores visualizem o AWS KMS console sem erros, o diretor precisa da tag: GetResources permission, que não está incluída na

`AWSKeyManagementServicePowerUser` política. Você pode permitir essa permissão em uma política do IAM separada.

A política AWSKeyManagementServicePowerUsergerenciada do IAM inclui as seguintes permissões.

- Permite que as entidades principais criem chaves do KMS. Como esse processo inclui a definição da política de chaves, os usuários avançados podem conceder a si mesmos e a outros permissão para usar e gerenciar as chaves do KMS criadas por eles.
- Permite que as entidades principais criem e excluam aliases e tags em todas as chaves do KMS. Alterar uma etiqueta ou um alias pode conceder ou negar uma permissão para usar e gerenciar a chave do KMS. Para obter detalhes, consulte ABAC para AWS KMS.
- Permite que as entidades principais obtenham informações detalhadas sobre todas as chaves do KMS, incluindo seu ARN de chave, configuração criptográfica, política de chaves, aliases, tags e status de alternância.
- Permite que as entidades principais listem usuários, grupos e funções do IAM.
- Essa política não permite que as entidades principais usem nem gerenciem chaves do KMS não criadas por eles. No entanto, eles podem alterar aliases e tags em todas as chaves do KMS, o que pode permitir ou negar permissão para usar ou gerenciar uma chave do 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": "*"
        }
    ]
}
```

Exemplos de política do IAM

Nesta seção, você pode encontrar exemplos de políticas do IAM que concedem permissões para várias ações do AWS KMS .

> **Important**
>
> Algumas permissões das políticas a seguir são concedidas somente quando a política de chaves da chave do KMS também as concede. Para ter mais informações, consulte Referência de permissões.

Para ajuda sobre como escrever e formatar um documento de política JSON, consulte aReferência a políticas JSON do IAM, no Manual do usuário do IAM.

Exemplos

- Permitir que um usuário visualize as chaves KMS no console AWS KMS
- Permitir que um usuário crie chaves do KMS
- Permitir que um usuário criptografe e descriptografe com qualquer chave KMS em um local específico Conta da AWS
- Permitir que um usuário criptografe e descriptografe com qualquer chave KMS em uma região específica Conta da AWS
- Permitir que um usuário criptografe e descriptografe com chaves do KMS específicas
- Impedir que um usuário desabilite ou exclua qualquer chave do KMS

Permitir que um usuário visualize as chaves KMS no console AWS KMS

A política do IAM a seguir permite que os usuários tenham acesso somente de leitura ao AWS KMS console. Os usuários com essas permissões podem visualizar todas as chaves KMS em suas Conta da AWS, mas não podem criar ou alterar nenhuma chave KMS.

Para visualizar as chaves KMS nas páginas de chaves gerenciadas pelo cliente Chaves gerenciadas pela AWSe pelas páginas de chaves gerenciadas pelo clienteListKeys, os diretores exigem as GetResources permissões kms: ListAliases, kms: e tag:, mesmo que as chaves não tenham tags ou aliases. As permissões restantes, especialmente kms: DescribeKey, são necessárias para visualizar colunas e dados opcionais da tabela de chaves KMS nas páginas de detalhes da chave KMS. As ListRoles permissões iam: ListUsers e iam: são necessárias para exibir a política de chaves na visualização padrão sem erros. Para visualizar dados na página Armazenamentos de chaves personalizadas e detalhes sobre chaves KMS em armazenamentos de chaves personalizadas, os diretores também precisam da permissão kms:. DescribeCustomKeyStores

Se você limitar o acesso do console de um usuário a chaves do KMS específicas, o console exibirá um erro para cada chave do KMS que não estiver visível.

Essa política inclui duas declarações de política. O elemento `Resource` na primeira instrução de política habilita as permissões especificadas em todas as chaves do KMS em todas as regiões da Conta da AWS de exemplo. Os visualizadores do console não precisam de acesso adicional porque o console do AWS KMS exibe somente chaves do KMS na conta da entidade principal. Isso é verdade mesmo que eles tenham permissão para visualizar as chaves KMS em outros Contas da AWS. As permissões restantes AWS KMS e do IAM exigem um `"Resource": "*"` elemento porque não se aplicam a nenhuma chave KMS específica.

```
{
  "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": "*"
    }
  ]
}
```

Permitir que um usuário crie chaves do KMS

A seguinte política do IAM permite que um usuário crie todos os tipos de chaves do KMS. O valor do `Resource` elemento é * porque a `CreateKey` operação não usa nenhum AWS KMS recurso específico (chaves ou aliases do KMS).

Para restringir o usuário a tipos específicos de chaves KMS, use as chaves de condição kms: KeySpec, kms: KeyUsage e kms:. KeyOrigin

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "kms:CreateKey",
    "Resource": "*"
  }
}
```

As entidades principais que criam chaves podem precisar de algumas permissões relacionadas.

- kms: PutKeyPolicy — Os diretores que têm `kms:CreateKey` permissão podem definir a política inicial de chaves para a chave KMS. No entanto, o `CreateKey` chamador deve ter a PutKeyPolicy permissão kms:, que permite alterar a política de chaves do KMS, ou deve especificar o `BypassPolicyLockoutSafetyCheck` parâmetro de`CreateKey`, o que não é recomendado. O autor da chamada `CreateKey` pode obter a permissão `kms:PutKeyPolicy` para a chave do KMS a partir de uma política do IAM ou incluir essa permissão na política de chaves da chave do KMS que ele está criando.
- kms: TagResource — Para adicionar tags à chave KMS durante a `CreateKey` operação, o `CreateKey` chamador deve ter a TagResource permissão kms: em uma política do IAM. Não é

suficiente incluir essa permissão na política de chaves da nova chave do KMS. No entanto, se o autor da chamada `CreateKey` incluir `kms:TagResource` na política de chaves inicial, ele poderá adicionar etiquetas a uma chamada separada após a criação da chave do KMS.

- kms: CreateAlias — Os diretores que criam uma chave KMS no AWS KMS console devem ter a CreateAlias permissão kms: na chave KMS e no alias. (O console faz duas chamadas; uma para `CreateKey` e outra para `CreateAlias`). É necessário fornecer a permissão de alias em uma política do IAM. É possível fornecer a permissão da chave do KMS em uma política de chave ou política do IAM. Para obter detalhes, consulte Controlar o acesso a aliases.

Além dissokms:CreateKey, a política do IAM a seguir fornece `kms:TagResource` permissão para todas as chaves KMS na Conta da AWS e `kms:CreateAlias` permissão para todos os aliases da conta. Ela também inclui algumas permissões úteis somente leitura que podem ser fornecidas somente em uma política do IAM.

Essa política do IAM não inclui a permissão `kms:PutKeyPolicy` nem outras permissões que possam ser definidas em uma política de chaves. Uma prática recomendada é definir essas permissões na política de chaves em que elas se aplicam exclusivamente a uma chave do 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": "*"
    }
  ]
}
```

Permitir que um usuário criptografe e descriptografe com qualquer chave KMS em um local específico Conta da AWS

A política do IAM a seguir permite que um usuário criptografe e descriptografe dados com qualquer chave KMS em 111122223333. Conta da AWS

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

Permitir que um usuário criptografe e descriptografe com qualquer chave KMS em uma região específica Conta da AWS

A política do IAM a seguir permite que um usuário criptografe e descriptografe dados com qualquer chave KMS Conta da AWS 111122223333 na região Oeste dos EUA (Oregon).

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "kms:Encrypt",
      "kms:Decrypt"
    ],
    "Resource": [
      "arn:aws:kms:us-west-2:111122223333:key/*"
    ]
```

```
  }
}
```

Permitir que um usuário criptografe e descriptografe com chaves do KMS específicas

A política do IAM a seguir permite que um usuário criptografe e descriptografe dados com as duas chaves do KMS especificadas no elemento `Resource`. Ao especificar uma chave do KMS em uma instrução de política do IAM, você deve usar o ARN de chave dessa chave do 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"
    ]
  }
}
```

Impedir que um usuário desabilite ou exclua qualquer chave do KMS

A política do IAM a seguir impede que um usuário desabilite ou exclua chaves do KMS, mesmo quando outra política do IAM ou uma política de chaves concede essas permissões. Uma política que nega explicitamente permissões substitui todas as outras políticas, mesmo aquelas que concedem explicitamente as mesmas permissões. Para ter mais informações, consulte Solucionar problemas de acesso à chave.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Deny",
    "Action": [
      "kms:DisableKey",
      "kms:ScheduleKeyDeletion"
    ],
    "Resource": "*"
  }
```

```
}
```

Concessões no AWS KMS

Uma concessão é um instrumento de política que permite que as entidades principais da AWS usem chaves do KMS em operações de criptografia. Ela também pode permitir que essas entidades visualizem uma chave do KMS (`DescribeKey`) e criem e gerenciem concessões. Ao autorizar o acesso a uma chave do KMS, concessões são consideradas junto com políticas de chave e políticas do IAM. Concessões geralmente são usadas para permissões temporárias, pois você pode criar uma, usar suas permissões e excluí-la sem alterar suas principais políticas ou políticas do IAM.

Concessões são comumente usadas por serviços da AWS que se integram ao AWS KMS para criptografar seus dados em repouso. O serviço cria uma concessão em nome de um usuário na conta, usa suas permissões e desativa a concessão assim que sua tarefa é concluída. Para obter detalhes sobre como os serviçosda AWS usam concessões, consulte Como os serviços da AWS, usam o AWS KMS ou o tópico Criptografia em repouso no manual do usuário ou no guia do desenvolvedor do serviço.

Para exemplos de código que demonstram como trabalhar com subsídios em várias linguagens de programação, consulte Trabalhar com concessões.

Tópicos

- Sobre concessões
- Conceitos sobre concessões
- Práticas recomendadas para concessões do AWS KMS
- Criar concessões
- Gerencias concessões

Sobre concessões

Concessões são um mecanismo de controle de acesso muito flexível e útil. Quando você cria uma concessão para uma chave do KMS, essa concessão permite que a entidade principal autorizada chame as operações de concessão especificadas na chave do KMS, desde que todas as condições especificadas na concessão sejam atendidas.

- Cada concessão permite o acesso a exatamente uma chave do KMS. Você pode criar uma concessão para uma chave do KMS em uma Conta da AWS diferente.

- Uma concessão pode permitir acesso a uma chave do KMS, mas não pode negar acesso.
- Cada concessão tem uma entidade principal autorizada. A entidade principal autorizada pode representar uma ou mais identidades na mesma Conta da AWS como a chave do KMS ou em uma conta diferente.
- Uma concessão só pode permitir operações de concessão. Operações de concessão devem ter suporte pela chave do KMS na concessão. Se você especificar uma operação sem suporte, a CreateGrantsolicitação falhará com uma `ValidationError` exceção.
- A entidade principal autorizada pode usar as permissões autorizadas pela concessão sem especificar a concessão, exatamente como fariam se as permissões fossem provenientes de uma política de chave ou de uma política do IAM. No entanto, como a API do AWS KMS segue um modelo de consistência eventual, quando você cria, retira ou revoga uma concessão, pode haver um breve atraso antes que a alteração esteja disponível em todo o AWS KMS. Para usar as permissões em uma concessão imediatamente, use um token de concessão.
- Uma entidade principal autorizada pode excluir a concessão (retirar ou revogar a concessão). A exclusão de uma concessão elimina todas as permissões permitidas por ela. Você não precisa descobrir quais políticas adicionar ou remover para desfazer a concessão.
- A AWS KMS limita o número de concessões em cada chave do KMS. Para obter detalhes, consulte Concessões por chave do KMS: 50.000.

Tenha cautela ao criar concessões e ao dar permissão a outras pessoas para criar concessões. A permissão para criar concessões tem implicações de segurança, assim como permitir que o kms:PutKeyPolicy defina políticas.

- Usuários com permissão para criar concessões para uma chave do KMS (`kms:CreateGrant`) podem usar uma concessão para permitir que usuários e funções, incluindo serviços da AWS, usem a chave do KMS. As entidades principais podem ser identidades na sua própria Conta da AWS ou identidades em uma conta ou organização diferente.
- Concessões podem permitir apenas um subconjunto de operações da AWS KMS. É possível usar concessões para permitir que as entidades principais exibam a chave do KMS, usá-la em operações de criptografia e criar e retirar concessões. Para obter mais detalhes, consulte Operações de concessão. Você também pode usar restrições de concessão para limitar as permissões em uma concessão para uma chave de criptografia simétrica.
- As entidades principais podem obter permissão para criar concessões a partir de uma política de chave ou de uma política do IAM. Entidades principais que recebem a permissão `kms:CreateGrant` de uma política podem criar concessões para qualquer operação de

concessão na chave do KMS. Essas entidades principais não precisam ter a permissão que estão concedendo na chave. Quando você concede a permissão `kms:CreateGrant` em uma política, pode usar condições de políticas para limitar essa permissão.

- As entidades principais também podem obter permissão para criar concessões de uma concessão. Essas entidades principais só podem delegar as permissões que lhes foram concedidas, mesmo que tenham outras permissões de uma política. Para obter detalhes, consulte Concedendo permissão CreateGrant .

Para obter ajuda com conceitos relacionados a concessões, consulte a Terminologia de concessões.

Conceitos sobre concessões

Para usar concessões de maneira eficaz, você precisa entender os termos e conceitos que são usados pela AWS KMS.

Restrições de concessão

Uma condição que limita as permissões na concessão. No momento, o AWS KMS oferece suporte a restrições de concessão com base nocontexto de criptografia na solicitação de operação criptográfica. Para obter detalhes, consulte Usar restrições de concessão.

ID de concessão

O identificador exclusivo de uma concessão para uma chave do KMS. Você pode usar uma ID de concessão, junto com um identificador de chave, para identificar uma concessão em uma RevokeGrantsolicitação RetireGrantor.

Operações de concessão

As operações do AWS KMS que você pode permitir em uma concessão. Se você especificar outras operações, a CreateGrantsolicitação falhará com uma `ValidationError` exceção. Estas são também as operações que aceitam um token de concessão. Para obter informações detalhadas sobre essas permissões, consulte a AWS KMS permissões.

Essas operações de concessão realmente representam permissão para usar a operação. Portanto, para a operação `ReEncrypt`, você pode especificar `ReEncryptFrom`, `ReEncryptTo` ou ambos `ReEncrypt*`.

As operações de concessão são:

- Operações criptográficas

  - Decrypt
  - Encrypt
  - GenerateDataKey
  - GenerateDataKeyPair
  - GenerateDataKeyPairWithoutPlaintext
  - GenerateDataKeyWithoutPlaintext
  - GenerateMac
  - ReEncryptFrom
  - ReEncryptTo
  - Sign
  - Verificar
  - VerifyMac
- Outras operações
  - CreateGrant
  - DescribeKey
  - GetPublicKey
  - RetireGrant

As operações de concessão permitidas devem ter suporte pela chave do KMS na concessão. Se você especificar uma operação sem suporte, a CreateGrantsolicitação falhará com uma `ValidationError` exceção. Por exemplo, concessões para chaves do KMS de criptografia simétrica não podem permitir as operações Sign (Assinar), Verify (Verificar), `GenerateMac` ou `VerifyMac`. As concessões para chaves assimétricas do KMS não podem permitir nenhuma operação que gere chaves de dados ou pares de chaves de dados.

Token de concessão

A API do AWS KMS segue o modelo de consistência eventual. Quando você cria uma concessão, pode haver um breve atraso antes que a alteração esteja disponível em todo o AWS KMS. Normalmente, a alteração leva menos de alguns segundos para se propagar por todo o sistema, mas, em alguns casos, pode levar vários minutos. Se você tentar usar uma concessão antes de ela se propagar totalmente pelo sistema, poderá obter um erro de acesso negado. Um token de concessão permite que você faça referência à concessão e use as permissões de concessão imediatamente.

Um token de concessão é uma string única, não secreta, de comprimento variável e codificada em base64 que representa uma concessão. Você pode usar o token de concessão para identificar a concessão em qualquer operação de concessão. No entanto, como o valor do token é um resumo de hash, ele não revela detalhes sobre a concessão.

Um token de concessão é projetado para ser usado somente até que a concessão seja totalmente propagada em todo o AWS KMS. Depois disso, a entidade principal receptora da concessão pode usar a permissão nessa concessão sem fornecer um token de concessão ou qualquer outra evidência da concessão. Você pode usar um token de concessão a qualquer momento. Porém, uma vez que a concessão for eventualmente consistente, o AWS KMS a usará para determinar permissões, e não o token de concessão.

Por exemplo, o comando a seguir chama a GenerateDataKeyoperação. Ele usa um token de concessão para representar a concessão que dá ao autor da chamada (a entidade principal receptora da concessão) permissão para chamar `GenerateDataKey` na chave do KMS especificada.

```
$ aws kms generate-data-key \
        --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
        --key-spec AES_256 \
        --grant-token $token
```

Também é possível pode usar um token de concessão para identificar uma concessão em operações que gerenciam concessões. Por exemplo, o diretor que está se aposentando pode usar um token de concessão em uma chamada para a RetireGrantoperação.

```
$ aws kms retire-grant \
        --grant-token $token
```

`CreateGrant` é a única operação que retorna um token de concessão. Você não pode obter um token de concessão de nenhuma outra AWS KMS operação ou do evento de CloudTrail log da CreateGrant operação. As ListRetirableGrantsoperações ListGrantse retornam o ID de concessão, mas não um token de concessão.

Para obter detalhes, consulte Usar um token de concessão.

Entidade principal receptora da concessão

As identidades que obtêm as permissões especificadas na concessão. Cada concessão tem uma entidade principal autorizada, mas a entidade principal autorizada pode representar várias identidades.

A entidade principal receptora da concessão pode ser qualquer entidade principal da AWS, incluindo uma Conta da AWS (root), um usuário do IAM, uma função do IAM, um usuário ou função federada ou um usuário de função assumida. A entidade principal receptora da concessão pode estar na mesma conta da que a chave do KMS ou uma conta diferente. No entanto, a entidade principal receptora da concessão não pode ser umaentidade principal do serviço, umgrupo do IAM ou umAWS organização.

> **Note**
>
> As práticas recomendadas do IAM não encorajam o uso de usuários do IAM com credenciais de longo prazo. Sempre que possível, use os perfis do IAM, por fornecerem credenciais temporárias. Para obter detalhes, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

Retira (uma concessão)

Encerra uma concessão. Você retira uma concessão ao terminar de usar as permissões.

A revogação e a retirada de uma concessão excluem essa concessão. No entanto, o processo é feito por uma entidade principal especificada na concessão. A revogação geralmente é feita por um administrador de chave. Para obter detalhes, consulte Retirar e revogar concessões.

Retirada da entidade principal

Uma entidade principal que pode retirar uma concessão. Você pode especificar uma entidade de retirada em uma concessão, mas ela não é necessária. A entidade principal de retirada pode ser qualquer entidade principal da AWS, incluindoContas da AWS, usuários do IAM, funções do IAM, usuários federados e usuários de funções assumidas. A entidade principal de retirada pode estar na mesma conta da que a chave do KMS ou uma conta diferente.

> **Note**
>
> As práticas recomendadas do IAM não encorajam o uso de usuários do IAM com credenciais de longo prazo. Sempre que possível, use os perfis do IAM, por fornecerem

credenciais temporárias. Para obter detalhes, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

Além da entidade principal de retirada especificada na concessão, uma concessão pode ser retirada pela Conta da AWS em que ela foi criada. Se a concessão permitir a operação `RetireGrant`, a entidade principal receptora da concessão poderá retirar a concessão. Além disso, a Conta da AWS ou uma Conta da AWSque seja a entidade principal de desativação pode delegar a permissão para retirar uma concessão a um principal do IAM no mesmoConta da AWS. Para obter detalhes, consulte Retirar e revogar concessões.

Revocar (uma concessão)

Encerra uma concessão. Você revoga uma concessão para negar ativamente as permissões que a concessão permite.

A revogação e a retirada de uma concessão excluem essa concessão. No entanto, o processo é feito por uma entidade principal especificada na concessão. A revogação geralmente é feita por um administrador de chave. Para obter detalhes, consulte Retirar e revogar concessões.

Consistência eventual (para concessões)

A API do AWS KMS segue o modelo de consistência eventual. Quando você cria, retira ou revoga uma concessão, pode haver um breve atraso antes que a alteração esteja disponível em todo o AWS KMS. Normalmente, a alteração leva menos de alguns segundos para se propagar por todo o sistema, mas, em alguns casos, pode levar vários minutos.

Você pode ter conhecimento desse breve atraso se receber erros inesperados. Por exemplo, se você tentar gerenciar uma nova concessão ou usar as permissões em uma nova concessão antes que a concessão seja conhecida emAWS KMSVocê pode obter um erro de acesso negado. Se você retirar ou revogar uma concessão, a entidade principal receptora da concessão ainda poderá usar suas permissões por um breve período até que a concessão seja totalmente excluída. A estratégia típica é tentar novamente a solicitação e alguns SDKs da AWS incluem a lógica automática de retirada e repetição.

O AWS KMS tem recursos para atenuar esse breve atraso.

- Para usar as permissões em uma nova concessão imediatamente, use um token de concessão. Você pode usar um token de concessão para fazer referência a uma concessão em qualquer operação de concessão. Para obter instruções, consulte Usar um token de concessão.

- A CreateGrantoperação tem um `Name` parâmetro que impede que operações de repetição criem concessões duplicadas.

> **Note**
>
> Os tokens de concessão substituem a validade da concessão até que todos os endpoints do serviço sejam atualizados com o novo estado de concessão. Na maioria dos casos, a consistência eventual será alcançada em cinco minutos.

Para obter informações, consulte consistência eventual do AWS KMS.

Práticas recomendadas para concessões do AWS KMS

O AWS KMS recomenda as seguintes práticas recomendadas ao criar, usar e gerenciar concessões.

- Limite as permissões na concessão àquelas que são exigidas pela entidade principal receptora da concessão. Use o princípio de acesso com menos privilégio.
- Use uma entidade principal receptora da concessão específica, como uma função do IAM, e dê a ela permissão para usar somente as operações de API necessárias.
- Use restrições de concessão do contexto de criptografia para garantir que os autores de chamadas estejam usando a chave do KMS para o propósito pretendido. Para obter detalhes sobre como usar o contexto de criptografia em uma solicitação para proteger seus dados, consulte Como proteger a integridade de seus dados criptografados usando AWS Key Management Service e EncryptionContext no blog AWS de segurança.

> **Tip**
>
> Use a restrição de EncryptionContextEqualconcessão sempre que possível. A restrição de EncryptionContextSubsetconcessão é mais difícil de usar corretamente. Se precisar usá-la, leia atentamente a documentação e teste a restrição de concessão para se certificar de que ela funciona como pretendido.

- Exclua concessões duplicadas. Concessões duplicadas têm o mesmo ARN de chave, ações de API, entidade principal receptora da concessão, contexto de criptografia e nome. Se você retirar ou revogar a concessão original, mas deixar as duplicatas, as concessões duplicadas restantes constituirão escalonamentos não intencionais de privilégio. Para evitar duplicar concessões

ao tentar novamente uma solicitação `CreateGrant`, use o parâmetro `Name`. Para detectar concessões duplicadas, use a ListGrantsoperação. Se você criar acidentalmente uma concessão duplicada, retire ou revogue-a assim que possível.

> **Note**
>
> Concessões para chaves gerenciadas da AWS podem parecer duplicadas, mas têm diferentes entidades principais receptoras de concessão.
> O campo `GranteePrincipal` na resposta `ListGrants` geralmente contém o principal favorecido da concessão. No entanto, quando a entidade principal receptora na concessão é um serviço da AWS, o campo `GranteePrincipal` contém a entidade principal de serviço, que pode representar várias entidades principais entidade receptoras de concessão diferentes.

- Lembre-se de que as concessões não expiram automaticamente. Reitre ou revogue a concessão assim que a permissão não for mais necessária. Concessões que não forem excluídas podem criar riscos de segurança para recursos criptografados.

Criar concessões

Antes de criar uma concessão, saiba mais sobre as opções para personalizar sua concessão. Você pode usar restrições de concessão para limitar as permissões na concessão. Além disso, saiba mais sobre como conceder a permissão `CreateGrant`. As entidades principais que obtêm permissão para criar concessões a partir de uma concessão são limitados em termos das concessões que elas podem criar.

Tópicos

- Criar uma concessão
- Usar restrições de concessão
- Concedendo permissão CreateGrant

Criar uma concessão

Para criar uma concessão, chame a CreateGrantoperação. Especifique uma chave do KMS, uma entidade principal receptora da concessão e uma lista de operações de concessão. Você também

pode designar uma entidade principal de retirada opcional. Para personalizar a concessão, use parâmetros `Constraints` opcionais para definir as restrições de concessão

Quando você cria, retira ou revoga uma concessão, pode haver um breve atraso, geralmente menos de cinco minutos, antes que a alteração esteja disponível em todo o AWS KMS. Para obter informações, consulte Eventual consistency (for grants) (Consistência eventual (para concessões)).

Por exemplo, o comando `CreateGrant` a seguir cria uma concessão que permite que usuários que estão autorizados a assumir o perfil `keyUserRole` chamem a operação Decrypt na chave do KMS simétrica especificada. A concessão usa o parâmetro `RetiringPrincipal` para designar um principal que pode desativar a concessão. Ele também inclui uma restrição de concessão que concede a permissão somente quando o contexto de criptografia na solicitação inclui `"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 o seu código tentar novamente a operação `CreateGrant` ou usar umSDK da AWS que repete solicitações automaticamente, use o parâmetro Name opcional para impedir a criação de concessões duplicadas. Se o AWS KMS receber uma solicitação `CreateGrant` para uma concessão com as mesmas propriedades de uma concessão existente, incluindo o nome, ele reconhecerá a solicitação como uma nova tentativa e não criará uma nova concessão. Não é possível usar o valor `Name` para identificar a concessão em qualquer operação do AWS KMS.

> **Important**
>
> Não inclua informações confidenciais ou sigilosas no nome da concessão. Ele pode aparecer em texto simples em CloudTrail registros e outras saídas.

```
$ 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}
```

Para exemplos de código que demonstram como trabalhar com subsídios em várias linguagens de programação, consulte Trabalhar com concessões.

Usar restrições de concessão

Restrições de concessão definem condições para as permissões que a concessão fornece à entidade principal receptora da concessão. Restrições de concessão ocupam o lugar de chaves de condição em uma política de chaves ou política do IAM. Cada valor de restrição de concessão pode incluir até oito pares de contexto de criptografia. O valor do contexto de criptografia em cada restrição de concessão não pode exceder 384 caracteres.

> **Important**
>
> Não inclua informações confidenciais ou sigilosas nesse campo. Esse campo pode ser exibido em texto simples em CloudTrail registros e outras saídas.

O AWS KMS é compatível com duas restrições de concessão, `EncryptionContextEquals` e `EncryptionContextSubset`. Ambas estabelecem requisitos para o contexto de criptografia em uma solicitação de operação criptográfica.

As restrições de concessão de contexto de criptografia foram projetadas para serem usadas com operações de concessão que têm um parâmetro de contexto de criptografia.

- As restrições de contexto de criptografia são válidas somente em uma concessão para uma chave do KMS de criptografia simétrica. Operações criptográficas com outras chaves do KMS não são compatíveis com um contexto de criptografia.
- A restrição do contexto de criptografia é ignorada para operações `DescribeKey` e `RetireGrant`. `DescribeKey` e `RetireGrant` não têm um parâmetro de contexto de criptografia, mas você pode incluir essas operações em uma concessão que tenha uma restrição de contexto de criptografia.
- É possível usar uma restrição de contexto de criptografia em uma concessão para a operação `CreateGrant`. A restrição de contexto de criptografia requer que todas as concessões criadas com a permissão `CreateGrant` tenham uma restrição de contexto de criptografia igualmente rigorosa ou ainda mais rigorosa.

O AWS KMS oferece suporte às seguintes restrições de concessão de contexto de criptografia.

EncryptionContextEquals

Use `EncryptionContextEquals` para especificar o contexto de criptografia exato para solicitações permitidas.

`EncryptionContextEquals` requer que os pares de contexto de criptografia na solicitação sejam uma correspondência exata, com distinção entre maiúsculas e minúsculas, para os pares de contexto de criptografia na restrição de concessão. Os pares podem aparecer em qualquer ordem, mas as chaves e os valores em cada par não podem variar.

Por exemplo, se a restrição de concessão `EncryptionContextEquals` exigir o par de contexto de criptografia `"Department": "IT"`, a concessão permitirá solicitações do tipo especificado apenas quando o contexto de criptografia na solicitação for exatamente`"Department": "IT"`.

EncryptionContextSubset

Use `EncryptionContextSubset` para exigir que as solicitações incluam pares de contexto de criptografia específicos.

`EncryptionContextSubset` requer que a solicitação inclua todos os pares de contexto de criptografia na restrição de concessão (uma correspondência exata com distinção entre maiúsculas e minúsculas), mas a solicitação também pode conter pares de contexto de criptografia adicionais. Os pares podem aparecer em qualquer ordem, mas as chaves e os valores em cada par não podem variar.

Por exemplo, se a restrição de concessão `EncryptionContextSubset` exigir o par de contexto de criptografia `Department=IT`, a concessão permitirá solicitações do tipo especificado quando o contexto de criptografia na solicitação for `"Department": "IT"` ou incluir `"Department": "IT"` juntamente com outros pares de contexto de criptografia, como `"Department": "IT","Purpose": "Test"`.

Para especificar uma restrição de contexto de criptografia em uma concessão para uma chave KMS de criptografia simétrica, use o `Constraints` parâmetro na operação. CreateGrant A concessão que esse comando cria concede aos usuários que estão autorizados a assumir a permissão do perfil `keyUserRole` para chamar a operação Decrypt. Porém, essa permissão entrará em vigor somente quando o contexto de criptografia na solicitação `Decrypt` for um par de contexto de criptografia `"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}
```

A concessão resultante é semelhante à seguinte. Observe que a permissão concedida ao perfil `keyUserRole` entrará em vigor somente quando a solicitação `Decrypt` usar o mesmo par de contexto de criptografia especificado na restrição de concessão. Para encontrar as concessões em uma chave KMS, use a ListGrantsoperação.

```
$ 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"
        }
    ]
}
```

Para atender à restrição de concessão `EncryptionContextEquals`, o contexto de criptografia na solicitação para a operação `Decrypt` deve ser um par `"Department": "IT"`. Uma solicitação como a seguinte da entidade principal receptora da concessão atenderia à restrição de concessão `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 a restrição de concessão é `EncryptionContextSubset`, os pares de contexto de criptografia na solicitação devem incluir pares de contexto de criptografia na restrição de concessão, mas a solicitação também pode incluir outros pares de contexto de criptografia. A restrição de concessão a seguir exige que um dos pares de contexto de criptografia na solicitação seja `"Deparment": "IT"`.

```
"Constraints": {
   "EncryptionContextSubset": {
       "Department": "IT"
   }
}
```

A solicitação a seguir da entidade principal receptora da concessão atenderia a ambas as restrições de concessão `EncryptionContextEqual` e `EncryptionContextSubset` neste exemplo.

```
$ 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
```

No entanto, uma solicitação como o seguinte da entidade principal receptora da concessão atenderia a restrição de concessão `EncryptionContextSubset`, mas falharia na restrição de concessão `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
```

Os serviços da AWS geralmente usam restrições de contexto de criptografia nas concessões que dão a eles permissão para usar chaves do KMS em sua Conta da AWS. Por exemplo, o Amazon DynamoDB usa uma concessão, como a seguinte, para obter permissão de uso

da Chave gerenciada pela AWS para o DynamoDB na sua conta. A restrição de concessão `EncryptionContextSubset` nessa concessão colocará em vigor as permissões na concessão somente quando o contexto de criptografia na solicitação incluir os pares `"subscriberID": "111122223333"` e `"tableName": "Services"`. Essa restrição de concessão significa que a concessão permite que o DynamoDB use a chave do KMS especificada apenas para uma tabela específica na sua Conta da AWS.

Para obter essa saída, execute a ListGrantsoperação no Chave gerenciada pela AWS for DynamoDB em sua conta.

```
$ 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"
        }
    ]
}
```

Concedendo permissão CreateGrant

Uma concessão pode incluir permissão para chamar a operação `CreateGrant`. Porém, quando uma entidade principal receptora da concessão obtém permissão para chamar `CreateGrant` de uma concessão, em vez de uma política, essa permissão é limitada.

- A entidade principal receptora da concessão só pode criar concessões que permitam algumas ou todas as operações na concessão pai.
- As restrições de concessão nas concessões que elas criam devem ser pelo menos tão rigorosas quanto as contidos na concessão pai.

Essas limitações não se aplicam a entidades principais que obtêm a permissão `CreateGrant` de uma política, embora suas permissões possam ser limitadas por condições de política.

Por exemplo, considere uma concessão que permite que o principal favorecido chame as operações `GenerateDataKey`, `Decrypt` e `CreateGrant`. Chamamos uma concessão que aceita a permissão `CreateGrant` para uma concessão pai.

```
# 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"
                }
            },
```

```
        }
    ]
}
```

A entidade principal receptora da concessão, exampleUser, pode usar essa permissão para criar uma concessão que inclui qualquer subconjunto das operações especificadas na concessão original, como `CreateGrant` e `Decrypt`. A concessão filho não pode incluir outras operações, como `ScheduleKeyDeletion` ou `ReEncrypt`.

Além disso, as restrições de concessão nas concessões filho devem ser igualmente ou mais restritivas que as da concessão pai. Por exemplo, a concessão filho pode adicionar pares a uma restrição `EncryptionContextSubset` na concessão pai, mas não pode removê-los. A concessão filho pode alterar uma restrição `EncryptionContextSubset` para uma restrição `EncryptionContextEquals`, mas não o contrário.

Por exemplo, a entidade principal receptora da concessão pode usar a permissão `CreateGrant` que obteve da concessão pai para criar a seguinte concessão filho. As operações na concessão filho são um subconjunto das operações na concessão pai, e as restrições de concessão são mais restritivas.

```
# 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"
                }
            },
        }
    ]
}
```

A entidade principal receptora da concessão na concessão filho, `anotherUser`, pode usar a permissão `CreateGrant` para criar concessões. No entanto, as concessões criadas por `anotherUser` devem incluir as operações em sua concessão pai ou um subconjunto, e as restrições de concessão devem ser iguais ou mais rigorosas.

Gerencias concessões

Entidades principais com as permissões necessárias podem exibir, usar e excluir (retirar ou revogar) concessões. Para refinar permissões para criar e gerenciar concessões, o AWS KMS oferece suporte a várias condições de política que você pode usar em políticas de chave e políticas do IAM.

Tópicos

- Controlar o acesso a concessões
- Visualizar concessões
- Usar um token de concessão
- Retirar e revogar concessões

Controlar o acesso a concessões

Você pode controlar o acesso às operações que criam e gerenciam concessões em políticas de chaves, políticas do IAM e concessões. As entidades principais que recebem a permissão `CreateGrant` de uma concessão tem permissões de concessão mais limitadas.

Operação de API	Política de chaves ou política do IAM	Concessão
CreateGrant	✓	✓
ListGrants	✓	-

Operação de API	Política de chaves ou política do IAM	Concessão
ListRetirableGrants	✓	-
Retirar concessões	(Limitado. Consulte Retirar e revogar concessões)	✓
RevokeGrant	✓	-

Ao usar uma política de chaves ou uma política do IAM para controlar o acesso a operações que criam e gerenciam concessões, você pode usar uma ou mais das seguintes condições de política para limitar a permissão. O AWS KMS oferece suporte a todas as seguintes chaves de condição relacionadas a concessões. Para obter informações e exemplos detalhados, consulte AWS KMS chaves de condição.

kms: GrantConstraintType

Permite que as entidades principais criem uma concessão somente quando esta inclui a restrição de concessão especificada.

kms: GrantIsFor AWSResource

Permite que as entidades principais chamem `CreateGrant`, `ListGrants` ou `RevokeGrant` somente quando um serviço da AWS integrado ao AWS KMS envia a solicitação em nome da entidade principal.

kms: GrantOperations

Permite que as entidades principais criem uma concessão, mas limita a concessão às operações especificadas.

kms: GranteePrincipal

Permite que as entidades principais criem uma concessão somente para a entidade principal receptora da concessão.

kms: RetiringPrincipal

Permite que as entidades principais criem uma concessão somente quando esta especifica um entidade principal de retirada.

Visualizar concessões

Para visualizar a concessão, use a ListGrantsoperação. Você deve especificar a chave do KMS à qual as concessões se aplicam. Você também pode filtrar a lista de concessões por ID de concessão ou entidade principal receptora da concessão. Para obter mais exemplos, consulte Visualizar uma concessão.

Para ver todas as doações na Conta da AWS região com um determinado diretor aposentado, use ListRetirableGrants. As respostas incluem detalhes sobre cada concessão.

> **Note**
>
> O campo `GranteePrincipal` na resposta `ListGrants` geralmente contém o principal favorecido da concessão. No entanto, quando a entidade principal receptora na concessão é um serviço da AWS, o campo `GranteePrincipal` contém a entidade principal de serviço, que pode representar várias entidades principais entidade receptoras de concessão diferentes.

Por exemplo, o comando a seguir lista todas as concessões para uma chave do 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"
```

```
            ]
        }
    ]
}
```

Usar um token de concessão

A API do AWS KMS segue o modelo de consistência eventual. Ao criar uma concessão, esta pode não entrar em vigor imediatamente. Pode haver um breve atraso antes que a alteração esteja disponível em todo o AWS KMS. Normalmente, a alteração leva menos de alguns segundos para se propagar por todo o sistema, mas, em alguns casos, pode levar vários minutos. Uma vez que a alteração tenha se propagado em todo o sistema, a entidade principal receptora da concessão poderá usar as permissões na concessão sem especificar o token de concessão ou qualquer evidência da concessão. No entanto, se uma concessão for tão nova a ponto de ainda não ser conhecida pelo AWS KMS, a solicitação poderá falhar com um erro de `AccessDeniedException`.

Para usar as permissões em uma nova concessão imediatamente, use o token de concessão para a concessão. Salve o token de concessão que a CreateGrantoperação retorna. Em seguida, envie o token de concessão na solicitação para a operação AWS KMS. Você pode enviar um token de concessão para qualquer operação de concessão do AWS KMS e pode enviar vários tokens de concessão na mesma solicitação.

O exemplo a seguir usa a `CreateGrant` operação para criar uma concessão que permite as operações GenerateDataKeye Decrypt. Ele salva o token de concessão retornado por `CreateGrant` na variável `token`. Em seguida, em uma chamada para `GenerateDataKey`, ele usa o token de concessão na variável `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
```

As entidades principais com permissão também podem usar um token de concessão para retirar uma nova concessão mesmo antes que ela se torne disponível por meio do AWS KMS. (A operação `RevokeGrant` não aceita um token de concessão.) Para obter detalhes, consulte Retirar e revogar concessões.

```
# Retire the grant
$ aws kms retire-grant --grant-token $token
```

Retirar e revogar concessões

Para excluir uma concessão, retire-a ou revogue-a.

As RevokeGrantoperações RetireGrante são muito semelhantes entre si. Ambas excluem uma concessão, o que elimina as permissões por ela permitidas. A principal diferença entre elas é como elas são autorizadas.

RevokeGrant

Como a maioria das operações do AWS KMS, o acesso à operação `RevokeGrant`é controlado por meio de políticas de chaves e políticas do IAM. A RevokeGrantAPI pode ser chamada por qualquer diretor com `kms:RevokeGrant` permissão. Essa permissão está incluída nas permissões padrão fornecidas aos administradores de chaves. Normalmente, os administradores revogam uma concessão para negar permissões que são permitidas pela concessão.

RetireGrant

A concessão determina quem pode retirá-la. Esse design permite que você controle o ciclo de vida de uma concessão sem alterar políticas de chaves ou políticas do IAM. Normalmente, você retira uma concessão ao terminar de usar suas permissões.

Uma concessão pode ser retirada por uma entidade principal de retirada especificada nessa concessão. A entidade principal receptora da concessão também pode retirar a concessão, mas somente se ela também for uma entidade principal de retirada ou se a concessão incluir a operação `RetireGrant`. Como backup, a Conta da AWS em que a concessão foi criada pode retirar essa concessão.

Existe uma permissão `kms:RetireGrant` que pode ser usada em políticas do IAM, mas sua utilidade é limitada. Entidades principais especificadas na concessão podem retirar uma

concessão sem a permissão `kms:RetireGrant`. A permissão `kms:RetireGrant` por si só não permite que as entidades principais retirem uma concessão. A permissão `kms:RetireGrant` não é eficaz em uma política de chaves.

- Para negar permissão para retirar uma concessão, você pode usar uma ação `Deny` com a permissão `kms:RetireGrant`.
- A Conta da AWS que tem a chave do KMS pode delegar a permissão `kms:RetireGrant` à entidade principal do IAM na conta.
- Se a entidade principal que está sendo desativada for uma Conta da AWS diferente, os administradores na outra conta poderão usar `kms:RetireGrant` para delegar permissões para retirar a concessão a uma entidade principal do IAM nessa conta.

A API do AWS KMS segue o modelo de consistência eventual. Quando você cria, retira ou revoga uma concessão, pode haver um breve atraso antes que a alteração esteja disponível em todo o AWS KMS. Normalmente, a alteração leva menos de alguns segundos para se propagar por todo o sistema, mas, em alguns casos, pode levar vários minutos. Se precisar excluir uma nova concessão imediatamente antes que ela esteja disponível no AWS KMS, use um token de concessão para retirar a concessão. Não é possível usar um token de concessão para revogar uma concessão.

Conectar-se ao AWS KMS por meio de um endpoint da VPC

Você pode se conectar diretamente ao AWS KMS por meio de um endpoint privado de interface em sua nuvem privada virtual (VPC). Quando você usa um endpoint da VPC de interface, a comunicação entre a VPC e o AWS KMS é realizada inteiramente dentro da rede da AWS.

O AWS KMS é compatível com endpoints da Amazon Virtual Private Cloud (Amazon VPC) desenvolvidos pelo AWS PrivateLink. Cada endpoint da VPC é representado por uma ou mais interfaces de rede elástica (ENIs) com endereços IP privados em sua sub-redes da VPC.

O VPC endpoint de interface conecta a VPC diretamente ao AWS KMS sem um gateway da Internet, dispositivo NAT, conexão VPN ou conexão AWS Direct Connect. As instâncias na sua VPC não necessitam que endereços IP públicos se comuniquem com o AWS KMS.

Regiões

O AWS KMS é compatível com endpoints da VPC e políticas de endpoint da VPC em todas as Regiões da AWS com suporte para o AWS KMS.

Tópicos

- Considerações sobre endpoints da VPC do AWS KMS
- Criar um endpoint da VPC para o AWS KMS
- Conectar-se a um endpoint da VPC do AWS KMS
- Controlar o acesso a um endpoint da VPC
- Usar um endpoint da VPC em uma declaração de política
- Registrar o endpoint da VPC em log

Considerações sobre endpoints da VPC do AWS KMS

Antes de configurar um endpoint de interface da VPC para o AWS KMS, consulte o tópico Propriedades e limitações do endpoint de interface no Guia do AWS PrivateLink.

O suporte do AWS KMS para um endpoint de VPC inclui o seguinte.

- Você pode usar o endpoint da VPC para chamar todas as operações de API do AWS KMS em sua VPC.
- É possível criar um endpoint da VPC de interface que se conecta a um endpoint da região do AWS KMS ou um endpoint FIPS do AWS KMS.
- Você também pode usar os logs do AWS CloudTrail para auditar o uso de chaves do KMS por meio do endpoint da VPC. Para obter mais detalhes, consulte Registrar o endpoint da VPC em log.

Criar um endpoint da VPC para o AWS KMS

Você pode criar um endpoint da VPC para o AWS KMS usando o console da Amazon VPC ou a API da Amazon VPC. Para mais informações, consulte Criar um endpoint de interface no Guia do usuário do AWS PrivateLink.

- Para criar um endpoint da VPC para o AWS KMS, use o seguinte nome de serviço:

  ```
  com.amazonaws.region.kms
  ```

  Por exemplo, na Região Oeste dos EUA (Oregon) (`us-west-2`), o nome do serviço seria:

  ```
  com.amazonaws.us-west-2.kms
  ```

- Para criar um endpoint da VPC na que se conecta a um endpoint FIPS do AWS KMS, use o seguinte nome de serviço:

  ```
  com.amazonaws.region.kms-fips
  ```

  Por exemplo, na Região Oeste dos EUA (Oregon) (`us-west-2`), o nome do serviço seria:

  ```
  com.amazonaws.us-west-2.kms-fips
  ```

Para facilitar o uso do endpoint da VPC, é possível habilitar um nome de DNS privado para seu endpoint da VPC. Se você selecionar a opção Enable DNS Name (Habilitar nome DNS), o nome de host DNS padrão do AWS KMS será resolvido para seu endpoint da VPC. Por exemplo, `https://kms.us-west-2.amazonaws.com` resolveria para um endpoint da VPC conectado ao nome de serviço `com.amazonaws.us-west-2.kms`.

Essa opção facilita usar o endpoint da VPC. Os AWS SDKs e a AWS CLI usam o nome de host DNS padrão do AWS KMS. Dessa forma, não é necessário especificar o URL do endpoint da VPC em aplicações e comandos.

Para mais informações, consulte Acessar um serviço por meio de um endpoint de interface no Guia do AWS PrivateLink.

Conectar-se a um endpoint da VPC do AWS KMS

É possível se conectar ao AWS KMS por meio do endpoint da VPC usando um AWS SDK, a AWS CLI ou o AWS Tools for PowerShell. Para especificar o endpoint da VPC, use seu nome de DNS.

Por exemplo, este comando list-keys usa o parâmetro `endpoint-url` para especificar o endpoint da VPC. Para usar um comando como este, substitua o exemplo de ID de endpoint da VPC na sua conta.

```
$ aws kms list-keys --endpoint-url https://vpce-1234abcdf5678c90a-09p7654s-us-east-1a.ec2.us-east-1.vpce.amazonaws.com
```

Se os nomes de host privados tiverem sido ativados ao criar o endpoint da VPC, você não precisa especificar o URL do endpoint da VPC nos comandos de CLI ou na configuração da aplicação. O nome de host DNS padrão do AWS KMS será resolvido para o endpoint da VPC. A AWS CLI e

os SDKs usam esse nome de host por padrão. Assim, você pode começar a usar o endpoint da VPC para se conectar a um endpoint regional do AWS KMS sem alterar nada em seus scripts e aplicações.

Para usar nomes de host privados, os atributos`enableDnsHostnames` e `enableDnsSupport` da sua VPC devem ser definidos como `true`. Para definir esses atributos, use a ModifyVpcAttributeoperação. Para mais detalhes, consulte Exibir e atualizar atributos DNS para sua VPC no Guia do usuário do Amazon VPC.

Controlar o acesso a um endpoint da VPC

Para controlar o acesso ao endpoint da VPC para o AWS KMS, associe uma política de endpoint da VPC ao endpoint da VPC. A política de endpoint determina se as entidades principais podem usar o endpoint da VPC para chamar operações do AWS KMS em recursos do AWS KMS.

É possível criar uma política de endpoint da VPC ao criar seu endpoint e alterar a política de endpoint da VPC a qualquer momento. Use o console de gerenciamento da VPC CreateVpcEndpointou ModifyVpcEndpointas operações. Você também pode criar e alterar uma política de endpoint da VPC usando um modelo do AWS CloudFormation. Para obter ajuda sobre o uso do console de gerenciamento da VPC, consulte Criar um endpoint de interface e Modificar um endpoint de interface no Guia do AWS PrivateLink.

> **Note**
>
> AWS KMSO é compatível com políticas de endpoint da VPC a partir de julho de 2020. Os endpoint da VPCs para AWS KMS que foram criados antes dessa data têm a política de endpoint da VPC padrão, mas você pode alterá-la a qualquer momento.

Para ajuda sobre como escrever e formatar um documento de política JSON, consulte aReferência a políticas JSON do IAM, no Manual do usuário do IAM.

Tópicos

- Sobre políticas de endpoint da VPC
- Política de endpoint da VPC padrão
- Criar uma política de endpoint da VPC
- Visualizar uma política de endpoint da VPC

Sobre políticas de endpoint da VPC

Para que uma solicitação do AWS KMS que usa um endpoint da VPC seja bem-sucedida, a entidade principal requer permissões de duas origens:

- Uma política de chaves, uma política do IAM ou uma concessão deve conceder à entidade principal permissão para chamar a operação no recurso (chave do KMS ou alias).
- Uma política de endpoint da VPC deve dar permissão à entidade principal para usar o endpoint para fazer a solicitação.

Por exemplo, uma política de chaves pode dar à entidade principal permissão para chamar Decrypt em uma chave do KMS específica. No entanto, a política de endpoint da VPC pode não permitir que a entidade principal chame `Decrypt` nessa chave do KMS usando o endpoint.

Ou uma política de VPC endpoint pode permitir que um principal use o endpoint para chamar DisableKeydeterminadas chaves do KMS. Porém, se a entidade principal não tiver essas permissões de uma política de chaves, política do IAM ou concessão, ocorrerá falha na solicitação.

Política de endpoint da VPC padrão

Cada endpoint da VPC tem uma política de endpoint da VPC, mas não é necessário especificar a política. Se você não especificar uma política, a política de endpoint padrão permitirá todas as operações por todas as entidades principais em todos os recursos sobre o endpoint.

No entanto, para recursos do AWS KMS, a entidade principal também deve ter permissão para chamar a operação a partir de uma política de chaves, uma política do IAM ou uma concessão. Portanto, na prática, a política padrão diz que se uma entidade principal tem permissão para chamar uma operação em um recurso, ela também pode chamá-la usando o endpoint.

```
{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",
      "Principal": "*",
      "Resource": "*"
    }
  ]
}
```

Para permitir que entidades principais usem o endpoint da VPC apenas para um subconjunto de suas operações permitidas, crie ou atualize a política de endpoint da VPC.

Criar uma política de endpoint da VPC

Uma política de endpoint da VPC determina se uma entidade principal tem permissão para usar o endpoint da VPC para executar operações em um recurso. Para recursos do AWS KMS, a entidade principal também deve ter permissão para realizar as operações a partir de uma política de chave, uma política do IAM ou uma concessão.

Cada declaração de política de endpoint da VPC requer os seguintes elementos:

- A entidade principal que pode executar ações
- As ações que podem ser executadas
- Os recursos nos quais as ações podem ser executadas

A declaração de política não especifica o endpoint da VPC. Em vez disso, ele se aplica a qualquer endpoint da VPC ao qual a política está associada. Para obter mais informações, consulte Controlar o acesso a serviços com endpoint da VPCs no Guia do usuário da Amazon VPC.

Veja a seguir uma política de endpoint da VPC demonstrativa para o AWS KMS. Quando associada a um endpoint da VPC, essa política permite que o `ExampleUser` use o endpoint da VPC para chamar as operações especificadas nas chaves do KMS determinadas. Antes de usar uma política como esta, substitua a entidade principal e o ARN de chave demonstrativos por valores válidos de sua conta.

```
{
   "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 CloudTrailA registra todas as operações que usam o endpoint da VPC. No entanto, seus CloudTrail registros não incluem operações solicitadas por diretores em outras contas nem operações de chaves KMS em outras contas.

Dessa forma, convém criar uma política de endpoint da VPC que impeça que as entidades principais em contas externas usem o endpoint da VPC para chamar qualquer operação do AWS KMS em qualquer chave na conta local.

O exemplo a seguir usa a chave de condição aws: PrincipalAccount global para negar acesso a todos os principais para todas as operações em todas as chaves do KMS, a menos que o principal esteja na conta local. Antes de usar uma política como esta, substitua o ID de conta demonstrativo por um válido.

```
{
  "Statement": [
    {
      "Sid": "AccessForASpecificAccount",
      "Principal": {"AWS": "*"},
      "Action": "kms:*",
      "Effect": "Deny",
      "Resource": "arn:aws:kms:*:111122223333:key/*",
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalAccount": "111122223333"
        }
      }
    }
  ]
}
```

Visualizar uma política de endpoint da VPC

Para visualizar a política de VPC endpoint para um endpoint, use o console de gerenciamento da VPC ou a operação. DescribeVpcEndpoints

O comando de AWS CLI a seguir obtém a política para o endpoint com o ID de endpoint da VPC especificado.

Antes de executar esse comando, substitua o ID de endpoint demonstrativo por um válido da sua conta.

```
$ aws ec2 describe-vpc-endpoints \
--query 'VpcEndpoints[?VpcEndpointId==`vpce-1234abcdf5678c90a`].[PolicyDocument]'
--output text
```

Usar um endpoint da VPC em uma declaração de política

É possível controlar o acesso a recursos e operações do AWS KMS quando a solicitação vem da VPC ou usa um endpoint da VPC. Para fazer isso, use uma das chaves de condição global a seguir em uma política de chave ou política do IAM.

- Use a chave de condição `aws:sourceVpce` para conceder ou restringir o acesso com base no endpoint da VPC.
- Use a chave de condição `aws:sourceVpc` para conceder ou restringir o acesso a uma VPC que hospedar o endpoint privado.

> **Note**
>
> Tome cuidado ao criar políticas de chaves e políticas do IAM com base no seu endpoint da VPC. Se uma declaração de política exigir que as solicitações sejam provenientes de uma VPC ou endpoint da VPC específico, as solicitações de serviços integrados da AWS que usam o AWS KMS em seu nome poderão falhar. Para obter ajuda, consulte Usar condições do endpoint da VPC em políticas com permissões do AWS KMS.
> Além disso, a chave de condição `aws:sourceIP` não será efetiva se a solicitação vier de um endpoint da Amazon VPC. Para restringir solicitações a um endpoint da VPC, use as chaves de condições `aws:sourceVpce` ou `aws:sourceVpc`. Para obter mais informações, consulte Gerenciamento de identidade e acesso para VPC endpoints e serviços de VPC endpoint no Guia do AWS PrivateLink.

Você pode usar essas chaves de condição globais para controlar o acesso a AWS KMS keys (chaves KMS), aliases e operações como essas CreateKeyque não dependem de nenhum recurso específico.

Por exemplo, o exemplo de política de chave a seguir permite que um usuário execute algumas operações de criptografia com uma chave do KMS somente quando a solicitação usa o endpoint da

VPC especificado. Quando um usuário faz uma solicitação para AWS KMS, o ID do endpoint da VPC na solicitação está comparado com a chave-valor de condição `aws:sourceVpce` na política. Se não coincidirem, a solicitação será negada.

Para usar uma política como essa, substitua o ID Conta da AWS de espaço reservado e os IDs de endpoint da VPC por valores válidos para a sua conta.

```
{
    "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"
                }
            }
        }

    ]
}
```

Você também pode usar a chave de condição `aws:sourceVpc` para restringir o acesso às suas chaves do KMS com base na VPC no qual o endpoint da VPC reside.

O exemplo de política de chave a seguir permite comandos que gerenciam a chave do KMS somente quando eles são provenientes do `vpc-12345678`. Além disso, ele permite comandos que usam a chave do KMS para operações de criptografia somente quando eles são provenientes de `vpc-2b2b2b2b`. Você pode usar uma política como essa se uma aplicação é executada em uma VPC, mas você usa uma segunda VPC isolada para funções de gerenciamento.

Para usar uma política como essa, substitua o ID Conta da AWS de espaço reservado e os IDs de endpoint da VPC por valores válidos para a sua conta.

```
{
    "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": "*",
        }
    ]
}
```

Registrar o endpoint da VPC em log

AWS CloudTrailA registra todas as operações que usam o endpoint da VPC. Quando uma solicitação para o AWS KMS usa um endpoint da VPC, o ID do endpoint da VPC aparece na entrada de log do AWS CloudTrail que registra a solicitação. Você pode usar o ID de endpoint para auditar o uso do seu endpoint da VPC do AWS KMS.

No entanto, seus CloudTrail registros não incluem operações solicitadas por diretores em outras contas nem solicitações de AWS KMS operações em chaves e aliases do KMS em outras contas. Além disso, para proteger sua VPC, as solicitações que são negadas por uma política de endpoint da VPC, mas teriam sido permitidas de outra forma, não são registradas na AWS CloudTrail.

Por exemplo, este exemplo de entrada de log registra uma solicitação de GenerateDataKey que usou o VPC endpoint. O campo `vpcEndpointId` aparece no final da entrada de 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"
}
```

Chaves de condição para AWS KMS

Você pode especificar condições nas principais políticas e políticas do IAM que controlam o acesso aos AWS KMS recursos. A declaração de política é efetiva apenas quando as condições forem verdadeiras. Por exemplo, talvez você deseje que uma declaração de política só entre em vigor após uma data específica. Ou, você pode querer que uma declaração de política controle o acesso apenas quando um valor específico existe em uma solicitação de API.

Para especificar condições, use chaves de condição no elemento `Condition` de uma instrução de política com operadores de condição do IAM. Algumas chaves de condição geralmente se aplicam a AWS; outras são específicas AWS KMS a.

Os valores da chave de condição devem seguir as regras de caracteres e codificação das AWS KMS principais políticas e políticas do IAM. Para obter detalhes sobre as regras de documento de política de chaves, consulte Formato de política de chaves. Para obter detalhes sobre as regras de documento de política do IAM, consulte Requisitos de nome do IAM no Guia do usuário do IAM.

Tópicos

- AWS chaves de condição globais

- AWS KMS chaves de condição
- AWS KMS chaves de condição para AWS Nitro Enclaves

AWS chaves de condição globais

AWS define chaves de condição globais, um conjunto de chaves de condições de política para todos os AWS serviços que usam o IAM para controle de acesso. AWS KMS suporta todas as chaves de condição globais. Você pode usá-las nas AWS KMS principais políticas e nas políticas do IAM.

Por exemplo, você pode usar a chave de condição aws: PrincipalArn global para permitir o acesso a uma AWS KMS key (chave KMS) somente quando o principal na solicitação for representado pelo Amazon Resource Name (ARN) no valor da chave de condição. Para oferecer suporte ao controle de acesso baseado em atributos (ABAC) em AWS KMS, você pode usar a chave de condição global aws:ResourceTag/tag-key em uma política do IAM para permitir o acesso às chaves do KMS com uma tag específica.

Para ajudar a evitar que um AWS serviço seja usado como substituto confuso em uma política em que o diretor é o principal do AWS serviço, você pode usar as chaves de condição aws:SourceArnou as chaves de condição aws:SourceAccountglobais. Para obter detalhes, consulte Uso de chaves de condição `aws:SourceArn` ou `aws:SourceAccount`.

Para obter informações sobre chaves de condição AWS globais, incluindo os tipos de solicitações nas quais elas estão disponíveis, consulte Chaves de contexto de condição AWS global no Guia do usuário do IAM. Para exemplos de como usar chaves de condição globais em políticas do IAM, consulte Controlar o acesso a solicitações e Controlar chaves de etiquetas, no Manual do usuário do IAM.

Os tópicos a seguir fornecem orientações especiais para o uso de chaves de condição com base em endereços IP e endpoint da VPCs.

Tópicos

- Usar a condição de endereço IP em políticas com permissões do AWS KMS
- Usar condições do endpoint da VPC em políticas com permissões do AWS KMS

Usar a condição de endereço IP em políticas com permissões do AWS KMS

Você pode usar AWS KMS para proteger seus dados em um AWS serviço integrado. Mas tenha cuidado ao especificar os operadores de condição de endereço IP ou a chave de `aws:SourceIp`

condição na mesma declaração de política que permite ou nega acesso a. AWS KMS Por exemplo, a política em AWS: Nega acesso a AWS Com base no IP de origem restringe AWS as ações às solicitações do intervalo de IP especificado.

Considere este cenário:

1. Você anexa uma política como a mostrada em AWS: Nega acesso AWS com base no IP de origem a uma identidade do IAM. Defina o valor da `aws:SourceIp` chave de condição para o intervalo de endereços IP para a empresa do usuário. Essa identidade do IAM tem outras políticas vinculadas que permitem que ela use o Amazon EBS, o Amazon EC2 e o AWS KMS.
2. A identidade tenta vincular um volume do EBS criptografado a uma instância do EC2. Esta ação falha com um erro de autorização, embora o usuário tenha permissão para usar todos os serviços relevantes.

A etapa 2 falha porque a solicitação AWS KMS para descriptografar a chave de dados criptografada do volume vem de um endereço IP associado à infraestrutura do Amazon EC2. Para que a solicitação seja bem-sucedida, ela deve ter o endereço IP do usuário de origem. Como a política na etapa 1 nega explicitamente todas as solicitações de endereços IP que não sejam aqueles especificados, o Amazon EC2 não recebe permissão para descriptografar a chave de dados criptografada do volume do EBS.

Além disso, a chave de condição `aws:sourceIP` não será efetiva se a solicitação vier de um endpoint da Amazon VPC. Para restringir solicitações a um endpoint da VPC, incluindo um endpoint da VPC do AWS KMS, use as chaves de condições `aws:sourceVpce` ou `aws:sourceVpc`. Para obter mais informações, consulte endpoint da VPCs – controle do uso de endpoints no Manual do usuário do Amazon VPC.

Usar condições do endpoint da VPC em políticas com permissões do AWS KMS

AWS KMS suporta endpoints da Amazon Virtual Private Cloud (Amazon VPC) que são alimentados por. AWS PrivateLink Você pode usar as seguintes chaves de condição globais nas políticas de chaves e nas políticas do IAM para controlar o acesso aos AWS KMS recursos quando a solicitação vem de uma VPC ou usa um VPC endpoint. Para obter detalhes, consulte Usar um endpoint da VPC em uma declaração de política.

- `aws:SourceVpc` limita o acesso a solicitações da VPC especificado.
- `aws:SourceVpce` limita o acesso a solicitações do endpoint da VPC especificado.

Se você usar essas chaves de condição para controlar o acesso às chaves KMS, poderá inadvertidamente negar o acesso aos AWS serviços usados AWS KMS em seu nome.

Tome cuidado para evitar uma situação como o exemplo de chaves de condições de endereço IP. Se você restringir as solicitações de uma chave KMS a uma VPC ou VPC endpoint, as chamadas AWS KMS de um serviço integrado, como Amazon S3 ou Amazon EBS, podem falhar. Isso pode acontecer mesmo se a solicitação de origem for originada, em última análise, na VPC ou no endpoint da VPC.

AWS KMS chaves de condição

AWS KMS fornece um conjunto de chaves de condição que você pode usar em políticas de chaves e políticas do IAM. Essas chaves de condição são específicas para AWS KMS. Por exemplo, é possível usar a chave de condição `kms:EncryptionContext:`*`context-key`* para exigir um contexto de criptografia específico ao controlar o acesso a uma chave do KMS de criptografia simétrica.

Condições para uma solicitação de operação de API

Muitas chaves de AWS KMS condição controlam o acesso a uma chave KMS com base no valor de um parâmetro na solicitação de uma AWS KMS operação. Por exemplo, você pode usar a chave de KeySpec condição kms: em uma política do IAM para permitir o uso da CreateKeyoperação somente quando o valor do `KeySpec` parâmetro na `CreateKey` solicitação for`RSA_4096`.

Esse tipo de condição funciona mesmo quando o parâmetro não aparece na solicitação, como quando você usa o valor padrão do parâmetro. Por exemplo, você pode usar a chave de KeySpec condição kms: para permitir que os usuários usem a `CreateKey` operação somente quando o valor do `KeySpec` parâmetro for`SYMMETRIC_DEFAULT`, que é o valor padrão. Essa condição permite solicitações que têm o parâmetro `KeySpec` com o valor `SYMMETRIC_DEFAULT` e solicitações que não têm parâmetro `KeySpec`.

Condições para chaves do KMS usadas em operações de API

Algumas chaves de AWS KMS condição podem controlar o acesso às operações com base em uma propriedade da chave KMS usada na operação. Por exemplo, você pode usar a KeyOrigin condição kms: para permitir que os diretores GenerateDataKeychamem uma chave KMS somente quando a `Origin` chave KMS for. `AWS_KMS` Para descobrir se uma chave de condição pode ser usada dessa maneira, consulte a descrição da chave de condição.

A operação deve ser uma operação de recurso de chave do KMS, ou seja, uma operação autorizada para uma chave do KMS específica. Para identificar as operações de recursos de chaves do KMS, na Tabela de ações e recursos, procure um valor de `KMS key` na coluna `Resources` para a operação. Se você usar esse tipo de chave de condição com uma operação não autorizada para um determinado recurso de chave KMS, por exemplo ListKeys, a permissão não será efetiva porque a condição nunca poderá ser satisfeita. Não há recursos da chave do KMS envolvidos na autorização da operação `ListKeys` e nenhuma propriedade `KeySpec`.

Os tópicos a seguir descrevem cada chave de AWS KMS condição e incluem exemplos de declarações de política que demonstram a sintaxe da política.

Usar operadores de conjuntos com chaves de condição

Quando uma condição de política compara dois conjuntos de valores, como o conjunto de tags em uma solicitação e o conjunto de tags em uma política, você precisa saber AWS como comparar os conjuntos. O IAM define dois operadores de conjunto, `ForAnyValue` e `ForAllValues`, para essa finalidade. Use operadores de conjunto somente com chaves de condição de vários valores, que exigem esses operadores. Não use operadores de conjuntos com chaves de condição de valor único. Como sempre, teste suas instruções de política completamente antes de usá-las em um ambiente de produção.

Chaves de condição são de valor único ou de vários valores. Para determinar se uma chave de AWS KMS condição tem valor único ou de vários valores, consulte a coluna Tipo de valor na descrição da chave de condição.

- Chaves de condição de valor único têm no máximo um valor no contexto de autorização (a solicitação ou o recurso). Por exemplo, como cada chamada de API pode ser originada de apenas uma Conta da AWS, kms: CallerAccount é uma chave de condição de valor único. Não use um operador de conjunto com uma chave de condição de valor único.
- Chaves de condição de vários valores têm diversos valores no contexto de autorização (a solicitação ou o recurso). Por exemplo, como cada chave KMS pode ter vários aliases, kms: ResourceAliases pode ter vários valores. Chaves de condição de vários valores exigem um operador de conjunto.

Observe que a diferença entre chaves de condição de valor único e de vários valores depende do número de valores no contexto de autorização, e não do número de valores na condição da política.

> **Warning**
>
> O uso de um operador de conjunto com uma chave de condição de valor único pode criar uma instrução de política excessivamente permissiva (ou excessivamente restritiva). Use operadores de conjunto somente com chaves de condição de vários valores.
> Se você criar ou atualizar uma política que inclua um operador de `ForAllValues` conjunto com a chave de contexto ou as chaves de `aws:RequestTag/`*`tag-key`* condição kmsEncryptionContext::, AWS KMS retornará a seguinte mensagem de erro: `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.`

Para obter informações detalhadas sobre os operadores de conjunto `ForAnyValue` e `ForAllValues`, consulte Usar várias chaves e valores, no Manual do usuário do IAM. Para obter informações sobre o risco de usar o operador `ForAllValues` set com uma condição de valor único, consulte Aviso de segurança — ForAllValues com chave de valor único no Guia do usuário do IAM.

Tópicos

- kms: BypassPolicyLockoutSafetyCheck
- kms: CallerAccount
- kms: CustomerMasterKeySpec (obsoleto)
- kms: CustomerMasterKeyUsage (obsoleto)
- kms: DataKeyPairSpec
- kms: EncryptionAlgorithm
- kms:EncryptionContext: chave de contexto
- kms: EncryptionContextKeys
- kms: ExpirationModel
- kms: GrantConstraintType
- kms: GrantIsFor AWSResource
- kms: GrantOperations
- kms: GranteePrincipal

- kms: KeyOrigin
- kms: KeySpec
- kms: KeyUsage
- kms: MacAlgorithm
- kms: MessageType
- kms: MultiRegion
- kms: MultiRegionKeyType
- kms: PrimaryRegion
- kms: ReEncryptOnSameKey
- kms: RequestAlias
- kms: ResourceAliases
- kms: ReplicaRegion
- kms: RetiringPrincipal
- kms: RotationPeriodInDays
- kms: ScheduleKeyDeletionPendingWindowInDays
- kms: SigningAlgorithm
- kms: ValidTo
- kms: ViaService
- kms: WrappingAlgorithm
- kms: WrappingKeySpec

kms: BypassPolicyLockoutSafetyCheck

AWS KMS chaves de condição	Tipo de condição	Tipo de valor	Operações de API	Tipo de política
`kms:BypassPolicyLockoutSafetyCheck`	Booleano	Valor único	`CreateKey` `PutKeyPolicy`	Somente políticas do IAM

AWS KMS chaves de condição	Tipo de condição	Tipo de valor	Operações de API	Tipo de política
				Políticas de chaves e políticas do IAM

A chave de `kms:BypassPolicyLockoutSafetyCheck` condição controla o acesso às PutKeyPolicyoperações CreateKeye com base no valor do `BypassPolicyLockoutSafetyCheck` parâmetro na solicitação.

A instrução de política do IAM de exemplo a seguir impede que os usuários ignorem a verificação de segurança de bloqueio da política ao negar a eles a permissão para criar chaves do KMS quando o valor do parâmetro `BypassPolicyLockoutSafetyCheck` na solicitação `CreateKey` é `true`.

```
{
  "Effect": "Deny",
  "Action": [
    "kms:CreateKey",
    "kms:PutKeyPolicy"
  ],
  "Resource": "*",
  "Condition": {
    "Bool": {
      "kms:BypassPolicyLockoutSafetyCheck": true
    }
  }
}
```

Você também pode usar a chave de condição `kms:BypassPolicyLockoutSafetyCheck` em uma política do IAM ou política de chaves para controlar o acesso à operação `PutKeyPolicy`. A declaração de política de exemplo a seguir de uma política de chaves impede que os usuários ignorem a verificação de segurança de bloqueio da política ao alterar a política de uma chave do KMS.

Em vez de usar `Deny` de forma explícita, esta declaração de política usa `Allow` com o operador de condição nula para permitir o acesso somente quando a solicitação não inclui o parâmetro `BypassPolicyLockoutSafetyCheck`. Quando o parâmetro não for usado, o valor padrão será

`false`. Essa instrução de política um pouco mais fraca pode ser substituída no caso raro em que uma derivação é necessária.

```
{
  "Effect": "Allow",
  "Action": "kms:PutKeyPolicy",
  "Resource": "*",
  "Condition": {
    "Null": {
      "kms:BypassPolicyLockoutSafetyCheck": true
    }
  }
}
```

Consulte também

- kms: KeySpec
- kms: KeyOrigin
- kms: KeyUsage

kms: CallerAccount

AWS KMS chaves de condição	Tipo de condição	Tipo de valor	Operações de API	Tipo de política
`kms:CallerAccount`	String	Valor único	Operações de recursos de chaves do KMS Operações do armazenamento de chaves personalizado	Políticas de chaves e políticas do IAM

É possível usar essa chave de condição para permitir ou negar acesso a todas as identidades (usuários e perfis) em uma Conta da AWS. Em políticas de chaves, você pode usar o elemento

`Principal` para especificar as identidades às quais a declaração de política se aplica. A sintaxe do elemento `Principal` não fornece uma forma de especificar todas as identidades em uma Conta da AWS. Mas você pode obter esse efeito combinando essa chave de condição com um `Principal` elemento que especifica todas as AWS identidades.

Você pode usá-lo para controlar o acesso a qualquer operação de recurso de chave KMS, ou seja, qualquer AWS KMS operação que use uma chave KMS específica. Para identificar as operações de recursos de chaves do KMS, na Tabela de ações e recursos, procure um valor de `KMS key` na coluna `Resources` para a operação. Ele também é válido para operações que gerenciam armazenamentos de chaves personalizados.

Por exemplo, a instrução de política de chaves a seguir demonstra como usar a chave de condição `kms:CallerAccount`. Esta declaração de política está na política principal do Chave gerenciada pela AWS Amazon EBS. Ele combina um `Principal` elemento que especifica todas as AWS identidades com a chave de `kms:CallerAccount` condição para permitir efetivamente o acesso a todas as identidades em 111122223333. Conta da AWS Ele contém uma chave de AWS KMS condição adicional (`kms:ViaService`) para limitar ainda mais as permissões, permitindo somente solicitações provenientes do Amazon EBS. Para ter mais informações, consulte kms: 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: CustomerMasterKeySpec (obsoleto)

A chave de condição `kms:CustomerMasterKeySpec` está defasada. Em vez disso, use a chave de KeySpec condição kms:.

As chaves de condição `kms:CustomerMasterKeySpec` e `kms:KeySpec` funcionam da mesma forma. Apenas os nomes são diferentes. Recomendamos usar o `kms:KeySpec`. No entanto, para evitar alterações significativas, AWS KMS suporta as duas teclas de condição.

kms: CustomerMasterKeyUsage (obsoleto)

A chave de condição `kms:CustomerMasterKeyUsage` está defasada. Em vez disso, use a chave de KeyUsage condição kms:.

As chaves de condição `kms:CustomerMasterKeyUsage` e `kms:KeyUsage` funcionam da mesma forma. Apenas os nomes são diferentes. Recomendamos usar o `kms:KeyUsage`. No entanto, para evitar alterações significativas, AWS KMS suporta as duas teclas de condição.

kms: DataKeyPairSpec

AWS KMS chaves de condição	Tipo de condição	Tipo de valor	Operações de API	Tipo de política

`kms:DataKeyPairSpec`	String	Valor único	`GenerateDataKeyPair`
			
			`GenerateDataKeyPairWithoutPlaintext`
				Políticas de chaves e políticas do IAM

Você pode usar essa chave de condição para controlar o acesso às GenerateDataKeyPairWithoutPlaintextoperações GenerateDataKeyPaire com base no valor do `KeyPairSpec` parâmetro na solicitação. Por exemplo, é possível permitir que os usuários gerem somente tipos de pares de chaves de dados específicos.

O exemplo de instrução de política de chaves a seguir usa a chave de condição `kms:DataKeyPairSpec` para permitir que os usuários usem a chave do KMS para gerar somente pares de chaves de dados RSA.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": [
    "kms:GenerateDataKeyPair",
    "kms:GenerateDataKeyPairWithoutPlaintext"
  ],
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:DataKeyPairSpec": "RSA*"
    }
  }
}
```

Consulte também

- kms: KeySpec
- the section called “kms: EncryptionAlgorithm”
- the section called “kms:EncryptionContext: chave de contexto”
- the section called “kms: EncryptionContextKeys”

kms: EncryptionAlgorithm

AWS KMS chaves de condição	Tipo de condição	Tipo de valor	Operações de API	Tipo de política
`kms:EncryptionAlgorithm`	String	Valor único	`Decrypt` `Encrypt`	Políticas de chaves e políticas do IAM

AWS KMS chaves de condição	Tipo de condição	Tipo de valor	Operações de API	Tipo de política

			`GenerateDataKey`
			`GenerateDataKeyPair`
			`GenerateDataKeyPairWithoutPlaintext`
			`GenerateDataKeyWithoutPlaintext`
			`ReEncrypt`	

É possível usar a chave de condição `kms:EncryptionAlgorithm` para controlar o acesso às operações de criptografia com base no algoritmo de criptografia usado na operação. Para as ReEncryptoperações Encrypt, Decrypt e, ele controla o acesso com base no valor do EncryptionAlgorithmparâmetro na solicitação. Para operações que geram chaves de dados e pares de chaves de dados, ela controla o acesso com base no algoritmo de criptografia que é usado para criptografar a chave de dados.

Essa chave de condição não tem efeito nas operações realizadas fora da AWS KMS, como a criptografia com a chave pública em um par de chaves KMS assimétrico fora da. AWS KMS

EncryptionAlgorithm parâmetro em uma solicitação

Para permitir que os usuários usem apenas um algoritmo de criptografia específico com uma chave do KMS, use uma instrução de política com um efeito `Deny` e um operador de condição `StringNotEquals`. Por exemplo, o seguinte exemplo de instrução de política de chaves proíbe que as entidades principais capazes de assumir a função `ExampleRole` usem essa chave do KMS nas

operações de criptografia especificadas, a menos que o algoritmo de criptografia na solicitação seja `RSAES_OAEP_SHA_256`, um algoritmo criptográfico assimétrico usado em chaves RSA do KMS.

Diferente de uma instrução de política que permite que um usuário utilize um algoritmo de criptografia específico, uma instrução de política com um duplo negativo como essa evita que outras políticas e concessões da chave do KMS permitam que essa função use outros algoritmos de criptografia. O `Deny` nessa instrução de política de chaves tem precedência sobre qualquer política de chaves ou política do IAM com um efeito `Allow` e tem precedência sobre todas as concessões dessa chave do KMS e suas entidades principais.

```
{
  "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 de criptografia usado para a operação

Você também pode usar a chave de condição `kms:EncryptionAlgorithm` para controlar o acesso às operações com base no algoritmo de criptografia utilizado na operação, mesmo quando esse algoritmo não está especificado na solicitação. Isso permite exigir ou proibir o algoritmo `SYMMETRIC_DEFAULT`, que pode não ser especificado em uma solicitação por ser o valor padrão.

Também é possível usar a chave de condição `kms:EncryptionAlgorithm` para controlar o acesso às operações que geram chaves de dados e pares de chaves de dados. Essas operações só usam chaves do KMS de criptografia simétrica e o algoritmo `SYMMETRIC_DEFAULT`.

Por exemplo, essa política do IAM limita seus principais à criptografia simétrica. Ela nega o acesso a qualquer chave do KMS na conta de exemplo para operações de criptografia, a menos que o algoritmo de criptografia especificado na solicitação ou usado na operação seja SYMMETRIC_DEFAULT. Incluindo `GenerateDataKey*` GenerateDataKeyPairacréscimos GenerateDataKeyGenerateDataKeyWithoutPlaintext,, e GenerateDataKeyPairWithoutPlaintextàs permissões. A condição não tem efeito nessas operações porque elas sempre utilizam um algoritmo de criptografia simétrica.

```
{
  "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"
    }
  }
}
```

Consulte também

- the section called “kms: MacAlgorithm”
- kms: SigningAlgorithm

kms:EncryptionContext: chave de contexto

AWS KMS chaves de condição	Tipo de condição	Tipo de valor	Operações de API	Tipo de política
`kms:EncryptionCont`	String	Valor único	`CreateGrant` `Encrypt`	Políticas de chaves e políticas do IAM

AWS KMS chaves de condição	Tipo de condição	Tipo de valor	Operações de API	Tipo de política

`ext: context-key`			`Decrypt`
			
			`GenerateDataKey`
			
			`GenerateDataKeyPair`
			
			`GenerateDataKeyPairWithoutPlaintext`
			
			`GenerateDataKeyWithoutPlaintext`
			
			`ReEncrypt`	

É possível usar a chave de condição `kms:EncryptionContext:context-key` para controlar o acesso a uma chave do KMS de criptografia simétrica com base no contexto de criptografia em uma solicitação de uma operação criptográfica. Use essa chave de condição para avaliar a chave e o valor no par de contexto de criptografia. Para avaliar somente as chaves do contexto de criptografia ou exigir um contexto de criptografia, independentemente das chaves ou dos valores, use a chave de EncryptionContextKeys condição kms:.

> **Note**
>
> Os valores das chaves de condição devem estar em conformidade com as regras de caracteres para políticas de chaves e políticas do IAM. Alguns caracteres que são válidos em um contexto de criptografia não são válidos em políticas. Talvez você não consiga usar essa chave de condição para expressar todos os valores válidos de contexto de criptografia. Para obter detalhes sobre as regras de documento de política de chaves, consulte Formato

de política de chaves. Para obter detalhes sobre as regras de documento de política do IAM, consulte Requisitos de nome do IAM no Guia do usuário do IAM.

Não é possível especificar um contexto de criptografia em uma operação criptográfica com uma chave do KMS assimétrica ou uma chave do KMS de Hash-based message authentication code (HMAC – Código de autenticação de mensagem por hash). Algoritmos assimétricos e algoritmos de Message authentication code (MAC – Código de autenticação de mensagem) não são compatíveis com um contexto de criptografia.

Para usar a chave de condição kms:EncryptionContext: context-key, substitua o espaço reservado da chave *contextual pela chave de contexto* da criptografia. Substitua o espaço reservado *context-value* pelo valor de contexto de criptografia.

```
"kms:EncryptionContext:context-key": "context-value"
```

Por exemplo, a seguinte chave de condição especifica um contexto de criptografia no qual a chave é `AppName` e o valor é `ExampleApp` (`AppName = ExampleApp`).

```
"kms:EncryptionContext:AppName": "ExampleApp"
```

Esta é uma chave de condição de valor único. A chave na chave de condição especifica uma chave de contexto de criptografia específica (context-key). Embora seja possível incluir vários pares de contexto de criptografia em cada solicitação de API, o par de contexto de criptografia com a context-key especificada pode ter somente um valor. Por exemplo, a chave de condição `kms:EncryptionContext:Department` aplica-se somente a pares de contexto de criptografia com uma chave `Department`, e qualquer par de contexto de criptografia com a chave `Department` pode ter somente um valor.

Não use um operador de conjunto com a chave de condição `kms:EncryptionContext:`*`context-key`*. Se você criar uma instrução de política com uma ação `Allow`, a chave de condição `kms:EncryptionContext:`*`context-key`* e o operador de conjunto `ForAllValues`, a condição permitirá solicitações sem contexto de criptografia e solicitações com pares de contexto de criptografia que não estão especificados na condição de política.

> **Warning**
>
> Não use um operador de conjunto `ForAnyValue` ou `ForAllValues` com essa chave de condição de valor único. Esses operadores de conjunto podem criar uma condição de política que não requer valores que você pretende exigir e permite valores que você pretende proibir. Se você criar ou atualizar uma política que inclua um operador de `ForAllValues` conjunto com a chave de contexto kms:EncryptionContext:, AWS KMS retornará a seguinte mensagem de erro: `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.`

Para exigir um par de contexto de criptografia específico, use a chave de condição `kms:EncryptionContext:`*`context-key`* com o operador `StringEquals`.

A seguinte instrução de política de chaves de exemplo permite que as entidades principais que podem assumir a função usem a chave do KMS em uma solicitação `GenerateDataKey` apenas quando o contexto de criptografia nessa solicitação inclui o par `AppName:ExampleApp`. Outros pares de contexto de criptografia são permitidos.

O nome da chave não é sensível a maiúsculas e minúsculas. A diferenciação de maiúsculas e minúsculas do valor é determinada pelo operador de condição, como `StringEquals`. Para obter detalhes, consulte Diferenciação de letras maiúsculas e minúsculas da condição de contexto de criptografia.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:AppName": "ExampleApp"
    }
  }
```

```
}
```

Para exigir um par de contexto de criptografia e proibir todos os outros pares de contexto de criptografia, use kms:EncryptionContext: context-key e `kms:EncryptionContextKeys`na declaração de política. A instrução de política de exemplo a seguir usa a condição `kms:EncryptionContext:AppName` para exigir o par de contextos de criptografia `AppName=ExampleApp` na solicitação. Ela também usa uma chave de condição `kms:EncryptionContextKeys` com o operador de conjunto `ForAllValues` para permitir apenas a chave de contexto de criptografia `AppName`.

O operador de conjunto `ForAllValues` limita as chaves de contexto de criptografia na solicitação para `AppName`. Se a condição `kms:EncryptionContextKeys` com o operador de conjunto `ForAllValues` tivesse sido usada sozinha em uma instrução de política, esse operador de conjunto permitiria solicitações sem contexto de criptografia. No entanto, se a solicitação não tivesse um contexto de criptografia, a condição `kms:EncryptionContext:AppName` falharia. Para detalhes sobre o operador de conjunto `ForAllValues`, consulteUsar várias chaves e valores, no Manual do usuário do 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"
      ]
    }
  }
}
```

Também é possível usar essa chave de condição para negar acesso a uma chave do KMS para uma operação específica. O exemplo a seguir de instrução de política de chaves usa um efeito Deny para proibir a entidade principal de usar a chave do KMS quando o contexto de criptografia na

solicitação inclui um par de contextos de criptografia `Stage=Restricted`. Essa condição permite uma solicitação com outros pares de contextos de criptografia, incluindo pares de contextos de criptografia com a chave `Stage` e outros valores, como `Stage=Test`.

```
{
  "Effect": "Deny",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:Stage": "Restricted"
    }
  }
}
```

Usar vários pares de contextos de criptografia

Você pode exigir ou proibir vários pares de contextos de criptografia. Também pode exigir um dos vários pares de contextos de criptografia. Para obter detalhes sobre a lógica usada para interpretar essas condições, consulte Criar uma condição com várias chaves ou valores, no Manual do usuário do IAM.

> **Note**
>
> As versões anteriores deste tópico exibiam declarações de política que usavam os operadores `ForAnyValue` e `ForAllValues` definiam com a chave de condição kms:EncryptionContext: context-key. Usar um operador de conjunto com uma chave de condição de valor único pode resultar em políticas que permitem solicitações sem contexto de criptografia e pares de contextos de criptografia não especificados.
> Por exemplo, uma condição de política com o efeito `Allow`, o operador de conjunto `ForAllValues` e a chave de condição `"kms:EncryptionContext:Department": "IT"` não limita o contexto de criptografia ao par "Department=IT". Ele permite solicitações sem contexto de criptografia e solicitações com pares de contextos de criptografia não especificados, como `Stage=Restricted`.
> Revise suas políticas e elimine o operador definido de qualquer condição com kms:EncryptionContext: context-key. Tentativas de criar ou atualizar uma política com esse

formato falham com uma exceção `OverlyPermissiveCondition`. Para resolver o erro, exclua o operador de conjunto.

Para exigir vários pares de contextos de criptografia, liste esses pares na mesma condição. A seguinte instrução de política de chaves de exemplo requer dois pares de contextos de criptografia: `Department=IT` e `Project=Alpha`. Como as condições têm chaves diferentes (`kms:EncryptionContext:Department` e `kms:EncryptionContext:Project`), elas são implicitamente conectadas por um operador AND. Outros pares de contextos de criptografia são permitidos, mas não são necessários.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:Decrypt",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:Department": "IT",
      "kms:EncryptionContext:Project": "Alpha"
    }
  }
}
```

Para exigir um par de contextos de criptografia OU outro par, coloque cada chave de condição em uma instrução de política separada. O exemplo a seguir de política de chaves requer pares `Department=IT` ou `Project=Alpha`, ou ambos. Outros pares de contextos de criptografia são permitidos, mas não são necessários.

```
{
 "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"
  }
 }
}
```

Para exigir pares de criptografia específicos e excluir todos os outros pares de contexto de criptografia, use kms:EncryptionContext: context-key e [kms:EncryptionContextKeys](#)na declaração de política. A seguinte declaração de política de chaves usa a condição kms:EncryptionContext: context-key para exigir um contexto de criptografia com pares e*Department=IT*. `Project=Alpha` Ela usa uma chave de condição `kms:EncryptionContextKeys` com o operador de conjunto `ForAllValues` para permitir apenas as chaves de contexto de criptografia `Department` e `Project`.

O operador de conjunto `ForAllValues` limita as chaves de contexto de criptografia na solicitação para `Department` e `Project`. Se fosse usado sozinho em uma condição, esse operador de conjunto permitiria solicitações sem contexto de criptografia, mas nessa configuração, a chave de contexto kmsEncryptionContext:: nessa condição falharia.

```
{
  "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"
      ]
    }
  }
}
```

Você também pode proibir vários pares de contexto de criptografia. O seguinte exemplo de instrução de política de chaves usa um efeito `Deny` para proibir a entidade principal de usar as chaves do KMS se o contexto de criptografia na solicitação incluir um par `Stage=Restricted` ou `Stage=Production`.

Vários valores (`Restricted` e `Production`) para a mesma chave (`kms:EncryptionContext:Stage`) são implicitamente conectados por OR. Para obter mais detalhes, consulte Lógica de avaliação para condições com várias chaves ou valores, no Manual do usuário do IAM.

```
{
  "Effect": "Deny",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:Stage": [
         "Restricted",
         "Production"
      ]
    }
  }
}
```

Diferenciação de letras maiúsculas e minúsculas da condição de contexto de criptografia

O contexto de criptografia especificado em uma operação de criptografia deve ser uma correspondência exata, que diferencia maiúsculas de minúsculas para o contexto de criptografia

especificado na operação de criptografia. Somente a ordem dos pares em um contexto de criptografia com vários pares pode variar.

No entanto, em condições de política, a chave de condição não diferencia maiúsculas de minúsculas. A diferenciação de maiúsculas e minúsculas do valor da condição é determinada pelo operador de condição de política que você usa, como `StringEquals` ou `StringEqualsIgnoreCase`.

Dessa forma, a chave de condição, que consiste do prefixo `kms:EncryptionContext:` e da substituição *`context-key`*, não diferencia maiúsculas de minúsculas. Uma política que usa essa condição não verifica a capitalização dos elementos da chave de condição. A diferenciação de maiúsculas e minúsculas do valor, ou seja, a substituição *`context-value`*, é determinada pelo operador de condição de política.

Por exemplo, a declaração de política a seguir permite a operação quando o contexto de criptografia inclui uma chave `Appname`, independentemente da sua capitalização. A condição `StringEquals` exige que `ExampleApp` seja capitalizado da maneira como foi especificado.

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

Para exigir uma chave de contexto de criptografia com distinção entre maiúsculas e minúsculas, use a condição kms: EncryptionContextKeys policy com um operador de condição que diferencia maiúsculas de minúsculas, como. `StringEquals` Nesta condição de política, como a chave de contexto de criptografia é o valor da condição de política, o recurso é determinado pelo operador da condição.

```
{
  "Effect": "Allow",
  "Principal": {
```

```
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "*",
  "Condition": {
    "ForAnyValue:StringEquals": {
      "kms:EncryptionContextKeys": "AppName"
    }
  }
}
```

Para exigir uma avaliação com distinção entre maiúsculas e minúsculas da chave de contexto e do valor da criptografia, use as condições de política de chave de contexto *kms:EncryptionContextKeys* e kmsEncryptionContext:: juntas na mesma declaração de política. O operador de condição sensível a maiúsculas e minúsculas (como`StringEquals`) sempre aplica-se ao valor da condição. A chave de contexto de criptografia (como `AppName`) é o valor da condição `kms:EncryptionContextKeys`. O valor do contexto de criptografia (como`ExampleApp`) é o valor da condição kms:EncryptionContext: context-key.

Por exemplo, na instrução de política de chaves a seguir, como o operador `StringEquals` diferencia maiúsculas de minúsculas, a chave de contexto de criptografia e o valor de contexto de criptografia diferenciam maiúsculas de minúsculas.

```
{
  "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"
    }
  }
}
```

Usar variáveis em uma condição de contexto de criptografia

A chave e o valor em um par de contexto de criptografia devem ser strings literais simples. Não podem ser números inteiros, objetos, ou qualquer tipo que não esteja totalmente resolvido. Se você usar um tipo diferente, como um número inteiro ou flutuante, AWS KMS interprete-o como uma string literal.

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

No entanto, o valor da chave de condição `kms:EncryptionContext:`*`context-key`* pode ser uma variável de política do IAM. Essas variáveis de política são resolvidas em runtime com base nos valores da solicitação. Por exemplo, o `aws:CurrentTime` é resolvido como a hora da solicitação e `aws:username` é resolvido como o nome amigável do chamador.

É possível usar essas variáveis de política para criar uma declaração de política com uma condição que requer informações muito específicas em um contexto de criptografia, como o nome de usuário do chamador. Como contém uma variável, é possível usar a mesma declaração de política para todos os usuários que podem assumir a função. Não é necessário escrever uma declaração de política diferente para cada usuário.

Considere uma situação em que você deseja que todos os usuários que podem assumir uma função usem a mesma chave do KMS para criptografar e descriptografar seus dados. No entanto, você deseja permitir que eles descriptografem somente os dados que criptografaram. Comece exigindo que cada solicitação AWS KMS inclua um contexto de criptografia em que a chave esteja `user` e o valor seja o nome de AWS usuário do chamador, como o seguinte.

```
"encryptionContext": {
    "user": "bob"
}
```

Para impor esse requisito, é possível usar uma declaração de política como a do exemplo a seguir. Essa instrução de política concede à função `TestTeam` permissão para criptografar e descriptografar dados com a chave do KMS. No entanto, a permissão será válida somente quando o contexto de criptografia na solicitação incluir um par `"user": "`*`<username>`*`"`. Para representar o nome do usuário, a condição usa a variável de política `aws:username`.

Quando a solicitação for avaliada, o nome de usuário do chamador substituirá a variável na condição. Dessa forma, a condição requer um contexto de criptografia de `"user": "bob"` para "bob" e `"user": "alice"` para "alice".

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/TestTeam"
  },
  "Action": [
    "kms:Decrypt",
    "kms:Encrypt"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:user": "${aws:username}"
    }
  }
}
```

É possível usar uma variável de política do IAM somente no valor do par de chaves da condição `kms:EncryptionContext:`*`context-key`*. Não é possível usar uma variável na chave.

Também não é possível usar chaves de contexto específicas do provedor em variáveis. Essas chaves de contexto identificam de forma exclusiva os usuários que se conectaram AWS usando a federação de identidade da web.

Como todas as variáveis, essas variáveis podem ser usadas apenas na condição de política `kms:EncryptionContext:`*`context-key`*, não no contexto de criptografia real. E elas podem ser usadas apenas no valor da condição, não na chave.

Por exemplo, a declaração de política de chaves a seguir é semelhante à anterior. No entanto, a condição requer um contexto de criptografia em que a chave é `sub` e o valor identifica exclusivamente um usuário conectado a um grupo de usuários do Amazon Cognito. Para obter detalhes sobre como identificar usuários e funções no Amazon Cognito, consulte Funções do IAM, no Guia do desenvolvedor do 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}"
    }
  }
}
```

Consulte também

- the section called “kms: EncryptionContextKeys”
- the section called “kms: GrantConstraintType”

kms: EncryptionContextKeys

AWS KMS chaves de condição	Tipo de condição	Tipo de valor	Operações de API	Tipo de política

`kms:EncryptionContextKeys`	String (lista)	Vários valores	`CreateGrant`
			`Decrypt`
			`Encrypt`
			`GenerateDataKey`
			`GenerateDataKeyPair`
			`GenerateDataKeyPai`
				Políticas de chaves e políticas do IAM

AWS KMS chaves de condição	Tipo de condição	Tipo de valor	Operações de API	Tipo de política

			`rWithoutPlaintext`
			
			`GenerateDataKeyWithoutPlaintext`
			
			`ReEncrypt`	

É possível usar a chave de condição `kms:EncryptionContextKeys` para controlar o acesso a uma chave do KMS de criptografia simétrica com base no contexto de criptografia em uma solicitação de uma operação criptográfica. Use essa chave de condição para avaliar apenas a chave em cada par de contexto de criptografia. Para avaliar tanto a chave quanto o valor no contexto de criptografia, use a chave de condição `kms:EncryptionContext:`*`context-key`*.

Não é possível especificar um contexto de criptografia em uma operação criptográfica com uma chave do KMS assimétrica ou uma chave do KMS de Hash-based message authentication code (HMAC – Código de autenticação de mensagem por hash). Algoritmos assimétricos e algoritmos de Message authentication code (MAC – Código de autenticação de mensagem) não são compatíveis com um contexto de criptografia.

> **Note**
>
> Os valores da chave de condição, incluindo uma chave de contexto de criptografia, devem estar em conformidade com as regras de caracteres e codificação das políticas de AWS KMS chaves. Talvez você não consiga usar essa chave de condição para expressar todas as chaves válidas de contexto de criptografia. Para obter detalhes sobre as regras de documento de política de chaves, consulte Formato de política de chaves. Para obter detalhes sobre as regras de documento de política do IAM, consulte Requisitos de nome do IAM no Guia do usuário do IAM.

Esta é uma chave de condição de vários valores. Você pode especificar vários pares de contexto de criptografia em cada solicitação de API. `kms:EncryptionContextKeys` compara as chaves de contexto de criptografia na solicitação com o conjunto de chaves de contexto de criptografia na política. Para determinar como esses conjuntos são comparados, você deve fornecer um operador de conjunto `ForAnyValue` ou `ForAllValues` na condição de política. Para detalhes sobre os operadores de conjunto, consulteUsar várias chaves e valores, no Manual do usuário do IAM.

- `ForAnyValue`: pelo menos uma chave de contexto de criptografia na solicitação deve corresponder a uma chave de contexto de criptografia na condição da política. Outras chaves de contexto de criptografia são permitidas. Se a solicitação não tiver um contexto de criptografia, a condição não será atendida.
- `ForAllValues`: cada chave de contexto de criptografia na solicitação deve corresponder a uma chave de contexto de criptografia na condição da política. Esse operador de conjunto limita as chaves de contexto de criptografia àquelas na condição de política. Ele não requer uma chave de contexto de criptografia, mas proíbe chaves de contexto de criptografia não especificadas.

O exemplo a seguir de instrução de política de chaves usa a chave de condição `kms:EncryptionContextKeys` com o operador de conjunto `ForAnyValue`. Essa instrução de política permite o uso de uma chave do KMS para as operações especificadas, mas somente quando pelo menos um dos pares de contextos de criptografia na solicitação inclui a chave `AppName`, independentemente do seu valor.

Por exemplo, essa instrução de política de chaves permite uma solicitação `GenerateDataKey` com dois pares de contextos de criptografia, `AppName=Helper` e `Project=Alpha`, pois o primeiro par de contextos de criptografia atende à condição. Uma solicitação com apenas `Project=Alpha` ou sem um contexto de criptografia falharia.

Como a operação de StringEqualscondição diferencia maiúsculas de minúsculas, essa declaração de política exige a ortografia e as maiúsculas e minúsculas da chave de contexto de criptografia. No entanto, você pode usar um operador de condição que ignora a capitalização da chave, como `StringEqualsIgnoreCase`.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": [
```

```
    "kms:Encrypt",
    "kms:GenerateDataKey*"
  ],
  "Resource": "*",
  "Condition": {
    "ForAnyValue:StringEquals": {
      "kms:EncryptionContextKeys": "AppName"
    }
  }
}
```

Você também pode usar a chave de condição `kms:EncryptionContextKeys` para exigir um contexto de criptografia (qualquer um) em operações de criptografia que usam a chave do KMS.

A instrução de política de exemplo a seguir usa a chave de condição `kms:EncryptionContextKeys` com o Operador de condição nula para permitir o acesso a uma chave do KMS apenas quando o contexto de criptografia na solicitação da API não é nulo. Essa condição não confere as chaves ou os valores do contexto de criptografia. Ela só verifica se o contexto de criptografia existe.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": [
    "kms:Encrypt",
    "kms:GenerateDataKey*"
  ],
  "Resource": "*",
  "Condition": {
    "Null": {
      "kms:EncryptionContextKeys": false
    }
  }
}
```

Consulte também

- kms:EncryptionContext: chave de contexto
- kms: GrantConstraintType

kms: ExpirationModel

AWS KMS chaves de condição	Tipo de condição	Tipo de valor	Operações de API	Tipo de política
`kms:ExpirationModel`	String	Valor único	`ImportKeyMaterial`	Políticas de chaves e políticas do IAM

A chave de `kms:ExpirationModel` condição controla o acesso à ImportKeyMaterialoperação com base no valor do ExpirationModelparâmetro na solicitação.

`ExpirationModel` é um parâmetro opcional que determina se o material de chave importada expira. Os valores válidos são `KEY_MATERIAL_EXPIRES` e `KEY_MATERIAL_DOES_NOT_EXPIRE`. `KEY_MATERIAL_EXPIRES` é o valor padrão.

A data e a hora de expiração são determinadas pelo valor do ValidToparâmetro. O parâmetro `ValidTo` só não será necessário se o valor do parâmetro `ExpirationModel` for `KEY_MATERIAL_DOES_NOT_EXPIRE`. Você também pode usar a chave de ValidTo condição kms: para exigir uma data de expiração específica como condição de acesso.

A instrução de política exemplificada a seguir usa a chave de condição `kms:ExpirationModel` para permitir que os usuários importem o material de chave para uma chave do KMS somente quando a solicitação incluir o parâmetro `ExpirationModel` e seu valor for `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"
    }
  }
```

```
}
```

Também é possível usar a chave de condição `kms:ExpirationModel` para permitir que os usuários importem o material de chave somente quando este expirar. A instrução de política de chave exemplificada a seguir usa a chave de condição `kms:ExpirationModel` com o operador de condição Null para permitir que os usuários importem o material de chave somente quando a solicitação não tiver um parâmetro `ExpirationModel`. O valor padrão para ExpirationModel é`KEY_MATERIAL_EXPIRES`.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:ImportKeyMaterial",
  "Resource": "*",
  "Condition": {
    "Null": {
      "kms:ExpirationModel": true
    }
  }
}
```

Consulte também

- kms: ValidTo
- kms: WrappingAlgorithm
- kms: WrappingKeySpec

kms: GrantConstraintType

AWS KMS chaves de condição	Tipo de condição	Tipo de valor	Operações de API	Tipo de política
`kms:GrantConstraintType`	String	Valor único	`CreateGrant`	Políticas de chaves e políticas do IAM

Você pode usar essa chave de condição para controlar o acesso à CreateGrantoperação com base no tipo de restrição de concessão na solicitação.

Ao criar uma concessão, você pode especificar uma restrição de concessão para permitir as operações permitidas pela concessão apenas quando um contexto de criptografia específico existir. A restrição de concessão pode ser de dois tipos: `EncryptionContextEquals` ou `EncryptionContextSubset`. Você pode usar esta chave de condição para verificar se a solicitação contém um tipo ou outro.

> **Important**
>
> Não inclua informações confidenciais ou sigilosas nesse campo. Esse campo pode ser exibido em texto simples em CloudTrail registros e outras saídas.

A instrução de política de chaves exemplificada a seguir usa a chave de condição `kms:GrantConstraintType` para permitir que os usuários criem concessões somente quando a solicitação incluir uma restrição de concessão `EncryptionContextEquals`. O exemplo mostra uma declaração de política em uma política de chaves.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:CreateGrant",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:GrantConstraintType": "EncryptionContextEquals"
    }
  }
}
```

Consulte também

- kms:EncryptionContext: chave de contexto
- kms: EncryptionContextKeys
- kms: GrantIsFor AWSResource
- kms: GrantOperations

- kms: GranteePrincipal
- kms: RetiringPrincipal

kms: GrantIsFor AWSResource

AWS KMS chaves de condição	Tipo de condição	Tipo de valor	Operações de API	Tipo de política

`kms:GrantIsForAWSResource`	Booleano	Valor único	`CreateGrant`
			`ListGrants`
			`RevokeGrant`
				Políticas de chaves e políticas do IAM

Permite ou nega permissão para as RevokeGrantoperações CreateGrantListGrants,, ou somente quando um AWS serviço integrado AWS KMS chama a operação em nome do usuário. Essa condição de política não permite que o usuário chame essas operações de concessão diretamente.

A declaração de política de chaves demonstrativa a seguir usa a chave de condição `kms:GrantIsForAWSResource`. Ele permite que AWS serviços integrados AWS KMS, como o Amazon EBS, criem concessões nessa chave KMS em nome do principal especificado.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": "kms:CreateGrant",
  "Resource": "*",
  "Condition": {
    "Bool": {
      "kms:GrantIsForAWSResource": true
    }
  }
}
```

Consulte também

- kms: GrantConstraintType
- kms: GrantOperations
- kms: GranteePrincipal
- kms: RetiringPrincipal

kms: GrantOperations

AWS KMS chaves de condição	Tipo de condição	Tipo de valor	Operações de API	Tipo de política
`kms:GrantOperations`	String	Vários valores	`CreateGrant`	Políticas de chaves e políticas do IAM

Você pode usar essa chave de condição para controlar o acesso à CreateGrantoperação com base nas operações de concessão na solicitação. Por exemplo, é possível permitir que os usuários criem concessões que delegam permissão para criptografar, mas não para descriptografar. Para obter mais informações sobre concessões, consulte Usar concessões.

Esta é uma chave de condição de vários valores. O `kms:GrantOperations` compara o conjunto de operações de concessão na solicitação `CreateGrant` para o conjunto de operações de concessão na política. Para determinar como esses conjuntos são comparados, você deve fornecer um operador de conjunto `ForAnyValue` ou `ForAllValues` na condição de política. Para detalhes sobre os operadores de conjunto, consulteUsar várias chaves e valores, no Manual do usuário do IAM.

- `ForAnyValue`: pelo menos uma operação de concessão na solicitação deve corresponder a uma das operações de concessão na condição da política. Outras operações de concessão são permitidas.
- ForAllValues: cada operação de concessão na solicitação deve corresponder a uma operação de concessão na condição da política. Este operador de conjunto limita as operações de concessão àquelas especificadas na condição da política. Ele não requer uma operação de concessão, mas proíbe operações de concessão não especificadas.

ForAllValues também retorna verdadeiro quando não há operações de concessão na solicitação, mas `CreateGrant` não permite isso. Se o parâmetro `Operations` ausente ou tiver um valor nulo, o parâmetro `CreateGrant` falhará na solicitação.

A instrução de política de chaves exemplificada a seguir usa a chave de condição `kms:GrantOperations` para criar concessões somente quando as operações de concessões são `Encrypt` e/ou `ReEncryptTo`. Se a concessão incluir quaisquer outras operações, a solicitação `CreateGrant` falhará.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": "kms:CreateGrant",
  "Resource": "*",
  "Condition": {
    "ForAllValues:StringEquals": {
      "kms:GrantOperations": [
        "Encrypt",
        "ReEncryptTo"
      ]
    }
  }
}
```

Se você alterar o operador de conjunto na condição de política para `ForAnyValue`, a instrução de política exigirá que pelo menos uma das operações de concessão na concessão seja `Encrypt` ou `ReEncryptTo`, mas permitirá outras operações de concessão, como `Decrypt` ou `ReEncryptFrom`.

Consulte também

- kms: GrantConstraintType
- kms: GrantIsFor AWSResource
- kms: GranteePrincipal
- kms: RetiringPrincipal

kms: GranteePrincipal

AWS KMS chaves de condição	Tipo de condição	Tipo de valor	Operações de API	Tipo de política
`kms:GranteePrincipal`	String	Valor único	`CreateGrant`	Políticas do IAM e de chaves

Você pode usar essa chave de condição para controlar o acesso à CreateGrantoperação com base no valor do GranteePrincipalparâmetro na solicitação. Por exemplo, é possível criar concessões para usar uma chave do KMS somente quando a entidade principal favorecida na solicitação `CreateGrant` corresponder à entidade principal especificada na instrução de condição.

Para especificar o principal beneficiário, use o Amazon Resource Name (ARN) de um principal. AWS Os principais válidos incluem usuários do IAM Contas da AWS, funções do IAM, usuários federados e usuários com funções assumidas. Para obter ajuda com a sintaxe do ARN para um diretor, consulte ARNs do IAM no Guia do usuário do IAM.

A instrução de política de chaves exemplificada a seguir usa a chave de condição `kms:GranteePrincipal` para criar concessões para uma chave do KMS somente quando a entidade principal favorecida na concessão for `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"
    }
  }
}
```

Consulte também

- kms: GrantConstraintType
- kms: GrantIsFor AWSResource
- kms: GrantOperations
- kms: RetiringPrincipal

kms: KeyOrigin

AWS KMS chaves de condição	Tipo de condição	Tipo de valor	Operações de API	Tipo de política
`kms:KeyOrigin`	String	Valor único	`CreateKey` Operações de recursos de chaves do KMS	Políticas do IAM Políticas de chaves e políticas do IAM

A chave de condição `kms:KeyOrigin` controla o acesso às operações com base no valor da propriedade `Origin` da chave do KMS que é criada pela operação ou usada nela. Ela funciona como uma condição de recurso ou de solicitação.

Você pode usar essa chave de condição para controlar o acesso à CreateKeyoperação com base no valor do parâmetro Origin na solicitação. Os valores válidos para `Origin` são `AWS_KMS`, `AWS_CLOUDHSM` e `EXTERNAL`.

Por exemplo, você pode criar uma chave KMS somente quando o material da chave é gerado em AWS KMS (`AWS_KMS`), somente quando o material da chave é gerado em um AWS CloudHSM cluster associado a um armazenamento de chaves personalizado (`AWS_CLOUDHSM`) ou somente quando o material da chave é importado de uma fonte externa (`EXTERNAL`).

O exemplo de declaração de política de chaves a seguir usa a chave de `kms:KeyOrigin` condição para criar uma chave KMS somente quando AWS KMS cria o material da chave.

```
{
  "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"
        }
      }
    }
  ]
}
```

Também é possível usar a chave de condição `kms:KeyOrigin` para controlar o acesso a operações que usam ou gerenciam uma chave do KMS com base na propriedade `Origin` da chave do KMS usada para a operação. A operação deve ser uma operação de recurso de chave do KMS, ou seja, uma operação autorizada para uma chave do KMS específica. Para identificar as operações de recursos de chaves do KMS, na Tabela de ações e recursos, procure um valor de `KMS key` na coluna `Resources` para a operação.

Por exemplo, a política do IAM a seguir permite que as entidades principais realizem as operações de recursos de chave do KMS especificadas, mas somente com as chaves do KMS na conta que foram criadas em um armazenamento de chaves personalizado.

```
{
  "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"
    }
  }
}
```

Consulte também

- kms: BypassPolicyLockoutSafetyCheck
- kms: KeySpec
- kms: KeyUsage

kms: KeySpec

AWS KMS chaves de condição	Tipo de condição	Tipo de valor	Operações de API	Tipo de política
`kms:KeySpec`	String	Valor único	`CreateKey`	Políticas do IAM

AWS KMS chaves de condição	Tipo de condição	Tipo de valor	Operações de API	Tipo de política
			Operações de recursos de chaves do KMS	Políticas de chaves e políticas do IAM

A chave de condição `kms:KeySpec` controla o acesso às operações com base no valor da propriedade `KeySpec` da chave do KMS que é criada pela operação ou usada nela.

Você pode usar essa chave de condição em uma política do IAM para controlar o acesso à CreateKeyoperação com base no valor do KeySpecparâmetro em uma `CreateKey` solicitação. Por exemplo, é possível usar essa condição para permitir que os usuários criem somente chaves do KMS de criptografia simétrica ou somente chaves do KMS de HMAC.

O seguinte exemplo de instrução de política do IAM usa a chave de condição `kms:KeySpec` para permitir que as entidades principais criem apenas chaves do KMS assimétricas RSA. A permissão só é válida quando o `KeySpec` na solicitação começa com `RSA_`.

```
{
  "Effect": "Allow",
  "Action": "kms:CreateKey",
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:KeySpec": "RSA_*"
    }
  }
}
```

Também é possível usar a chave de condição `kms:KeySpec` para controlar o acesso a operações que usam ou gerenciam uma chave do KMS com base na propriedade `KeySpec` da chave do KMS usada para a operação. A operação deve ser uma operação de recurso de chave do KMS, ou seja, uma operação autorizada para uma chave do KMS específica. Para identificar as operações de recursos de chaves do KMS, na Tabela de ações e recursos, procure um valor de `KMS key` na coluna `Resources` para a operação.

Por exemplo, a seguinte política do IAM permite que as entidades principais executem as operações especificadas de recursos de chave do KMS, mas somente com chaves do KMS de criptografia simétrica na conta.

```
{
  "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"
    }
  }
}
```

Consulte também

- kms: BypassPolicyLockoutSafetyCheck
- kms: CustomerMasterKeySpec (obsoleto)
- kms: DataKeyPairSpec
- kms: KeyOrigin
- kms: KeyUsage

kms: KeyUsage

AWS KMS chaves de condição	Tipo de condição	Tipo de valor	Operações de API	Tipo de política
`kms:KeyUsage`	String	Valor único	`CreateKey`	Políticas do IAM Políticas de chaves e políticas do IAM

AWS KMS chaves de condição	Tipo de condição	Tipo de valor	Operações de API	Tipo de política
			Operações de recursos de chaves do KMS	

A chave de condição `kms:KeyUsage` controla o acesso às operações com base no valor da propriedade `KeyUsage` da chave do KMS que é criada pela operação ou usada nela.

Você pode usar essa chave de condição para controlar o acesso à CreateKeyoperação com base no valor do KeyUsageparâmetro na solicitação. Os valores válidos para `KeyUsage` são `ENCRYPT_DECRYPT`, `SIGN_VERIFY` e `GENERATE_VERIFY_MAC`.

Por exemplo, será possível criar uma chave do KMS somente quando `KeyUsage` for `ENCRYPT_DECRYPT` ou negar a permissão de um usuário quando `KeyUsage` for `SIGN_VERIFY`.

A instrução de política do IAM exemplificada a seguir usa a chave de condição `kms:KeyUsage` para criar uma chave do KMS somente quando `KeyUsage` for `ENCRYPT_DECRYPT`.

```
{
  "Effect": "Allow",
  "Action": "kms:CreateKey",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:KeyUsage": "ENCRYPT_DECRYPT"
    }
  }
}
```

Também é possível usar a chave de condição `kms:KeyUsage` para controlar o acesso a operações que usam ou gerenciam uma chave do KMS com base na propriedade `KeyUsage` da chave do KMS na operação. A operação deve ser uma operação de recurso de chave do KMS, ou seja, uma operação autorizada para uma chave do KMS específica. Para identificar as operações de recursos de chaves do KMS, na Tabela de ações e recursos, procure um valor de `KMS key` na coluna `Resources` para a operação.

Por exemplo, a política do IAM a seguir permite que as entidades principais realizem as operações de recursos de chaves do KMS especificadas, mas somente com as chaves do KMS na conta que são usadas para assinatura e verificação.

```
{
  "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"
    }
  }
}
```

Consulte também

- kms: BypassPolicyLockoutSafetyCheck
- kms: CustomerMasterKeyUsage (obsoleto)
- kms: KeyOrigin
- kms: KeySpec

kms: MacAlgorithm

AWS KMS chaves de condição	Tipo de condição	Tipo de valor	Operações de API	Tipo de política
`kms:MacAlgorithm`	String	Valor único	`GenerateMac` `VerifyMac`	Políticas de chaves e políticas do IAM

Você pode usar a chave de `kms:MacAlgorithm` condição para controlar o acesso às VerifyMacoperações GenerateMace com base no valor do `MacAlgorithm` parâmetro na solicitação.

O seguinte exemplo de política de chaves permite que usuários capazes de assumir a função `testers` só usem a chave do KMS de HMAC para gerar e verificar etiquetas HMAC quando o algoritmo de MAC na solicitação for `HMAC_SHA_384` ou `HMAC_SHA_512`. Essa política usa duas instruções distintas de política, cada uma com sua própria condição. Se você especificar mais de um algoritmo de MAC em uma única instrução de condição, a condição exigirá ambos os algoritmos em vez de um ou outro.

```
{
  "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"
```

```
        }
      }
    }
  ]
}
```

Consulte também

- the section called “kms: EncryptionAlgorithm”
- kms: SigningAlgorithm

kms: MessageType

AWS KMS chaves de condição	Tipo de condição	Tipo de valor	Operações de API	Tipo de política
`kms:MessageType`	String	Valor único	`Sign` `Verify`	Políticas de chaves e políticas do IAM

A chave de condição `kms:MessageType` controla o acesso às operações Sign e Verify com base no valor do parâmetro `MessageType` na solicitação. Os valores válidos para `MessageType` são `RAW` e `DIGEST`.

Por exemplo, a instrução de política de chaves a seguir usa a chave de condição `kms:MessageType` para usar uma chave do KMS assimétrica para assinar uma mensagem, mas não um resumo da mensagem.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": "kms:Sign",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
```

```
      "kms:MessageType": "RAW"
    }
  }
}
```

Consulte também

- the section called “kms: SigningAlgorithm”

kms: MultiRegion

AWS KMS chaves de condição	Tipo de condição	Tipo de valor	Operações de API	Tipo de política
`kms:MultiRegion`	Booleano	Valor único	`CreateKey` Operações de recursos de chaves do KMS	Políticas de chaves e políticas do IAM

Você pode usar essa chave de condição para permitir operações somente em chaves de região única ou somente em chaves de várias regiões. A chave de `kms:MultiRegion` condição controla o acesso às AWS KMS operações nas chaves KMS e à CreateKeyoperação com base no valor da `MultiRegion` propriedade da chave KMS. Os valores válidos são `true` (várias regiões) e `false` (região única). Todas as chaves do KMS têm uma propriedade `MultiRegion`.

Por exemplo, a seguinte instrução de política do IAM usa a chave de condição `kms:MultiRegion` para permitir que as entidades principais criem apenas chaves de região única.

```
{
  "Effect": "Allow",
  "Action": "kms:CreateKey",
  "Resource": "*",
  "Condition": {
    "Bool": {
      "kms:MultiRegion": false
    }
  }
```

```
}
```

kms: MultiRegionKeyType

AWS KMS chaves de condição	Tipo de condição	Tipo de valor	Operações de API	Tipo de política
`kms:MultiRegionKeyType`	String	Valor único	`CreateKey` Operações de recursos de chaves do KMS	Políticas de chaves e políticas do IAM

Você pode usar essa chave de condição para permitir operações somente em chaves primárias de várias regiões ou somente em chaves de réplica de várias regiões. A chave de `kms:MultiRegionKeyType` condição controla o acesso às AWS KMS operações nas chaves KMS e a CreateKeyoperação com base na `MultiRegionKeyType` propriedade da chave KMS. Os valores válidos são `PRIMARY` e `REPLICA`. Somente chaves de várias regiões têm uma propriedade `MultiRegionKeyType`.

Normalmente, você pode usar a chave de condição `kms:MultiRegionKeyType` em uma política do IAM para controlar o acesso a várias chaves do KMS. No entanto, como uma determinada chave de várias regiões pode mudar para primária ou réplica, convém usar essa condição em uma política de chaves para permitir uma operação somente quando a chave de várias regiões específica for uma chave primária ou de réplica.

Por exemplo, a instrução de política do IAM a seguir usa a chave de condição `kms:MultiRegionKeyType` para permitir que as entidades principais programem e cancelem a exclusão de chaves somente em chaves de réplica de várias regiões na Conta da AWS especificada.

```
{
  "Effect": "Allow",
  "Action": [
    "kms:ScheduleKeyDeletion",
    "kms:CancelKeyDeletion"
  ],
  "Resource": "arn:aws:kms:*:111122223333:key/*",
```

```
  "Condition": {
    "StringEquals": {
      "kms:MultiRegionKeyType": "REPLICA"
    }
  }
}
```

Para permitir ou negar acesso a todas as chaves de várias regiões, você pode usar ambos os valores ou um valor nulo com `kms:MultiRegionKeyType`. No entanto, a chave de MultiRegion condição kms: é recomendada para essa finalidade.

kms: PrimaryRegion

AWS KMS chaves de condição	Tipo de condição	Tipo de valor	Operações de API	Tipo de política
`kms:PrimaryRegion`	String (lista)	Valor único	`UpdatePrimaryRegion`	Políticas de chaves e políticas do IAM

Você pode usar essa chave de condição para limitar as regiões de destino em uma UpdatePrimaryRegionoperação. São elas Regiões da AWS que podem hospedar suas chaves primárias multirregionais.

A chave de `kms:PrimaryRegion` condição controla o acesso à UpdatePrimaryRegionoperação com base no valor do `PrimaryRegion` parâmetro. O `PrimaryRegion` parâmetro especifica a chave Região da AWS de réplica multirregional que está sendo promovida para primária. O valor da condição é um ou mais Região da AWS nomes, como `us-east-1` ou`ap-southeast-2`, ou padrões de nome de região, como `eu-*`

Por exemplo, a instrução de política de chaves a seguir usa a chave de condição `kms:PrimaryRegion` para permitir que as entidades principais atualizem a região primária de uma chave de várias regiões para uma das quatro regiões especificadas.

```
{
  "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"
      ]
    }
  }
}
```

kms: ReEncryptOnSameKey

AWS KMS chaves de condição	Tipo de condição	Tipo de valor	Operações de API	Tipo de política
`kms:ReEncryptOnSameKey`	Booleano	Valor único	`ReEncrypt`	Políticas de chaves e políticas do IAM

Você pode usar essa chave de condição para controlar o acesso à ReEncryptoperação com base no fato de a solicitação especificar uma chave KMS de destino que seja a mesma usada para a criptografia original.

Por exemplo, a instrução de política de chaves a seguir usa a chave de condição `kms:ReEncryptOnSameKey` para criptografar novamente somente quando a chave do KMS de destino é semelhante à usada para a criptografia original.

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

```
  "Condition": {
    "Bool": {
      "kms:ReEncryptOnSameKey": true
    }
  }
}
```

kms: RequestAlias

AWS KMS chaves de condição	Tipo de condição	Tipo de valor	Operações de API	Tipo de política
`kms:RequestAlias`	String (lista)	Valor único	Operações criptográficas DescribeKey GetPublicKey	Políticas de chaves e políticas do IAM

É possível usar essa chave de condição para permitir uma operação somente quando a solicitação usa um alias específico para identificar a chave do KMS. A chave de condição `kms:RequestAlias` controla o acesso a uma chave do KMS usada em uma operação criptográfica, `GetPublicKey` ou `DescribeKey` com base no alias que identifica essa chave do KMS na solicitação. (Essa condição de política não tem efeito na GenerateRandomoperação porque a operação não usa uma chave ou alias KMS.)

Essa condição oferece suporte ao controle de acesso baseado em atributos (ABAC) em AWS KMS, que permite controlar o acesso às chaves KMS com base nas tags e aliases de uma chave KMS. Você pode usar tags e aliases para conceder ou negar acesso a uma chave do KMS sem alterar políticas ou permissões. Para obter detalhes, consulte ABAC para AWS KMS.

Para especificar o alias nessa condição de política, use um nome de alias, como `alias/project-alpha`, ou um padrão de nome de alias, como `alias/*test*`. Não é possível especificar um ARN de alias no valor dessa chave de condição.

Para satisfazer essa condição, o valor do parâmetro`KeyId` na solicitação deve ser um nome de alias correspondente ou um ARN de alias. Se a solicitação usar umidentificador de chave diferente, ela não atenderá à condição, mesmo que identifique a mesma chave do KMS.

Por exemplo, a declaração de política chave a seguir permite que o diretor chame a GenerateDataKeyoperação na chave KMS. No entanto, isso é permitido somente quando o valor do parâmetro `KeyId` na solicitação é `alias/finance-key` ou um ARN de alias com esse nome de alias, como `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"
    }
  }
}
```

Você não pode usar essa chave de condição para controlar o acesso às operações de alias, como CreateAliasou DeleteAlias. Para obter informações sobre como controlar o acesso a todas as operações de alias, consulte Controlar o acesso a aliases.

kms: ResourceAliases

AWS KMS chaves de condição	Tipo de condição	Tipo de valor	Operações de API	Tipo de política
`kms:ResourceAliases`	String (lista)	Vários valores	Operações de recursos de chaves do KMS	Somente políticas do IAM

Use essa chave de condição para controlar o acesso a uma chave do KMS com base nos aliases que estão associados à chave do KMS. A operação deve ser uma operação de recurso de chave do KMS, ou seja, uma operação autorizada para uma chave do KMS específica. Para identificar as operações de recursos de chaves do KMS, na Tabela de ações e recursos, procure um valor de `KMS key` na coluna `Resources` para a operação.

Essa condição oferece suporte ao controle de acesso baseado em atributos (ABAC) no AWS KMS. Com o ABAC, você pode controlar o acesso a chaves do KMS com base nas etiquetas atribuídas a uma chave do KMS e nos aliases associados a uma chave do KMS. Você pode usar tags e aliases para conceder ou negar acesso a uma chave do KMS sem alterar políticas ou permissões. Para obter detalhes, consulte ABAC para AWS KMS.

Um alias deve ser exclusivo em uma região Conta da AWS e, mas essa condição permite controlar o acesso a várias chaves KMS na mesma região (usando o operador de `StringLike` comparação) ou a várias chaves KMS em diferentes contas Regiões da AWS .

> **Note**
>
> A ResourceAliases condição kms: é efetiva somente quando a chave KMS está em conformidade com os aliases por cota de chave KMS. Se uma chave do KMS exceder essa cota, as entidades principais autorizadas a usar essa chave pela condição `kms:ResourceAliases` terão acesso negado a ela.

Para especificar o alias nessa condição de política, use um nome de alias, como `alias/project-alpha`, ou um padrão de nome de alias, como `alias/*test*`. Não é possível especificar um ARN de alias no valor dessa chave de condição. Para atender à condição, a chave do KMS usada na operação deve ter o alias especificado. Não importa se ou como a chave do KMS é identificada na solicitação para a operação.

Esta é uma chave de condição de vários valores que compara o conjunto de aliases associados a uma chave do KMS com o conjunto de aliases na política. Para determinar como esses conjuntos são comparados, você deve fornecer um operador de conjunto `ForAnyValue` ou `ForAllValues` na condição de política. Para detalhes sobre os operadores de conjunto, consulteUsar várias chaves e valores, no Manual do usuário do IAM.

- ForAnyValue: pelo menos um alias associado à chave KMS deve corresponder a um alias na condição da política. Outros aliases são permitidos. Se a chave do KMS não tiver alias, a condição não será atendida.
- ForAllValues: cada alias associado à chave KMS deve corresponder a um alias na política. Esse operador de conjunto limita os aliases associados à chave do KMS àqueles na condição da política. Ele não requer aliases, mas proíbe aliases não especificados.

Por exemplo, a declaração de política do IAM a seguir permite que o diretor chame a GenerateDataKeyoperação em qualquer chave KMS especificada Conta da AWS associada ao `finance-key` alias. (As políticas de chaves das chaves do KMS afetadas também devem permitir que a conta da entidade principal as use para essa operação.) Para indicar que a condição é atendida quando um dos muitos aliases que podem estar associados à chave do KMS é `alias/finance-key`, a condição usa o operador de conjunto `ForAnyValue`.

Como a condição `kms:ResourceAliases` é baseada no recurso, e não na solicitação, uma chamada para `GenerateDataKey` é bem-sucedida para qualquer chave do KMS associada ao alias `finance-key`, mesmo que a solicitação use um ID de chave ou ARN de chave para identificar a chave do 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"
    }
  }
}
```

O seguinte exemplo de instrução de política do IAM permite que a entidade principal habilite e desabilite chaves do KMS, mas somente quando todos os aliases das chaves do KMS incluem “`Test`”. Essa instrução de política usa duas condições. A condição com o operador de conjunto `ForAllValues` requer que todos os aliases associados à chave do KMS incluam “Test”. A condição com o operador de conjunto `ForAnyValue` requer que a chave do KMS tenha pelo menos um alias com “Test”. Sem a condição `ForAnyValue`, essa instrução de política teria permitido que a entidade principal usasse chaves do KMS sem aliases.

```
{
  "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*"
      ]
    }
  }
}
```

kms: ReplicaRegion

AWS KMS chaves de condição	Tipo de condição	Tipo de valor	Operações de API	Tipo de política
`kms:ReplicaRegion`	String (lista)	Valor único	`ReplicateKey`	Políticas de chaves e políticas do IAM

Você pode usar essa chave de condição para limitar a Regiões da AWS possibilidade de um principal replicar uma chave multirregional. A chave de `kms:ReplicaRegion` condição controla o acesso à ReplicateKeyoperação com base no valor do ReplicaRegionparâmetro na solicitação. Esse parâmetro especifica a propriedade Região da AWS da nova chave de réplica.

O valor da condição é um ou mais Região da AWS nomes, como `us-east-1` ou`ap-southeast-2`, ou padrões de nomes, como`eu-*`. Para obter uma lista dos nomes desses Regiões da AWS AWS KMS suportes, consulte AWS Key Management Service endpoints e cotas no. Referência geral da AWS

Por exemplo, a declaração de política de chaves a seguir usa a chave de `kms:ReplicaRegion` condição para permitir que os diretores chamem a ReplicateKeyoperação somente quando o valor do `ReplicaRegion` parâmetro for uma das regiões especificadas.

```
{
  "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"
      ]
    }
  }
}
```

Essa chave de condição controla o acesso somente à ReplicateKeyoperação. Para controlar o acesso à UpdatePrimaryRegionoperação, use a chave de PrimaryRegion condição kms:.

kms: RetiringPrincipal

AWS KMS chaves de condição	Tipo de condição	Tipo de valor	Operações de API	Tipo de política
`kms:RetiringPrincipal`	String (lista)	Valor único	`CreateGrant`	Políticas de chaves e políticas do IAM

Você pode usar essa chave de condição para controlar o acesso à CreateGrantoperação com base no valor do RetiringPrincipalparâmetro na solicitação. Por exemplo, é possível criar concessões para usar uma chave do KMS somente quando `RetiringPrincipal` na solicitação `CreateGrant` corresponder a `RetiringPrincipal` na instrução da condição.

Para especificar o diretor que está se aposentando, use o Amazon Resource Name (ARN) de AWS um principal. Os principais válidos incluem usuários do IAM Contas da AWS, funções do IAM, usuários federados e usuários com funções assumidas. Para obter ajuda com a sintaxe do ARN para um diretor, consulte ARNs do IAM no Guia do usuário do IAM.

O exemplo de declaração de política de chaves a seguir permite que um usuário crie concessões para a chave KMS. A chave de `kms:RetiringPrincipal` condição restringe a permissão às `CreateGrant` solicitações em que o diretor aposentado da concessão é o. `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"
    }
  }
}
```

Consulte também

- kms: GrantConstraintType
- kms: GrantIsFor AWSResource
- kms: GrantOperations
- kms: GranteePrincipal

kms: RotationPeriodInDays

AWS KMS chaves de condição	Tipo de condição	Tipo de valor	Operações de API	Tipo de política
`kms:RotationPeriodInDays`	Numérico	Valor único	`EnableKeyRotation`	Políticas de chaves e políticas do IAM

Você pode usar essa chave de condição para limitar os valores que os diretores podem especificar no `RotationPeriodInDays` parâmetro de uma EnableKeyRotationsolicitação.

`RotationPeriodInDays`Especifica o número de dias entre cada data de rotação automática da chave. AWS KMS permite especificar um período de rotação entre 90 e 2560 dias, mas você pode usar a chave de `kms:RotationPeriodInDays` condição para restringir ainda mais o período de rotação, como impor um período mínimo de rotação dentro do intervalo válido.

Por exemplo, a declaração de política principal a seguir usa a chave de `kms:RotationPeriodInDays` condição para impedir que os diretores habilitem a rotação de chaves se o período de rotação for menor ou igual a 180 dias.

```
{
  "Effect": "Deny",
  "Action": "kms:EnableKeyRotation",
  "Principal": "*",
  "Resource": "*",
  "Condition" : {
      "NumericLessThanEquals" : {
        "kms:RotationPeriodInDays" : "180"
      }
  }
}
```

kms: ScheduleKeyDeletionPendingWindowInDays

AWS KMS chaves de condição	Tipo de condição	Tipo de valor	Operações de API	Tipo de política
`kms:ScheduleKeyDeletionPendingWindowInDays`	Numérico	Valor único	`ScheduleKeyDeletion`	Políticas de chaves e políticas do IAM

Você pode usar essa chave de condição para limitar os valores que os diretores podem especificar no `PendingWindowInDays` parâmetro de uma ScheduleKeyDeletionsolicitação.

`PendingWindowInDays`Especifica o número de dias que AWS KMS serão esperados antes de excluir uma chave. AWS KMS permite especificar um período de espera entre 7 e 30 dias, mas você pode usar a chave de `kms:ScheduleKeyDeletionPendingWindowInDays` condição para restringir ainda mais o período de espera, como impor um período mínimo de espera dentro do intervalo válido.

Por exemplo, a declaração de política de chave a seguir usa a chave de condição `kms:ScheduleKeyDeletionPendingWindowInDays` para impedir que a entidade principal programe a exclusão da chave se o período de espera for menor ou igual a 21 dias.

```
{
  "Effect": "Deny",
  "Action": "kms:ScheduleKeyDeletion",
  "Principal": "*",
  "Resource": "*",
  "Condition" : {
      "NumericLessThanEquals" : {
        "kms:ScheduleKeyDeletionPendingWindowInDays" : "21"
      }
  }
}
```

kms: SigningAlgorithm

AWS KMS chaves de condição	Tipo de condição	Tipo de valor	Operações de API	Tipo de política
`kms:SigningAlgorithm`	String	Valor único	`Sign` `Verify`	Políticas de chaves e políticas do IAM

Você pode usar a chave de `kms:SigningAlgorithm` condição para controlar o acesso às operações de Assinar e Verificar com base no valor do SigningAlgorithmparâmetro na solicitação. Essa chave de condição não tem efeito nas operações realizadas fora da AWS KMS, como a verificação de assinaturas com a chave pública em um par de chaves KMS assimétrico fora da. AWS KMS

O exemplo de política de chaves a seguir permite que os usuários que podem assumir a função `testers` usem a chave do KMS para assinar mensagens somente quando o algoritmo de assinatura usado para a solicitação é um algoritmo RSASSA_PSS, como `RSASSA_PSS_SHA512`.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/testers"
  },
  "Action": "kms:Sign",
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:SigningAlgorithm": "RSASSA_PSS*"
    }
  }
}
```

Consulte também

- kms: EncryptionAlgorithm
- the section called “kms: MacAlgorithm”

- the section called “kms: MessageType”

kms: ValidTo

AWS KMS chaves de condição	Tipo de condição	Tipo de valor	Operações de API	Tipo de política
`kms:ValidTo`	Timestamp	Valor único	`ImportKeyMaterial`	Políticas de chaves e políticas do IAM

A chave de `kms:ValidTo` condição controla o acesso à ImportKeyMaterialoperação com base no valor do ValidToparâmetro na solicitação, que determina quando o material da chave importada expira. O valor é expresso no horário do Unix.

Por padrão, o parâmetro `ValidTo` é obrigatório em uma solicitação `ImportKeyMaterial`. No entanto, se o valor do ExpirationModelparâmetro for`KEY_MATERIAL_DOES_NOT_EXPIRE`, o `ValidTo` parâmetro é inválido. Você também pode usar a chave de ExpirationModel condição kms: para exigir o `ExpirationModel` parâmetro ou um valor de parâmetro específico.

A seguinte instrução de política de exemplo permite a um usuário importar material-chave em uma chave do KMS. A chave de condição `kms:ValidTo` limita a permissão para solicitações `ImportKeyMaterial` em que o valor `ValidTo` é menor que ou igual a `1546257599.0` (31 de dezembro de 2018 23:59:59).

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": "kms:ImportKeyMaterial",
  "Resource": "*",
  "Condition": {
    "NumericLessThanEquals": {
      "kms:ValidTo": "1546257599.0"
    }
  }
```

```
}
```

Consulte também

- kms: ExpirationModel
- kms: WrappingAlgorithm
- kms: WrappingKeySpec

kms: ViaService

AWS KMS chaves de condição	Tipo de condição	Tipo de valor	Operações de API	Tipo de política
`kms:ViaService`	String	Valor único	Operações de recursos de chaves do KMS	Políticas de chaves e políticas do IAM

A chave de `kms:ViaService` condição limita o uso de uma chave KMS às solicitações de AWS serviços especificados. Você pode especificar um ou mais serviços em cada chave de condição `kms:ViaService`. A operação deve ser uma operação de recurso de chave do KMS, ou seja, uma operação autorizada para uma chave do KMS específica. Para identificar as operações de recursos de chaves do KMS, na Tabela de ações e recursos, procure um valor de `KMS key` na coluna `Resources` para a operação.

Por exemplo, a seguinte instrução de política de chaves usa a chave de condição `kms:ViaService` para permitir que uma chave gerenciada pelo cliente seja usada para as ações especificadas somente quando a solicitação vem do Amazon EC2 ou do Amazon RDS na região Oeste dos EUA (Oregon) em nome de `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"
      ]
    }
  }
}
```

Também é possível usar uma chave de condição `kms:ViaService` para negar permissão para usar uma chave do KMS quando a solicitação é proveniente de serviços específicos. Por exemplo, a instrução de política a seguir usa uma chave de condição `kms:ViaService` para impedir que uma chave gerenciada pelo cliente seja usada para operações `Encrypt` quando a solicitação é proveniente do AWS Lambda em nome de `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 você usa a chave de condição `kms:ViaService`, o serviço faz a solicitação em nome de uma entidade principal na conta da Conta da AWS. Essas entidades principais deve ter as seguintes permissões:

- Permissão para usar a chave do KMS. A entidade principal precisa conceder essas permissões ao serviço integrado, de forma que o serviço possa usar a chave gerenciada pelo cliente em nome da entidade principal. Para ter mais informações, consulte Como os serviços da AWS, usam o AWS KMS.
- Permissão para usar o serviço integrado. Para obter detalhes sobre como dar aos usuários acesso a um AWS serviço que se integra ao AWS KMS, consulte a documentação do serviço integrado.

Todas as Chaves gerenciadas pela AWS usam uma chave de condição `kms:ViaService` no seu documento de política de chaves. Essa condição permite que a chave do KMS seja usada apenas para solicitações provenientes do serviço que criou a chave do KMS. Para ver a política principal de um Chave gerenciada pela AWS, use a GetKeyPolicyoperação.

A chave de condição `kms:ViaService` é válida no IAM e em declarações de políticas de chaves. Os serviços que você especificar devem ser integrados ao AWS KMS e compatíveis com a chave de condição `kms:ViaService`.

Serviços que oferecem suporte à chave de condição **`kms:ViaService`**

A tabela a seguir lista AWS os serviços que estão integrados AWS KMS e oferecem suporte ao uso da chave de `kms:ViaService` condição nas chaves gerenciadas pelo cliente. Os serviços desta tabela podem não estar disponíveis em todas as regiões. Use o `.amazonaws.com` sufixo do AWS KMS ViaService nome em todas as AWS partições.

Note

Talvez seja necessário rolar horizontalmente ou verticalmente para ver todos os dados nessa tabela.

Nome do serviço	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 do Amazon Chime	chimevoiceconnector. *AWS_region* .amazonaws.com
AWS CodeArtifact	codeartifact. *AWS_region* .amazonaws.com
CodeGuru Revisor da Amazon	codeguru-reviewer. *AWS_region* .amazonaws.com
Amazon Comprehend	comprehend. *AWS_region* .amazonaws.com
Amazon Connect	connect.*AWS_region* .amazonaws.com
Amazon Connect Customer Profiles	profile.*AWS_region* .amazonaws.com

Nome do serviço	AWS KMS ViaService nome
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` (somente EBS)
Amazon Elastic Container Registry (Amazon ECR)	`ecr.`*`AWS_region`*` .amazonaws.com`
Amazon Elastic File System (Amazon EFS)	`elasticfilesystem.`*`AWS_region`*` .amazonaws.com`
Amazon ElastiCache	Inclua os dois ViaService nomes no valor da chave de condição: • `elasticache.`*`AWS_region`*` .amazonaws.com` • `dax.`*`AWS_region`*` .amazonaws.com`
AWS Elemental MediaTailor	`mediatailor.`*`AWS_region`*` .amazonaws.com`
AWS Resolução de entidades	`entityresolution.`*`AWS_region`*` .amazonaws.com`

Nome do serviço	AWS KMS ViaService nome
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
Amazon Keyspaces (para Apache Cassandra)	cassandra. *AWS_region* .amazonaws.com
Amazon Kinesis	kinesis.*AWS_region* .amazonaws.com
Amazon Data Firehose	firehose. *AWS_region* .amazonaws.com
Amazon Kinesis Video Streams	kinesisvideo. *AWS_region* .amazonaws.com
AWS Lambda	lambda.*AWS_region* .amazonaws.com
Amazon Lex	lex.*AWS_region* .amazonaws.com

Nome do serviço	AWS KMS ViaService nome
AWS License Manager	`license-manager.` *`AWS_region`* `.amazonaws.com`
Amazon Location Service	`geo.`*`AWS_region`* `.amazonaws.com`
Amazon Lookout for Equipment	`lookoutequipment.` *`AWS_region`* `.amazonaws.com`
Amazon Lookout for Metrics	`lookoutmetrics.` *`AWS_region`* `.amazonaws.com`
Amazon Lookout for Vision	`lookoutvision.` *`AWS_region`* `.amazonaws.com`
Amazon Macie	`macie.`*`AWS_region`* `.amazonaws.com`
AWS Mainframe Modernization	`m2.`*`AWS_region`* `.amazonaws.com`
Amazon Managed Blockchain	`managedblockchain.` *`AWS_region`* `.amazonaws.com`
Amazon Managed Streaming for Apache Kafka (Amazon MSK)	`kafka.`*`AWS_region`* `.amazonaws.com`
Amazon Managed Workflows for Apache Airflow (MWAA)	`airflow.`*`AWS_region`* `.amazonaws.com`
Amazon MemoryDB para 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`

Nome do serviço	AWS KMS ViaService nome
AWS HealthOmics	omics.*AWS_region* .amazonaws.com
OpenSearch Serviço Amazon	es.*AWS_region* .amazonaws.com , aoss.*AWS_region* .amazonaws.com
AWS Proton	proton.*AWS_region* .amazonaws.com
Amazon Quantum Ledger Database (Amazon QLDB)	qldb.*AWS_region* .amazonaws.com
Insights de Performance do Amazon RDS	rds.*AWS_region* .amazonaws.com
Amazon Redshift	redshift. *AWS_region* .amazonaws.com
Editor de consultas do Amazon Redshift V2	sqlworkbench. *AWS_region* .amazonaws.com
Amazon Redshift Serverless	redshift-serverless. *AWS_region* .amazonaws.com
Amazon Rekognition	rekognition. *AWS_region* .amazonaws.com
Amazon Relational Database Service (Amazon RDS)	rds.*AWS_region* .amazonaws.com
Armazenamento de dados replicado da 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

Nome do serviço	AWS KMS ViaService nome
Amazon Simple Email Service (Amazon SES)	`ses.`*`AWS_region`*` .amazonaws.com`
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 Contatos	`ssm-contacts.`*`AWS_region`*` .amazonaws.com`
Amazon Timestream	`timestream.`*`AWS_region`*` .amazonaws.com`
Amazon Translate	`translate.`*`AWS_region`*` .amazonaws.com`
Acesso Verificado pela 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`

Nome do serviço	AWS KMS ViaService nome
Amazon WorkSpaces Web	`workspaces-web.` *`AWS_region`* `.amazonaws.com`
AWS X-Ray	`xray.`*`AWS_region`*` .amazonaws.com`

kms: WrappingAlgorithm

AWS KMS chaves de condição	Tipo de condição	Tipo de valor	Operações de API	Tipo de política
`kms:WrappingAlgorithm`	String	Valor único	`GetParametersForImport`	Políticas de chaves e políticas do IAM

Essa chave de condição controla o acesso à GetParametersForImportoperação com base no valor do WrappingAlgorithmparâmetro na solicitação. Você pode usar essa condição para exigir que os principais usem determinado algoritmo para criptografar material de chaves durante o processo de importação. As solicitações para a chave pública e o token de importação exigidos falham quando especificam um algoritmo de empacotamento diferente.

A instrução de política de exemplo a seguir usa a chave de condição `kms:WrappingAlgorithm` para dar ao usuário de exemplo permissão para chamar a operação `GetParametersForImport`, mas o impede de usar o algoritmo de empacotamento `RSAES_OAEP_SHA_1`. Quando o `WrappingAlgorithm` na solicitação `GetParametersForImport` é `RSAES_OAEP_SHA_1`, a operação falha.

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

```
    "StringNotEquals": {
      "kms:WrappingAlgorithm": "RSAES_OAEP_SHA_1"
    }
  }
}
```

Consulte também

- kms: ExpirationModel
- kms: ValidTo
- kms: WrappingKeySpec

kms: WrappingKeySpec

AWS KMS chaves de condição	Tipo de condição	Tipo de valor	Operações de API	Tipo de política
`kms:WrappingKeySpec`	String	Valor único	`GetParametersForImport`	Políticas de chaves e políticas do IAM

Essa chave de condição controla o acesso à GetParametersForImportoperação com base no valor do WrappingKeySpecparâmetro na solicitação. Você pode usar essa condição para exigir que as entidades principais usem determinado tipo de chave pública durante o processo de importação. Se a solicitação especifica um tipo de chave diferente, ela falha.

Como o único valor válido para o valor do parâmetro `WrappingKeySpec` é `RSA_2048`, impedir que os usuários usem esse valor efetivamente os impede de usar a operação `GetParametersForImport`.

A declaração de política de exemplo a seguir usa a chave de condição `kms:WrappingAlgorithm` para exigir que `WrappingKeySpec` na solicitação seja `RSA_4096`.

```
{
  "Effect": "Allow",
  "Principal": {
```

```
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": "kms:GetParametersForImport",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:WrappingKeySpec": "RSA_4096"
    }
  }
}
```

Consulte também

- kms: ExpirationModel
- kms: ValidTo
- kms: WrappingAlgorithm

AWS KMS chaves de condição para AWS Nitro Enclaves

AWS O Nitro Enclaves é um recurso do Amazon EC2 que permite criar ambientes computacionais isolados chamados enclaves para proteger e processar dados altamente confidenciais. AWS KMS fornece chaves de condição para apoiar os AWS Nitro Enclaves. Essas chaves de condições são efetivas somente AWS KMS para solicitações de um Nitro Enclave.

Quando você chama as operações Decrypt, GenerateDataKeyGenerateDataKeyPair, ou GenerateRandomAPI com o documento de atestado assinado de um enclave, essas APIs criptografam o texto simples na resposta sob a chave pública do documento de atestado e retornam texto cifrado em vez de texto sem formatação. Esse texto cifrado pode ser descriptografado apenas usando a chave privada no enclave. Para ter mais informações, consulte Como o AWS Nitro Enclaves usa o AWS KMS.

As seguintes chaves de condição permitem limitar as permissões para essas operações com base no conteúdo do documento de atestado assinado. Antes de permitir uma operação, AWS KMS compara o documento de atestado do enclave com os valores nessas chaves de condição. AWS KMS

kmRecipientAttestation: 384 ImageSha

AWS KMS Chaves de condição	Tipo de condição	Tipo de valor	Operações de API	Tipo de política

`kms:RecipientAttestation:ImageSha384`	String	Valor único	`Decrypt`
			`GenerateDataKey`
			`GenerateDataKeyPair`
			`GenerateRandom`
				Políticas de chaves e políticas do IAM

A chave de condição `kms:RecipientAttestation:ImageSha384` controla o acesso a `Decrypt`, `GenerateDataKey`, `GenerateDataKeyPair` e `GenerateRandom` com uma chave do KMS quando o resumo da imagem do documento de atestado assinado na solicitação corresponde ao valor na chave de condição. O valor `ImageSha384` corresponde a PCR0 no documento de atestado. Essa chave de condição só é efetiva quando o `Recipient` parâmetro na solicitação especifica um documento de atestação assinado para um AWS enclave Nitro.

Esse valor também está incluído em CloudTraileventos AWS KMS para solicitações de enclaves Nitro.

> **Note**
>
> Essa chave de condição é válida em declarações de políticas de chaves e declarações de políticas do IAM, mesmo que não apareça no console do IAM ou na Referência de autorização de serviço do IAM.

Por exemplo, a declaração de política chave a seguir permite que a `data-processing` função use a chave KMS para descriptografar, GenerateDataKey, GenerateDataKeyPaire operações. GenerateRandom A chave de condição `kms:RecipientAttestation:ImageSha384` permite as operações somente quando o valor de resumo da imagem (PCR0) do documento de atestado

na solicitação corresponde ao valor de resumo da imagem na condição. Essa chave de condição só é efetiva quando o `Recipient` parâmetro na solicitação especifica um documento de atestação assinado para um AWS enclave Nitro.

Se a solicitação não incluir um documento de atestação válido de um enclave AWS Nitro, a permissão será negada porque essa condição não foi satisfeita.

```
{
  "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
    }
  }
}
```

km:: PCR RecipientAttestation <PCR_ID>

AWS KMS Chaves de condição	Tipo de condição	Tipo de valor	Operações de API	Tipo de política

`kms:RecipientAttestation:PCR<PCR_ID>`	String	Valor único	`Decrypt`
			`GenerateDataKey`
			`GenerateDataKeyPair`
				Políticas de chaves e políticas do IAM

AWS KMS Chaves de condição	Tipo de condição	Tipo de valor	Operações de API	Tipo de política
			`GenerateRandom`	

A chave de condição `kms:RecipientAttestation:PCR<PCR_ID>` permite solicitações `Decrypt`, `GenerateDataKey`, `GenerateDataKeyPair` e `GenerateRandom` com uma chave do KMS somente quando os registros de configuração de plataforma (PCRs) do documento de atestado assinado na solicitação correspondem aos PCRs na chave de condição. Essa chave de condição só é efetiva quando o `Recipient` parâmetro na solicitação especifica um documento de atestação assinado de um enclave Nitro. AWS

Esse valor também está incluído em CloudTraileventos que representam solicitações AWS KMS para enclaves Nitro.

> **Note**
>
> Essa chave de condição é válida em declarações de políticas de chaves e declarações de políticas do IAM, mesmo que não apareça no console do IAM ou na Referência de autorização de serviço do IAM.

Para especificar um valor de PCR, use o seguinte formato. Concatene o ID do PCR com o nome da chave da condição. O valor so PCR deve ser uma string hexadecimal minúscula de até 96 bytes.

```
"kms:RecipientAttestation:PCRPCR_ID": "PCR_value"
```

Por exemplo, a chave de condição a seguir especifica um valor específico para PCR1, que corresponde ao hash do kernel usado para o enclave e o processo de bootstrap.

```
kms:RecipientAttestation:PCR1:
 "0x1abcdef2abcdef3abcdef4abcdef5abcdef6abcdef7abcdef8abcdef9abcdef8abcdef7abcdef6abcdef5abcdef
```

Por exemplo, a instrução de política de chave a seguir permite que a função `data-processing` use a chave do KMS para a operação Decrypt.

A chave de condição `kms:RecipientAttestation:PCR` nessa instrução permite a operação somente quando o valor PCR1 no documento de atestado assinado na solicitação corresponde ao valor `kms:RecipientAttestation:PCR1` na condição. Use a política a`StringEqualsIgnoreCase` para exigir uma comparação sem distinção entre maiúsculas e minúsculas dos valores de PCR.

Se a solicitação não incluir um documento de atestado, a permissão será negada porque essa condição não foi atendida.

```
{
  "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 para AWS KMS

O controle de acesso baseado em atributos (ABAC) é uma estratégia de autorização que define permissões com base em atributos. O AWS KMS oferece suporta ao ABAC, permitindo que você controle o acesso às suas chaves gerenciadas pelo cliente com base nas etiquetas e nos aliases associados às chaves do KMS. As chaves de condição de etiqueta e alias que habilitam o ABAC no AWS KMS fornecem uma maneira eficiente e flexível de autorizar as entidades principais a usar chaves do KMS sem editar políticas ou gerenciar concessões. Porém, você deve usar esse recurso com cuidado, para que as entidades principais não sejam tenham o acesso inadvertidamente permitido ou negado.

Se você usar ABAC, esteja ciente de que a permissão para gerenciar etiquetas e aliases agora é uma permissão de controle de acesso. Certifique-se de conhecer as etiquetas e os aliases existentes em todas as chaves do KMS antes de implantar uma política que depende de etiquetas ou aliases.

Tome precauções razoáveis ao adicionar, excluir e atualizar aliases e ao marcar e desmarcar chaves. Conceda permissões para gerenciar etiquetas e aliases apenas às entidades principais que precisam deles e limite as etiquetas e os aliases que eles podem gerenciar.

> **Observações**
>
> Ao usar o ABAC para o AWS KMS, tenha cuidado ao conceder permissão a entidades principais para gerenciar etiquetas e aliases. A alteração de uma etiqueta ou de um alias pode permitir ou negar permissão para uma chave do KMS. Os administradores de chaves que não tiverem permissão para alterar políticas de chaves ou criar concessões poderão controlar o acesso às chaves do KMS se tiverem permissão para gerenciar etiquetas ou aliases.
>
> Pode levar até cinco minutos para que alterações de etiqueta e alias afetem a autorização de chaves do KMS. Alterações recentes podem estar visíveis em operações de API antes de afetarem a autorização.
>
> Para controlar o acesso a uma chave do KMS com base em seu alias, você deve usar uma chave de condição. Você não pode usar um alias para representar uma chave do KMS no elemento `Resource`de uma instrução de política. Quando um alias é exibido no elemento `Resource`, a instrução de política aplica-se a esse alias, e não à chave do KMS associada.

Saiba mais

- Para obter detalhes sobre o suporte do AWS KMSpara o ABAC, incluindo exemplos, consulte Usar aliases para controlar o acesso a chaves do KMSe Usar etiquetas para controlar o acesso a chaves do KMS.
- Para informações mais gerais sobre como usar etiquetas para controlar o acesso a recursos da AWS, consulte O que é o ABAC para a AWS? eControlar o acesso a recursos do AWS usando etiquetas de recursos, no Manual do usuário do IAM.

Chaves de condição de ABAC para o AWS KMS

Para autorizar o acesso a chaves do KMS com base em suas etiquetas e aliases, use as seguintes chaves de condição em uma política de chaves ou política do IAM.

Chave de condição para ABAC	Descrição	Tipo de política	Operações do AWS KMS
leis: ResourceTag	A etiqueta (chave e valor) na chave do KMS corresponde à etiqueta (chave e valor) ou ao padrão de etiqueta na política	Somente política do IAM	Operações de recursos de chaves do KMS [2]
aws:RequestTag//tecla de tag	A etiqueta (chave e valor) na solicitação corresponde à etiqueta (chave e valor) ou ao padrão de etiqueta na política	Políticas de chaves e políticas do IAM[1]	TagResource, UntagResource
leis: TagKeys	Chaves de etiqueta na solicitação correspondem a chaves de etiqueta na política	Políticas de chaves e políticas do IAM[1]	TagResource, UntagResource
kms: ResourceAliases	Aliases associados à chave do KMS correspondem a aliases ou padrões de alias na política	Somente política do IAM	Operações de recursos de chaves do KMS [2]
kms: RequestAlias	O alias que representa a chave do KMS na solicitação corresponde ao alias ou aos padrões de alias na política.	Políticas de chaves e políticas do IAM[1]	Operações criptográficas, DescribeKeyGetPublicKey

[1]Qualquer chave de condição que possa ser usada em uma política de chaves também pode ser usada em uma política do IAM, mas somente sea política de chaves a permitir.

[2]A operação de recurso de chave do KMS é uma operação autorizada para uma chave do KMS específica. Para identificar as operações de recursos de chaves do KMS, no tabela de permissões do AWS KMS, procure um valor de chave do KMS na coluna `Resources`para a operação.

Por exemplo, é possível usar essas chaves de condição para criar as seguintes políticas.

- Uma política do IAM com `kms:ResourceAliases` que concede permissão para usar chaves do KMS com um alias específico ou um padrão de alias. Isso é um pouco diferente de políticas que dependem de etiquetas: Embora seja possível usar padrões de alias em uma política, cada alias deve ser exclusivo em uma região e Conta da AWS. Isso permite aplicar uma política a um conjunto selecionado de chaves do KMS sem listar os ARNs dessas chaves na instrução de política. Para adicionar ou remover chaves do KMS do conjunto, altere o alias da chave do KMS.
- Uma política de chaves com `kms:RequestAlias` que permite que as entidades principais usem uma chave do KMS em uma operação `Encrypt`, mas somente quando a solicitação `Encrypt` usa esse alias para identificar a chave do KMS.
- Uma política do IAM com `aws:ResourceTag/`*`tag-key`* que nega permissão para usar chaves do KMS com uma determinada chave de etiqueta e um valor de etiqueta. Isso permite aplicar uma política a um conjunto selecionado de chaves do KMS sem listar os ARNs dessas chaves na instrução de política. Para adicionar ou remover chaves do KMS do conjunto, marque ou desmarque a chave do KMS.
- Uma política do IAM com `aws:RequestTag/`*`tag-key`* que permite que as entidades principais excluam somente etiquetas `"Purpose"="Test"` de chaves do KMS.
- Uma política do IAM com `aws:TagKeys` que nega permissão para marcar ou desmarcar uma chave do KMS com uma chave de etiqueta `Restricted`.

O ABAC torna o gerenciamento de acesso flexível e escalável. Por exemplo, você pode usar a chave de condição `aws:ResourceTag/`*`tag-key`* para criar uma política do IAM que permite que as entidades principais usem uma chave do KMS para operações especificadas somente quando essa chave tem uma etiqueta `Purpose=Test`. A política aplica-se a todas as chaves do KMS em todas as regiões da Conta da AWS.

Quando anexada a um usuário ou função, a seguinte política do IAM permite que as entidades principais usem todas as chaves do KMS existentes com uma etiqueta `Purpose=Test` para as operações especificadas. Para fornecer esse acesso a chaves do KMS novas ou existentes, não é

necessário alterar a política. Basta anexar a etiqueta `Purpose=Test`às chaves do KMS. Da mesma forma, para remover esse acesso das chaves do KMS com uma etiqueta `Purpose=Test`, edite ou exclua essa etiqueta.

```
{
  "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"
        }
      }
    }
  ]
}
```

No entanto, se você usar esse recurso, tenha cautela ao gerenciar etiquetas e aliases. Operações de adicionar, alterar ou excluir uma marca ou alias podem inadvertidamente permitir ou negar acesso a uma chave do KMS. Os administradores de chaves que não tiverem permissão para alterar políticas de chaves ou criar concessões poderão controlar o acesso às chaves do KMS se tiverem permissão para gerenciar etiquetas e aliases. Para atenuar esse risco, considerelimitar permissões para gerenciar etiquetas ealiases. Por exemplo, é possível permitir que apenas as entidades principais selecionadas gerenciem etiquetas do `Purpose=Test`. Para obter mais detalhes, consulte Usar aliases para controlar o acesso a chaves do KMS e Usar etiquetas para controlar o acesso a chaves do KMS.

Etiquetas ou aliases?

O AWS KMS oferece suporte ao ABAC com etiquetas e aliases. Ambas as opções proporcionam uma estratégia de controle de acesso flexível e escalável, mas são ligeiramente diferentes uma da outra.

Você pode optar por usar etiquetas ou aliases com base em seus padrões de uso específicos da AWS. Por exemplo, se você já concedeu permissões de marcação para a maioria dos administradores, talvez seja mais fácil controlar uma estratégia de autorização baseada em aliases. Ou, se você estiver se aproximando da cota de aliases por chave do KMS, talvez prefira uma estratégia de autorização baseada em etiquetas.

Os benefícios a seguir são de interesse geral.

Benefícios do controle de acesso baseado em tags

- O mesmo mecanismo de autorização para diferentes tipos de recursos da AWS.

  É possível usar a mesma etiqueta ou chave de etiqueta para controlar o acesso a vários tipos de recursos, como cluster do Amazon Relational Database Service (Amazon RDS), volume do Amazon Elastic Block Store (Amazon EBS) e chave do KMS. Esse recurso permite diversos modelos de autorização diferentes que são mais flexíveis que o controle de acesso baseado em função tradicional.
- Autorize o acesso a um grupo de chaves do KMS.

  É possível usar etiquetas para gerenciar o acesso a um grupo de chaves do KMS na mesma região e Conta da AWS. Atribua a mesma etiqueta ou chave de etiqueta às chaves do KMS qye você escolher. Em seguida, crie uma declaração easy-to-maintain de política simples baseada na tag ou na chave da tag. Para adicionar ou remover uma chave do KMS do seu grupo de autorização, adicione ou remova a etiqueta: não é necessário editar a política.

Benefícios do controle de acesso baseado em alias

- Autorize o acesso a operações de criptografia com base em aliases.

  A maioria das condições de política baseadas em solicitações para atributos, incluindo aws:RequestTag/tag-key, afetam somente as operações que adicionam, editam ou excluem o atributo. Mas a chave kms: RequestAlias condition controla o acesso às operações criptográficas com base no alias usado para identificar a chave KMS na solicitação. Por exemplo, você pode conceder uma permissão à entidade principal para usar uma chave do KMS em uma operação `Encrypt`, mas somente quando o valor do parâmetro `KeyIdéalias/restricted-key-1`. Para atender a essa condição, é necessário o seguinte:

  - A chave do KMS deve estar associada a esse alias.
  - A solicitação deve usar o alias para identificar a chave do KMS.

- A entidade principal deve ter permissão para usar a chave do KMS sujeita à condição `kms:RequestAlias`.

  Isso é particularmente útil quando suas aplicações costumam usar nomes de alias ou ARNs de alias para fazer referência a chaves do KMS.

- Forneça permissões muito limitadas.

  O alias deve ser exclusivo em uma região e Conta da AWS. Como resultado, o ato de conceder acesso para as entidades principais a uma chave do KMS baseada em um alias pode ser muito mais restritivo do que o conceder acesso para eles com base em uma etiqueta. Diferentemente de aliases, etiquetas podem ser atribuídas a várias chaves do KMS na mesma conta e região. Se você escolher, é possível usar um padrão de alias, como`alias/test*`, a fim de conceder acesso para as entidades principais a um grupo de chaves do KMS na mesma conta e região. Porém, permitir ou negar o acesso a um alias específico possibilita um controle muito rigoroso sobre as chaves do KMS.

Solução de problemas com o ABAC para o AWS KMS

Controlar o acesso a chaves do KMS com base em etiquetas e aliases é uma estratégia conveniente e poderosa. No entanto, ela está propensa a alguns erros previsíveis que convém evitar.

Acesso alterado devido a mudanças de etiqueta

Se uma etiqueta for excluída ou seu valor for alterado, as entidades principais que tiverem acesso a uma chave do KMS com base apenas nessa etiqueta terão acesso negado à chave do KMS. Isso também pode acontecer quando uma etiqueta incluída em uma instrução de política de negação é adicionada a uma chave do KMS. Adicionar uma etiqueta relacionada a uma política a uma chave do KMS pode permitir acesso a entidades principais que não devem ter esse acesso a uma chave do KMS.

Por exemplo, suponha que uma entidade principal tenha acesso a uma chave do KMS com base na etiqueta `Project=Alpha`, como a permissão fornecida pelo seguinte exemplo de instrução de política do IAM.

```
{
  "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 a etiqueta for excluída dessa chave do KMS ou se o valor da etiqueta for alterado, a entidade principal não terá mais permissão para usar a chave do KMS nas operações especificadas. Isso pode ficar evidente quando o diretor tenta ler ou gravar dados em um AWS serviço que usa uma chave gerenciada pelo cliente. Para rastrear a alteração da tag, revise seus CloudTrail registros TagResourceou UntagResource entradas.

Para restaurar o acesso sem atualizar a política, altere as etiquetas na chave do KMS. Essa ação tem impacto mínimo diferente de um breve período em que está entrando em vigor no AWS KMS. Para evitar um erro como esse, conceda permissões de marcação e desmarcação apenas a entidades principais que precisem delas elimite as permissões de marcação a etiquetas que eles precisam gerenciar. Antes de alterar uma etiqueta, pesquise políticas para detectar o acesso que depende dessa etiqueta e obtenha chaves do KMS em todas as regiões que tenham a etiqueta. Você pode considerar criar um CloudWatch alarme da Amazon quando determinadas tags forem alteradas.

Alteração do acesso devido a mudanças de alias

Se um alias for excluído ou associado a uma chave do KMS diferente, as entidades principais que tiverem acesso a essa chave do KMS com base apenas nesse alias terão acesso negado a ela. Isso também pode acontecer quando um alias associado a uma chave do KMS é incluído em uma instrução de política de negação. Adicionar um alias relacionado a uma política a uma chave do KMS também pode permitir acesso a entidades principais que não devem ter esse acesso a uma chave do KMS.

Por exemplo, a seguinte declaração de política do IAM usa a chave de ResourceAliases condição kms: para permitir o acesso às chaves KMS em diferentes regiões da conta com qualquer um dos aliases especificados.

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

Para rastrear a alteração do alias, revise seus CloudTrail registros de CreateAliasUpdateAlias, e DeleteAliasentradas.

Para restaurar o acesso sem atualizar a política, modifique o alias associado à chave do KMS. Como cada alias pode ser associado a apenas uma chave do KMS em uma conta e região, o gerenciamento de aliases é um pouco mais difícil que o de etiquetas. Restaurar o acesso a algumas das entidades principais em uma chave do KMS pode negar acesso para as mesmas ou outras entidades principais a uma chave do KMS diferente.

Para evitar esse erro, conceda permissões de gerenciamento de alias somente às entidades principais que precisam dele e limite suas permissões de gerenciamento de alias para aliases que elas precisam gerenciar. Antes de atualizar ou excluir um alias, pesquise políticas para detectar o acesso que depende do alias e localize chaves do KMS em todas as regiões associadas a ele.

Acesso negado devido à cota de aliases

Os usuários autorizados a usar uma chave KMS por meio de uma ResourceAliases condição kms: receberão uma `AccessDenied` exceção se a chave KMS exceder os aliases padrão por cota de chave KMS para essa conta e região.

Para restaurar o acesso, exclua aliases associados à chave do KMS, para que esta esteja em conformidade com a cota. Outra opção é usar um mecanismo alternativo para conceder aos usuários acesso à chave do KMS.

Alteração de autorização atrasadas

Alterações feitas em etiquetas e aliases podem levar até cinco minutos para afetar a autorização de chaves do KMS. Como resultado, uma alteração de etiqueta ou alias pode ser refletida nas respostas das operações da API antes que estas afetem a autorização. Esse atraso provavelmente será maior que o breve atraso de consistência final que afeta a maioria das operações do AWS KMS.

Por exemplo, você pode ter uma política do IAM que permita que certas entidades principais utilizem qualquer chave do KMS com uma etiqueta `"Purpose"="Test"`. Em seguida, você adiciona a etiqueta `"Purpose"="Test"` a uma chave do KMS. Embora a TagResourceoperação seja concluída e a ListResourceTagsresposta confirme que a tag está atribuída à chave KMS, os diretores podem não ter acesso à chave KMS por até cinco minutos.

Para evitar erros, crie esse atraso esperado no seu código.

Solicitações com falha devido a atualizações de alias

Quando você atualiza um alias, associa um alias existente a uma chave do KMS diferente.

A descriptografia e as ReEncryptsolicitações que especificam o nome do alias ou o ARN do alias podem falhar porque o alias agora está associado a uma chave KMS que não criptografou o texto cifrado. Essa situação geralmente retorna uma `IncorrectKeyException` ou `NotFoundException`. Ou, se a solicitação não tiver o parâmetro `KeyId` ou `DestinationKeyId`, a operação pode falhar com uma exceção `AccessDenied` porque o autor da chamada não tem mais acesso à chave do KMS que criptografou o texto cifrado.

Você pode rastrear a alteração examinando CloudTrail os registros de CreateAliasUpdateAlias, e as entradas de DeleteAliasregistro. Você também pode usar o valor do `LastUpdatedDate` campo na ListAliasesresposta para detectar uma alteração.

Por exemplo, o ListAliasesexemplo de resposta a seguir mostra que o `ProjectAlpha_Test` alias na `kms:ResourceAliases` condição foi atualizado. Como resultado, as entidades principais que têm acesso com base nesse alias perdem acesso à chave do KMS anteriormente associada. Em vez disso, elas têm acesso à chave do KMS recém-associada.

```
$ 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
        }
    ]
}
```

A solução para essa alteração não é simples. É possível atualizar o alias novamente para associá-lo à chave do KMS original. No entanto, antes de fazer isso, você precisa considerar o efeito dessa alteração na chave do KMS atualmente associada. Se as entidades principais usaram a última chave do KMS em operações de criptografia, talvez elas precisem de acesso contínuo a ela. Nesse caso, convém atualizar a política para garantir que as entidades principais tenham permissão para usar as duas chaves do KMS.

Para evitar um erro como esse, antes de atualizar um alias, pesquise políticas para detectar o acesso que depende do alias. Em seguida, obtenha chaves do KMS em todas as regiões associadas a esse alias. Conceda permissões de gerenciamento de alias somente às entidades principais que precisam dele e limite suas permissões de gerenciamento de alias para aliases que elas precisam gerenciar.

Permitir que usuários de outras contas usem uma chave do KMS

É possível permitir que usuários ou perfis em uma Conta da AWS diferente usem uma chave do KMS em sua conta. O acesso entre contas requer permissão na política de chaves da chave do KMS e em uma política do IAM na conta do usuário externo.

A permissão entre contas é efetiva apenas nas seguintes operações:

- Operações criptográficas
- CreateGrant
- DescribeKey
- GetKeyRotationStatus
- GetPublicKey
- ListGrants
- RetireGrant
- RevokeGrant

Se você conceder a um usuário em outra conta permissão para outras operações, essas permissões não terão efeito. Por exemplo, se você der a um principal em uma conta diferente kms: ListKeys permissão em uma política do IAM ou kms: ScheduleKeyDeletion permissão em uma chave KMS em uma política de chaves, as tentativas do usuário de chamar essas operações em seus recursos ainda falharão.

Para obter detalhes sobre como usar chaves do KMS em contas diferentes para operações do AWS KMS, consulte a coluna Uso entre contas em AWS KMS permissões e Usar chaves do KMS em outras contas. Existe também uma seção Uso entre contas em cada descrição da API na Referência de APIs do AWS Key Management Service.

> **Warning**
>
> Tenha cautela ao conceder permissões para as entidades principais usarem suas chaves do KMS. Sempre que possível, siga o princípio de menor privilégio. Conceda aos usuários acesso apenas às chaves do KMS necessárias para a conclusão de suas operações. Além disso, tenha cautela ao usar qualquer chave do KMS desconhecida, especialmente uma chave do KMS em outra conta. Usuários mal-intencionados podem conceder a você

permissões para usar a chave do KMS deles para obter informações sobre você ou sua conta.
Para obter informações sobre como usar políticas para proteger os recursos em sua conta, consulte Práticas recomendadas para políticas do IAM.

Para conceder permissão para usuários e funções usarem uma chave do KMS em outra conta, você deve usar dois tipos diferentes de políticas:

- A política de chaves da chave do KMS deve conceder à conta externa (ou aos usuários e às funções na conta externa) permissão para usar a chave do KMS. A política de chaves está na conta proprietária da chave do KMS.
- Políticas do IAM na conta externa devem delegar as permissões de políticas de chaves para seus usuários e funções. Essas políticas são definidas na conta externa e concedem permissões a usuários e funções nessa conta.

A política de chaves determina quem pode ter acesso à chave do KMS. A política do IAM determina quem tem acesso à chave do KMS. Sozinhas, nem a política de chaves, nem a política do IAM são suficientes: você deve alterar as duas.

Para editar a política de chaves, você pode usar a Exibição de Política nas PutKeyPolicyoperações AWS Management Console CreateKeyou usar as. Para obter ajuda sobre como definir a política de chaves ao criar uma chave do KMS, consulte Criar chaves do KMS que podem ser usadas por outras contas.

Para obter ajuda sobre como editar políticas do IAM, consulte Usando políticas do IAM com AWS KMS.

Para obter um exemplo que mostra como a política de chaves e as políticas do IAM funcionam em conjunto para permitir o uso de uma chave do KMS em uma conta diferente, consulte Exemplo 2: o usuário assume uma função com permissão para usar uma chave do KMS em outra Conta da AWS.

É possível visualizar as operações do AWS KMS entre contas resultantes na chave do KMS nos seus logs do AWS CloudTrail. Operações que usam chaves do KMS em outras contas são registradas na conta do autor da chamada e na conta do proprietário da chave do KMS.

Tópicos

- Etapa 1: Incluir uma declaração de política de chaves na conta local

- Etapa 2: Adicionar políticas do IAM à conta externa
- Criar chaves do KMS que podem ser usadas por outras contas
- Permitir o uso de chaves do KMS externas com Serviços da AWS
- Usar chaves do KMS em outras contas

> **Note**
>
> Os exemplos neste tópico mostram como usar uma política de chaves e uma política do IAM juntas para fornecer e limitar o acesso a uma chave do KMS. Estes exemplos genéricos não têm como objetivo representar as permissões que qualquer AWS service (Serviço da AWS) específico requer em uma chave do KMS. Para obter informações sobre as permissões de que um AWS service (Serviço da AWS) precisa, consulte o tópico de criptografia na documentação do serviço.

Etapa 1: Incluir uma declaração de política de chaves na conta local

A política de chaves de uma chave do KMS é o determinante principal de quem pode acessar a chave do KMS e quais operações podem ser realizadas. A política de chaves está sempre na conta proprietária da chave do KMS. Ao contrário de políticas do IAM, políticas de chaves não especificam um recurso. O recurso é a chave do KMS associada à política de chaves. Ao fornecer permissões entre contas, a política de chaves para a chave do KMS deve conceder à conta externa (ou aos usuários e perfis na conta externa) permissão para usar a chave do KMS.

Para conceder permissão a uma conta externa para usar a chave do KMS, adicione uma instrução à política de chaves que especifique a conta externa. No elemento `Principal` da política de chaves, insira o Amazon Resource Name (ARN) da conta externa.

Quando você especifica uma conta externa em uma política de chaves, os administradores do IAM na conta externa podem usar políticas do IAM para delegar essas permissões a todos os usuários e funções na conta externa. Eles também podem decidir quais ações especificadas na política de chaves os usuários e as funções podem executar.

As permissões concedidas à conta externa e suas entidades principais serão efetivas somente se a conta externa estiver habilitada na região que hospeda a chave do KMS e sua política de chaves. Para obter informações sobre regiões não habilitadas por padrão (“regiões de adesão”), consulte Gerenciar Regiões da AWS em Referência geral da AWS.

Por exemplo, suponha que você queira permitir que a conta 444455556666 use uma chave do KMS de criptografia simétrica na conta 111122223333. Para isso, adicione uma instrução de política, como a instrução no exemplo a seguir, à política de chaves na conta 111122223333. Essa instrução de política permite que a conta externa (444455556666) use a chave do KMS em operações criptográficas para chaves do KMS de criptografia simétrica.

> **Note**
>
> O exemplo a seguir representa uma amostra de política de chaves para o compartilhamento de uma chave do KMS com outra conta. Substitua os valores de exemplo `Sid`, `Principal` e `Action` por valores válidos para o uso pretendido de sua chave do 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": "*"
}
```

Em vez de conceder permissão à conta externa, você pode especificar usuários e funções externos específicos na política de chaves. No entanto, esses usuários e funções não poderão usar a chave do KMS até que os administradores do IAM na conta externa associem as políticas do IAM adequadas às suas identidades. As políticas do IAM podem conceder permissão a todos ou a um subconjunto de usuários e funções externos especificados na política de chaves. E podem permitir todas ou um subconjunto das ações especificadas na política de chaves.

Especificar identidades em uma política de chaves restringe as permissões que os administradores do IAM na conta externa podem fornecer. No entanto, isso torna o gerenciamento de políticas com

duas contas mais complexo. Por exemplo, suponha que você precise adicionar um usuário ou uma função. É necessário adicionar essa identidade à política de chaves na conta que possui a chave do KMS e criar políticas do IAM na conta da identidade.

Para especificar determinados usuários ou funções externos em uma política de chaves, no elemento `Principal`, insira o Amazon Resource Name (ARN) de um usuário ou função na conta externa.

Por exemplo, a instrução de política de chaves exemplificada a seguir permite que `ExampleRole` na conta `444455556666` use uma chave do KMS na conta `111122223333`. Essa instrução de política de chaves permite que a conta externa (`444455556666`) use a chave do KMS em operações criptográficas para chaves do KMS de criptografia simétrica.

> **Note**
>
> O exemplo a seguir representa uma amostra de política de chaves para o compartilhamento de uma chave do KMS com outra conta. Substitua os valores de exemplo `Sid`, `Principal` e `Action` por valores válidos para o uso pretendido de sua chave do 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**
>
> Não defina a entidade principal como um asterisco (*) em qualquer instrução de política de chave que permita permissões, a menos que você utilize condições para limitar a política

de chave. Um asterisco dá à cada identidade em cada permissão da Conta da AWS para usar a chave do KMS, a menos que outra instrução de política negue essa permissão explicitamente. Usuários em outras Contas da AWS podem usar a chave do KMS sempre que tiverem as permissões correspondentes em suas próprias contas.

Você também precisa decidir quais permissões deseja conceder à conta externa. Para obter uma lista de permissões em chaves do KMS, consulte AWS KMS permissões.

É possível conceder permissão à conta externa para usar a chave do KMS em operações de criptografia e usar a chave do KMS com serviços da AWS que estão integrados ao AWS KMS. Para fazer isso, use a seção Key Users (Usuários de chaves) no AWS Management Console. Para obter detalhes, consulte Criar chaves do KMS que podem ser usadas por outras contas.

Para especificar outras permissões em políticas de chaves, edite o documento da política de chaves. Por exemplo, você pode conceder aos usuários permissão para descriptografar, mas não para criptografar, ou permissão para visualizar a chave do KMS, mas não para usá-la. Para editar o principal documento de política, você pode usar a Exibição de Política nas AWS Management Console PutKeyPolicyoperações CreateKeyou ou.

Etapa 2: Adicionar políticas do IAM à conta externa

A política de chaves na conta proprietária da chave do KMS define o intervalo válido de permissões. No entanto, os usuários e as funções na conta externa não poderão usar a chave do KMS até que você anexe as políticas do IAM que deleguem essas permissões ou use concessões para gerenciar o acesso à chave do KMS. As políticas do IAM são definidas na conta externa.

Se a política de chaves conceder permissão à conta externa, você poderá anexar as políticas do IAM a qualquer usuário ou função na conta. No entanto, se a política de chaves conceder permissão a usuários ou funções especificados, a política do IAM só poderá conceder essas permissões a todos ou a um subconjunto de usuários e funções especificados. Se uma política do IAM conceder acesso à chave do KMS para outros usuários ou funções externos, este não terá efeito.

A política de chaves também limita as ações na política do IAM. A política do IAM pode delegar todas as ações ou um subconjunto das ações especificadas na política de chaves. Se a política do IAM listar ações que não estão especificadas na política de chaves, essas permissões não terão efeito.

O seguinte exemplo de política do IAM permite que a entidade principal use a chave do KMS na conta `111122223333` para operações de criptografia. Para conceder essa permissão a usuários

e funções na conta 444455556666, associe a política aos usuários ou às funções na conta 444455556666.

> **Note**
>
> O exemplo a seguir representa uma amostra de política do IAM para o compartilhamento de uma chave do KMS com outra conta. Substitua os valores de exemplo `Sid`, `Resource` e `Action` por valores válidos para o uso pretendido de sua chave do 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"
}
```

Observe os seguintes detalhes sobre essa política:

- Ao contrário de políticas de chaves, as instruções de políticas do IAM não contêm o elemento `Principal`. Nas políticas do IAM, a identidade principal é aquela à qual a política está anexada.
- O elemento `Resource`na política do IAM identifica a chave do KMS que a entidade principal pode usar. Para especificar uma chave do KMS, adicione seu ARN de chave ao elemento `Resource`.
- É possível especificar mais de uma chave do KMS no elemento `Resource`. No entanto, se você não especificar chaves do KMS específicas no elemento `Resource`, poderá conceder acesso acidentalmente a mais chaves do KMS do que o desejado.
- Para permitir que o usuário externo use a chave do KMS com serviços da AWS que se integram ao AWS KMS, pode ser necessário adicionar permissões à política de chaves ou à política do IAM. Para obter detalhes, consulte Permitir o uso de chaves do KMS externas com Serviços da AWS.

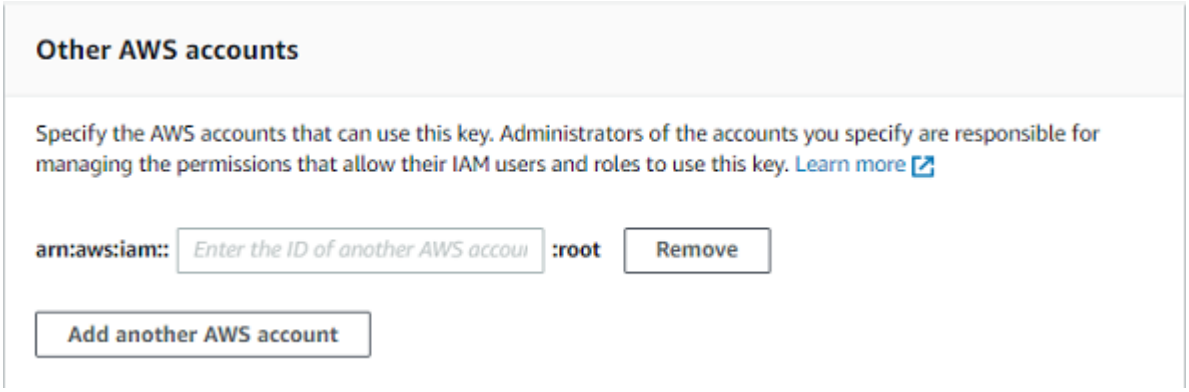
Para mais informações sobre como trabalhar com políticas do IAM, consulte Políticas do IAM.

Criar chaves do KMS que podem ser usadas por outras contas

Ao usar a CreateKeyoperação para criar uma chave KMS, você pode usar seu `Policy` parâmetro para especificar uma política de chaves que conceda a uma conta externa, ou usuários e funções externos, permissão para usar a chave KMS. Você também deve adicionar políticas do IAM à conta externa que delega essas permissões aos usuários e às funções dessa conta, mesmo quando estes últimos estão especificados na política de chaves. Você pode alterar a política de chaves a qualquer momento usando a PutKeyPolicyoperação.

Ao criar uma chave do KMS no AWS Management Console, você também cria sua política de chaves. Ao selecionar identidades nas seções Key Administrators (Administradores de chaves) e Key Users (Usuários de chaves), o AWS KMS adiciona instruções de política para essas identidades à política de chaves da chave do KMS.

A seção Key Users (Usuários de chaves) também permite adicionar contas externas como usuários de chaves.



Quando você insere o ID de uma conta externa, o AWS KMS adiciona duas declarações à política de chaves. Essa ação afeta somente a política de chaves. Os usuários e funções na conta externa não poderão usar a chave do KMS até que você anexe as políticas do IAM para conceder a eles algumas dessas permissões ou todas elas.

A primeira instrução de política concede à conta externa permissão para usar a chave do KMS em operações de criptografia.

> **Note**
>
> Os exemplos a seguir representam uma amostra de política de chaves para o compartilhamento de uma chave do KMS com outra conta. Substitua os valores de exemplo `Sid`, `Principal` e `Action` por valores válidos para o uso pretendido de sua chave do 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": "*"
}
```

A segunda instrução de política permite que a conta externa crie, visualize e revogue concessões na chave do KMS, mas somente quando a solicitação é proveniente de um serviço da AWS integrado ao AWS KMS. Essas permissões permitem que outros serviços da AWS, como os que criptografam dados do usuário, usem a chave do KMS.

Essas permissões são projetadas para chaves KMS que criptografam dados do usuário em AWS serviços, como a Amazon. WorkMail Esses serviços geralmente usam concessões para obter as permissões de que precisam para usar a chave do KMS em nome do usuário. Para obter detalhes, consulte Permitir o uso de chaves do KMS externas com Serviços da 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 essas permissões não atenderem às suas necessidades, você poderá editá-las na visualização de políticas do console ou usando a PutKeyPolicyoperação. Você pode especificar usuários e funções externos específicos, em vez de conceder permissão à conta externa. Você pode alterar as ações que a política especifica. E você pode usar condições globais e de política do AWS KMS para refinar as permissões.

Permitir o uso de chaves do KMS externas com Serviços da AWS

Você pode conceder a um usuário em outra conta permissão para usar sua chave do KMS com um serviço integrado ao AWS KMS. Por exemplo, um usuário em uma conta externa pode usar sua chave do KMS para criptografar os objetos em um bucket do Amazon S3 ou para criptografar os segredos que ele armazena no AWS Secrets Manager.

A política de chaves deve conceder ao usuário externo ou à conta do usuário externo a devida permissão para usar a chave do KMS. Além disso, você precisa vincular políticas do IAM à identidade que concede permissões ao usuário para usar o AWS service (Serviço da AWS). O serviço também pode exigir que os usuários tenham permissões adicionais na política de chaves ou na política do IAM. Para obter uma lista das permissões requeridas pelo AWS service (Serviço da AWS) em uma chave gerenciada pelo cliente, consulte o tópico Data Protection (Proteção de dados) no capítulo Security (Segurança) no guia do usuário ou no guia do desenvolvedor do serviço.

Usar chaves do KMS em outras contas

Se você tiver permissão para usar uma chave do KMS em uma Conta da AWS diferente, poderá usar essa chave do KMS no AWS Management Console, em AWS SDKs, na AWS CLI e no AWS Tools for PowerShell.

Para identificar uma chave do KMS em uma conta diferente em um comando shell ou solicitação de API, use os seguintes identificadores de chave.

- Para operações criptográficas, e DescribeKeyGetPublicKey, use o ARN da chave ou o alias ARN da chave KMS.
- Para CreateGrant, GetKeyRotationStatus, ListGrants, e RevokeGrant, use a chave ARN da chave KMS.

Se você inserir apenas um ID de chave ou um nome de alias, a AWS assumirá que a chave do KMS está na sua conta.

O console do AWS KMS não exibe chaves do KMS em outras contas, mesmo que você tenha permissão para usá-las. Além disso, as listas de chaves do KMS exibidas nos consoles de outros serviços da AWS não incluem chaves do KMS em outras contas.

Para especificar uma chave do KMS em uma conta diferente no console de um serviço da AWS, você deve inserir o ARN da chave ou o ARN do alias da chave do KMS. O identificador de chave necessário varia de acordo com o serviço e pode diferir entre o console de serviço e suas operações de API. Para obter detalhes, consulte a documentação do serviço.

Usar perfis vinculados ao serviço do AWS KMS

O AWS Key Management Service usa funções vinculadas a serviços do AWS Identity and Access Management (IAM). O perfil vinculado a serviço é um tipo exclusivo de perfil do IAM vinculado diretamente ao AWS KMS. As funções vinculadas a serviços são definidas pelo AWS KMS e incluem todas as permissões que o serviço requer para chamar outros serviços da AWS em seu nome.

Uma função vinculada ao serviço facilita a configuração do AWS KMS porque você não precisa adicionar as permissões necessárias manualmente. AWS KMS define as permissões de suas funções vinculadas ao serviço e, a menos que definido de outra forma, somente AWS KMS pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões. Essa política não pode ser anexada a nenhuma outra entidade do IAM.

Você pode excluir um perfil vinculado ao serviço somente depois de excluir os atributos relacionados. Isso protege seus recursos do AWS KMS, pois você não pode remover por engano as permissões de acesso aos recursos.

Para obter informações sobre outros serviços compatíveis com funções vinculadas a serviços, consulte Serviços da AWS compatíveis com o IAM e procure os serviços que apresentam Sim na coluna Função vinculada a serviço. Escolha um Sim com um link para visualizar a documentação do perfil vinculado a esse serviço.

Permissões da função vinculada ao serviço para armazenamento de chaves personalizado do AWS KMS

AWS KMSusa uma função vinculada ao serviço chamada AWSServiceRoleForKeyManagementServiceCustomKeyStorespara oferecer suporte a

armazenamentos de chaves personalizadas. Essa função vinculada ao serviço fornece ao AWS KMS permissão para ver seus clusters do AWS CloudHSM e criar a infraestrutura de rede para oferecer suporte a uma conexão entre seu armazenamento de chaves personalizado e seu cluster do AWS CloudHSM. O AWS KMS cria essa função somente quando você cria um armazenamento de chaves personalizado. Não é possível criar diretamente essa função vinculada a serviço.

A função vinculada a serviço AWSServiceRoleForKeyManagementServiceCustomKeyStores confia em `cks.kms.amazonaws.com` para assumir a função. Como resultado, somente o AWS KMS pode assumir essa função vinculada a serviço.

As permissões na função são limitadas às ações que o AWS KMS executa para conectar um armazenamento de chaves personalizado a um cluster do AWS CloudHSM. Ele não concede permissões adicionais ao AWS KMS. Por exemplo, o AWS KMS não tem permissão para criar, gerenciar ou excluir clusters, HSMs ou backups do AWS CloudHSM.

Para obter mais informações sobre a função AWSServiceRoleForKeyManagementServiceCustomKeyStores, incluindo uma lista de permissões e instruções sobre como visualizar a função, editar a descrição da função, excluir a função, e fazer com que o AWS KMS seja recriado, consulte Autorizar o AWS KMS a gerenciar recursos do AWS CloudHSM e do Amazon EC2.

Permissões de função vinculada ao serviço para chaves de várias regiões do AWS KMS

AWS KMSusa uma função vinculada ao serviço chamada AWSServiceRoleForKeyManagementServiceMultiRegionKeyspara oferecer suporte a chaves multirregionais. Essa função vinculada ao serviço concede permissão ao AWS KMS para sincronizar quaisquer alterações no material de chave de uma chave primária de várias regiões para suas chaves de réplica. O AWS KMS cria essa função somente quando você cria uma chave primária de várias regiões. Não é possível criar diretamente essa função vinculada a serviço.

A função vinculada a serviço AWSServiceRoleForKeyManagementServiceMultiRegionKeys confia em `mrk.kms.amazonaws.com` para assumir a função. Como resultado, somente o AWS KMS pode assumir essa função vinculada a serviço. As permissões na função estão limitadas às ações que o AWS KMS realiza para manter sincronizado o material de chave em chaves de várias regiões relacionadas. Ele não concede permissões adicionais ao AWS KMS.

Para obter mais informações sobre a função AWSServiceRoleForKeyManagementServiceMultiRegionKeys, incluindo uma lista de permissões

e instruções sobre como visualizar a função, editar a descrição da função, excluir a função, e fazer com que o AWS KMS seja recriado, consulte Autorizar o AWS KMS a sincronizar chaves de várias regiões.

Atualizações do AWS KMS para políticas gerenciadas pela AWS

Visualizar detalhes sobre atualizações em políticas gerenciadas pela AWS para o AWS KMS desde que esse serviço começou a rastrear essas alterações. Para obter alertas automáticos sobre alterações feitas nesta página, inscreva-se no feed RSS na página Histórico do documento do AWS KMS.

Alteração	Descrição	Data
AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy: atualizar para uma política existente.	AWS KMSadicionou as `ec2:DescribeNetworkInterfaces` permissões `ec2:DescribeVpcs` `ec2:DescribeNetworkAcls` ,, e para monitorar as alterações na VPC que contém seu AWS CloudHSM cluster para que AWS KMS possa fornecer mensagens de erro claras em caso de falhas.	10 de novembro de 2023
O AWS KMS iniciou o rastreamento das alterações	O AWS KMS começou a monitorar as alterações para as políticas gerenciadas da AWS.	10 de novembro de 2023

Usar TLS pós-quântico híbrido com o AWS KMS

O AWS Key Management Service (AWS KMS) é compatível com uma opção de troca de chaves pós-quântica híbrida para o protocolo de criptografia de rede Transport Layer Security (TLS). Você pode usar essa opção TLS ao se conectar aos endpoints de API do AWS KMS. Estamos oferecendo esse recurso antes que os algoritmos pós-quânticos sejam padronizados para que você possa

começar a testar o efeito desses protocolos de troca de chaves nas chamadas do AWS KMS. Esses recursos opcionais de troca de chaves pós-quânticas híbridas são, no mínimo, tão seguros quanto a criptografia TLS que usamos atualmente e provavelmente fornecerão benefícios adicionais de segurança em longo prazo. No entanto, eles afetam a latência e o throughput em comparação com os protocolos clássicos de troca de chaves em uso atualmente.

Os dados enviados para o AWS Key Management Service (AWS KMS) são protegidos em trânsito pela criptografia fornecida por uma conexão Transport Layer Security (TLS). Os pacotes de criptografia clássica aos quais o AWS KMS oferece suporte a sessões TLS tornam inviáveis os ataques de força bruta nos mecanismos de troca de chaves com a tecnologia atual. No entanto, se a computação quântica em grande escala se tornar prática no futuro, os pacotes de criptografia clássica usados nos mecanismos de troca de chaves TLS serão suscetíveis a esses ataques. Se você estiver desenvolvendo aplicações que dependem da confidencialidade de longo prazo de dados passados por uma conexão TLS, você deverá considerar um plano para migrar para criptografia pós-quântica antes que computadores quânticos de grande escala sejam disponibilizados para uso. A AWS está trabalhando para se preparar para este futuro, e queremos que você esteja bem preparado também.

Para proteger dados criptografados atualmente contra possíveis ataques futuros, a AWS está participando junto com a comunidade criptográfica no desenvolvimento de algoritmos quânticos ou pós-quânticos. Implementamos pacotes de codificação de troca de chaves pós-quânticas híbridas no AWS KMS que combinam elementos clássicos e pós-quânticos para garantir que sua conexão TLS seja, no mínimo, tão forte quanto seria com pacotes de codificação clássicos.

Esses pacotes de criptografia híbrida estão disponíveis para uso em suas workloads de produção na maioria das Regiões da AWS. No entanto, como as características de performance e os requisitos de largura de banda dos pacotes de criptografia híbrida são diferentes dos mecanismos clássicos de troca de chaves, recomendamos testá-los em suas chamadas de API do AWS KMS sob diferentes condições.

Feedback

Como sempre, agradecemos seu feedback e sua participação em nossos repositórios de código aberto. Gostaríamos especialmente de saber como sua infraestrutura interage com essa nova variante do tráfego TLS.

- Para fornecer feedback sobre esse tópico, use o link Feedback no canto superior direito desta página.

- Estamos desenvolvendo esses pacotes de criptografia híbrida em código aberto no s2n-tlsrepositório em. GitHub Para fornecer feedback sobre a usabilidade dos pacotes de criptografia ou compartilhar novas condições de teste ou resultados, crie uma ocorrência no repositório s2n-tls.
- Estamos escrevendo exemplos de código para usar o TLS pós-quântico híbrido AWS KMS aws-kms-pq-tls-example GitHubno repositório. Para fazer perguntas ou compartilhar ideias sobre como configurar seu cliente HTTP ou cliente AWS KMS para usar os pacotes de criptografia híbrida, crie uma ocorrência no repositório aws-kms-pq-tls-example.

Compatível Regiões da AWS

O TLS pós-quântico para o AWS KMS está disponível em todas as Regiões da AWS compatíveis com o AWS KMS, exceto para China (Pequim) e China (Ningxia).

> **Note**
>
> O AWS KMS não é compatível com o TLS pós-quântico híbrido para endpoints FIPS no AWS GovCloud (US).

Para obter uma lista de endpoints do AWS KMS para cada Região da AWS, consulte endpoints e cotas do AWS Key Management Service no Referência geral da Amazon Web Services. Para obter informações sobre endpoints do FIPS, consulte Endpoints do FIPS no Referência geral da Amazon Web Services.

Sobre a troca de chaves pós-quântica híbrida no TLS

AWS KMSO oferece suporte a pacotes de criptografia de troca de chaves pós-quânticas híbridas. É possível usar o AWS SDK for Java 2.x e o runtime comum da AWS em sistemas Linux para configurar um cliente HTTP que usa esses pacotes de codificação. Depois, sempre que você se conectar a um endpoint do AWS KMS com o cliente HTTP, os pacotes de criptografia híbrida serão usados.

Este cliente HTTP usa s2n-tls, que é uma implementação de código aberto do protocolo TLS. Os pacotes de codificação híbridos usados por s2n-tls são implementados apenas para troca de chaves, não para a criptografia de dados direta. Durante a troca de chaves, o cliente e o servidor calculam a chave que usarão para criptografar e descriptografar os dados na rede.

Os algoritmos utilizados por s2n-tls são um híbrido que combina o Elliptic Curve Diffie-Hellman (ECDH), um algoritmo clássico de intercâmbio de chaves atualmente utilizado no TLS, com Kyber,

um algoritmo de criptografia de chave pública e de estabelecimento de chaves que o National Institute for Standards and Technology (NIST) designou como seu primeiro algoritmo padrão de acordo de chaves pós-quântico. Esse híbrido utiliza cada um dos algoritmos de maneira independente para gerar uma chave. Depois, ele combina as duas chaves criptograficamente. Com s2n-tls, é possível configurar um cliente HTTP para ter o TLS pós-quântico como preferência, o que define ECDH com Kyber em primeiro lugar na lista de preferências. Algoritmos clássicos de troca de chaves são incluídos na lista de preferências para garantir a compatibilidade, mas eles estarão mais abaixo na ordem de preferência.

Se pesquisas em curso revelarem que o algoritmo Kyber não tem a força pós-quântica prevista, a chave híbrida ainda será pelo menos tão forte quanto a chave ECDH única atualmente em uso. Até que a pesquisa sobre algoritmos pós-quânticos esteja concluída, recomendamos o uso de algoritmos híbridos no lugar de algoritmos pós-quânticos exclusivamente.

Usar TLS pós-quântico híbrido com o AWS KMS

É possível usar o TLS pós-quântico híbrido para suas chamadas para o AWS KMS. Ao configurar seu ambiente de teste de cliente HTTP, esteja ciente das seguintes informações:

Criptografia em trânsito

Os pacotes de criptografia híbrida no s2n-tls são usados somente para a criptografia em trânsito. Elas protegem seus dados enquanto estes viajam do cliente para o endpoint do AWS KMS. O AWS KMS não usa esses pacotes de criptografia para criptografar em AWS KMS keys.

Em vez disso, quando o AWS KMS criptografa os dados em chaves do KMS, ele usa a criptografia simétrica com chaves de 256 bits e o algoritmo Advanced Encryption Standard in Galois Counter Mode (AES-GCM), que já é resistente para quântico. Num futuro teórico, ataques de computação quântica em grande escala em textos cifrados criados sob chaves AES-GCM de 256 bits reduzem a segurança efetiva da chave para 128 bits. Esse nível de segurança é suficiente para tornar inviáveis ataques de força bruta contra textos cifrados do AWS KMS.

Sistemas suportados

O uso dos pacotes de criptografia híbrida no s2n-tls tem suporte atualmente somente em sistemas Linux. Além disso, esses pacotes de criptografia são compatíveis somente com os SDKs que oferecem suporte ao runtime comum da AWS, como o AWS SDK for Java 2.x. Para ver um exemplo, consulte Como configurar o TLS pós-quântico híbrido.

Endpoints do AWS KMS

Ao usar os pacotes de criptografia híbrida, use o endpoint do AWS KMS padrão. Os pacotes de criptografia híbrida no s2n-tls não são compatíveis com os endpoints validados FIPS 140-2 do AWS KMS.

Quando você configura um cliente HTTP para ter conexões TLS pós-quânticas com s2n-tls como preferência, as codificações pós-quânticas são as primeiras na lista de preferências de codificação. No entanto, a lista de preferências inclui as cifras clássicas não híbridas mais abaixo na ordem de preferência para a compatibilidade. Quando você configura um cliente HTTP para ter o TLS pós-quântico com um endpoint FIPS 140-2 do AWS KMS validado como preferência, s2n-tls negocia uma codificação de troca de chave clássica e não híbrida.

Para obter uma lista de endpoints do AWS KMS para cada Região da AWS, consulte endpoints e cotas do AWS Key Management Service no Referência geral da Amazon Web Services. Para obter informações sobre endpoints do FIPS, consulte Endpoints do FIPS no Referência geral da Amazon Web Services.

Desempenho esperado

Nosso teste inicial de comparação mostra que os pacotes de criptografia híbrida no s2n-tls são mais lentos do que os pacotes de criptografia TLS clássicos. O efeito varia de acordo com o perfil de rede, a velocidade da CPU, o número de núcleos e a taxa de chamada. Para conhecer resultados de testes de desempenho, consulte Como ajustar o TLS para criptografia pós-quântica híbrida com o Kyber.

Como configurar o TLS pós-quântico híbrido

Neste procedimento, adicione uma dependência do Maven para o cliente HTTP de runtime comum da AWS. Em seguida, configure um cliente HTTP com preferência em TLS pós-quântico. Em seguida, crie um cliente AWS KMS que use o cliente HTTP.

Para ver exemplos funcionais completos de configuração e uso do TLS pós-quântico híbrido com o AWS KMS, consulte o repositório aws-kms-pq-tls-example.

> **Note**
>
> O cliente HTTP de runtime comum da AWS, que estava disponível como uma prévia, tornou-se disponível para o público em fevereiro de 2023. Nesse lançamento, a classe `tlsCipherPreference` e o parâmetro de método `tlsCipherPreference()` foram

substituídos pelo parâmetro de método `postQuantumTlsEnabled()`. Se você estava usando este exemplo durante a prévia, precisará atualizar seu código.

1. Adicione o cliente de runtime comum da AWS às suas dependências do Maven. Recomendamos usar a versão mais recente disponível.

   Por exemplo, esta instrução adiciona a versão `2.20.0` do cliente de runtime comum da AWS para suas dependências do Maven.

   ```
   <dependency>
       <groupId>software.amazon.awssdk</groupId>
       <artifactId>aws-crt-client</artifactId>
       <version>2.20.0</version>
   </dependency>
   ```

2. Para habilitar os pacotes de criptografia pós-quântica híbrida, adicione o AWS SDK for Java 2.x ao seu projeto e inicialize-o. Em seguida, habilite os pacotes de codificação pós-quântica híbrida em seu cliente HTTP, conforme mostrado no exemplo a seguir.

   Esse código usa o parâmetro de método `postQuantumTlsEnabled()` para configurar um cliente HTTP de runtime comum da AWS que prefere o pacote de codificação pós-quântica híbrida recomendado, ECDH com Kyber. Em seguida, o cliente HTTP configurado é usado para criar uma instância do cliente assíncrono do AWS KMS, `KmsAsyncClient`. Após a conclusão desse código, todas as solicitações de API do AWS KMS na instância `KmsAsyncClient` usam TLS pós-quântico híbrido.

   ```
   // Configure HTTP client
   SdkAsyncHttpClient awsCrtHttpClient = AwsCrtAsyncHttpClient.builder()
              .postQuantumTlsEnabled(true)
              .build();

   // Create the AWS KMS async client
   KmsAsyncClient kmsAsync = KmsAsyncClient.builder()
             .httpClient(awsCrtHttpClient)
             .build();
   ```

3. Teste suas chamadas do AWS KMS com TLS pós-quântico híbrido.

Quando você chama operações de API do AWS KMS no cliente do AWS KMS configurado, as chamadas são transmitidas para o endpoint do AWS KMS usando TLS pós-quântico híbrido. Para testar a configuração, chame uma API do AWS KMS, como `ListKeys`.

```
ListKeysReponse keys = kmsAsync.listKeys().get();
```

Testar o TLS pós-quântico híbrido com o AWS KMS

Considere executar os testes a seguir com pacotes de criptografia híbrida em suas aplicações que chamam o AWS KMS.

- Execute testes de carga e de comparação. Os pacotes de criptografia híbrida têm uma performance diferente dos algoritmos tradicionais de troca de chaves. Talvez seja necessário ajustar os tempos limite de conexão para permitir os tempos de handshake mais longos. Se você estiver executando dentro de uma função AWS Lambda, estenda a configuração de tempo limite de execução.
- Tente conectar-se de diferentes locais. Dependendo do caminho de rede que sua solicitação segue, é possível descobrir quais hosts intermediários, proxies ou firewalls com inspeção profunda de pacotes (DPI) bloqueiam a solicitação. Isso pode resultar do uso dos novos conjuntos de criptografia na ClientHelloparte do handshake TLS ou de mensagens maiores de troca de chaves. Se você tiver problemas para resolver esses problemas, trabalhe com sua equipe de segurança ou administradores de TI para atualizar a configuração relevante e desbloquear os novos pacotes de criptografia TLS.

Saiba mais sobre o TLS pós-quântico no AWS KMS

Para obter mais informações sobre como usar o TLS pós-quântico híbrido no AWS KMS, consulte os recursos a seguir.

- Para saber mais sobre criptografia pós-quântica na AWS, incluindo links para postagens de blog e artigos de pesquisa, consulte Post-Quantum Cryptography (Criptografia pós-quântica).
- Para obter informações sobre o s2n-tls, consulte Apresentação do s2n-tls, uma nova implementação do TLS de código aberto e Uso do s2n-tls.

- Para obter informações sobre o cliente HTTP de runtime da AWS, consulte Configuring the AWS CRT-based HTTP client (Configurar o cliente HTTP da baseado em CRT) no Guia do desenvolvedor do AWS SDK for Java 2.x.
- Para obter informações sobre o projeto de criptografia pós-quântica no Instituto Nacional de Padrões e Tecnologia (NIST — National Institute for Standards and Technology), consulte Criptografia pós-quântica.
- Para obter informações sobre a padronização de criptografia pós-quântica do NIST, consulte Post-Quantum Cryptography Standardization (Padronização de criptografia pós-quântica).

Determinar acesso a AWS KMS keys

Para determinar a extensão total de quem ou o quê atualmente tem acesso a uma AWS KMS key, é necessário examinar a política de chaves da chave do KMS, todas as concessões que se aplicam a essa chave do KMS e, potencialmente, todas as políticas do AWS Identity and Access Management (IAM). Você pode fazer isso para determinar o escopo do uso potencial de uma chave do KMS ou para ajudar a cumprir os requisitos de conformidade ou de auditoria. Os tópicos a seguir podem ajudar você a gerar uma lista completa das entidades principais da AWS (identidades) que no momento têm acesso a uma chave do KMS.

Tópicos

- Examinar a política de chaves
- Examinar políticas do IAM
- Examinar concessões
- Solucionar problemas de acesso à chave

Examinar a política de chaves

Políticas de chaves são a principal maneira de controlar o acesso a chaves do KMS. Cada chave do KMS tem exatamente uma política de chaves.

Quando uma política de chaves consiste em ou inclui a política de chaves padrão, ela permite que os administradores do IAM na conta usem políticas do IAM para controlar o acesso à chave do KMS. Além disso, se a política de chaves conceder a outra Conta da AWS permissão para usar a chave do KMS, os administradores do IAM na conta externa poderão usar políticas do IAM para delegar essas permissões. Para determinar a lista completa de entidades principais que podem acessar a chave do KMS, examine as políticas do IAM.

Para ver a política de chaves de uma chave gerenciada pelo AWS KMS cliente ou Chave gerenciada pela AWSem sua conta, use a operação AWS Management Console ou a GetKeyPolicyoperação na AWS KMS API. Para visualizar a política de chaves, é necessário ter permissões `kms:GetKeyPolicy` para a chave do KMS. Para obter instruções sobre como visualizar a política de chaves de uma chave do KMS, consulte the section called “Visualizar uma política de chaves”.

Examine o documento de política de chaves e anote todas as principais especificadas em cada elemento `Principal` da declaração de política. Em uma instrução de política com um efeito `Allow`, os usuários do IAM, os perfis do IAM e as Contas da AWS no elemento `Principal` têm acesso a essa chave do KMS.

> **Note**
>
> Não defina a entidade principal como um asterisco (*) em qualquer instrução de política de chave que permita permissões, a menos que você utilize condições para limitar a política de chave. Um asterisco dá à cada identidade em cada permissão da Conta da AWS para usar a chave do KMS, a menos que outra instrução de política negue essa permissão explicitamente. Usuários em outras Contas da AWS podem usar a chave do KMS sempre que tiverem as permissões correspondentes em suas próprias contas.

Os exemplos a seguir usam as declarações de política encontradas na política de chaves padrão para demonstrar como fazer isso.

Example Declaração de política 1

```
{
  "Sid": "Enable IAM User Permissions",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:root"},
  "Action": "kms:*",
  "Resource": "*"
}
```

Na instrução de política 1, `arn:aws:iam::111122223333:root` é uma entidade principal da AWS que se refere à Conta da AWS 111122223333. (Não corresponde ao usuário raiz da conta.) Por padrão, uma instrução de política como esta é incluída no documento de política de chaves quando

você cria uma nova chave do KMS com o AWS Management Console ou cria uma nova chave do KMS programaticamente, mas não fornece uma política de chaves.

Um documento de política de chaves com uma instrução que permite o acesso à Conta da AWS possibilita que as políticas do IAM na conta permitam o acesso à chave do KMS. Isso significa que os usuários e perfis na conta podem ter acesso à chave do KMS, mesmo se não estiverem explicitamente listados como entidades principais no documento de política de chaves. Tenha cuidado ao examinar todas as políticas do IAM em todas as Contas da AWS listadas como as entidades principais para determinar se elas permitem o acesso a essa chave do KMS.

Example Declaração de política 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": "*"
}
```

Na declaração de política 2, `arn:aws:iam::111122223333:role/KMSKeyAdmins` refere-se à função do IAM chamada KMS KeyAdmins em Conta da AWS 111122223333. Os usuários autorizados a assumir esse perfil podem executar as ações listadas na instrução de política, que são as ações administrativas para gerenciar uma chave do KMS.

Example Declaração de política 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": "*"
}
```

Na declaração de política 3, `arn:aws:iam::111122223333:role/EncryptionApp` refere-se à função do IAM nomeada EncryptionApp em Conta da AWS 111122223333. As entidades principais autorizadas a assumir esse perfil podem executar as ações listadas na instrução de política, que incluem as operações criptográficas para uma chave do KMS de criptografia simétrica.

Example Declaração de política 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}}
}
```

Na declaração de política 4, `arn:aws:iam::111122223333:role/EncryptionApp` refere-se à função do IAM nomeada EncryptionApp em Conta da AWS 111122223333. As entidades principais autorizadas assumem esse perfil e podem executar as ações listadas na instrução de política. Essas ações, quando combinadas com as ações permitidas na Instrução de política de exemplo 3, são aquelas necessárias para delegar o uso da chave do KMS à maioria dos serviços da AWS integrados ao AWS KMS, especificamente os serviços que usam concessões. O GrantIsFor AWSResource valor kms: no `Condition` elemento garante que a delegação seja permitida somente quando o delegado é um AWS serviço que se integra AWS KMS e usa concessões para autorização.

Para conhecer todas as diferentes maneiras de especificar uma entidade principal em um documento de política de chaves, consulte Especificar uma entidade principal , no Manual do usuário do IAM.

Para saber mais sobre as políticas de chaves do AWS KMS, consulte Políticas-chave em AWS KMS.

Examinar políticas do IAM

Além da política de chaves e concessões, também é possível usar as políticas do IAM para permitir o acesso a uma chave do KMS. Para obter mais informações sobre como as políticas do IAM e as políticas de chaves funcionam juntas, consulte Solucionar problemas de acesso à chave.

Para determinar quais entidades principais têm acesso no momento a uma chave do KMS por meio de políticas do IAM, você pode usar a ferramenta baseada em navegador Simulador de políticas do IAM, ou pode fazer solicitações para a API do IAM.

Maneiras de examinar políticas do IAM

- Examinar políticas do IAM com o Simulador de políticas do IAM
- Examinar políticas do IAM com a API do IAM

Examinar políticas do IAM com o Simulador de políticas do IAM

O Simulador de políticas do IAM pode ajudar a saber quais entidades principais têm acesso a uma chave do KMS por meio de uma política do IAM.

Para usar o simulador de políticas do IAM para determinar o acesso a uma chave do KMS

1. Faça login no AWS Management Console e abra o Simulador de políticas do IAM em https://policysim.aws.amazon.com/.
2. No painel Users, Groups, and Roles (Usuários, grupos e funções), escolha o usuário, o grupo ou a função cujas políticas você deseja simular.
3. (Opcional) Desmarque a caixa de seleção ao lado de qualquer política que você deseja omitir da simulação. Para simular todas as políticas, deixe todas as políticas selecionadas.
4. No painel Policy Simulator (Simulador de políticas), faça o seguinte:

    a. Para Select service (Selecionar serviço), selecione Key Management Service.

    b. Para simular ações específicas do AWS KMS para Select actions (Selecionar ações), escolha as ações a serem simuladas. Para simular todas as ações do AWS KMS, selecione Selecionar tudo (Select All).

5. (Opcional) O Simulador de políticas simula o acesso a todas as chaves do KMS por padrão. Para simular o acesso a uma determinada chave do KMS, escolha Simulation Settings (Configurações de simulação) e digite o nome do recurso da Amazon (ARN) da chave do KMS a ser simulada.
6. Selecione Run Simulation (Executar simulação).

Você pode visualizar os resultados da simulação na seção Results (Resultados). Repita as etapas 2 a 6 para cada usuário, grupo e perfil na Conta da AWS.

Examinar políticas do IAM com a API do IAM

Você pode usar a API do IAM para examinar políticas do IAM programaticamente. As etapas a seguir fornecem uma visão geral de como fazer isso:

1. Para cada um Conta da AWS listado como principal na política de chaves (ou seja, cada principal de AWS conta especificado neste formato:`"Principal": {"AWS": "arn:aws:iam::111122223333:root"}`), use as ListRolesoperações ListUserse na API do IAM para obter todos os usuários e funções na conta.
2. Para cada usuário e função na lista, use a SimulatePrincipalPolicyoperação na API IAM, transmitindo os seguintes parâmetros:
   - Para `PolicySourceArn`, especifique o Amazon Resource Name (ARN) de um usuário ou função da sua lista. É possível especificar somente um `PolicySourceArn` para cada solicitação `SimulatePrincipalPolicy`, portanto, você deve chamar essa operação diversas vezes, uma vez para cada perfil e usuário em sua lista.
   - Para ver a lista `ActionNames`, especifique cada ação de API do AWS KMS a ser simulada. Para simular todas as ações de API do AWS KMS, use `kms:*`. Para testar ações de API individuais do AWS KMS, preceda cada ação de API com "`kms:`", por exemplo, "`kms:ListKeys`". Para obter uma lista completa das ações de API do AWS KMS, consulte Actions (Ações) na Referência de API do AWS Key Management Service.
   - (Opcional) Para determinar se os usuários ou perfis têm acesso a chaves do KMS específicas, use o parâmetro `ResourceArns` para especificar uma lista de nomes dos recursos da Amazon (ARNs) das chaves do KMS. Para determinar se os usuários ou perfis têm acesso a qualquer chave do KMS, omita o parâmetro `ResourceArns`.

O IAM responde a cada solicitação `SimulatePrincipalPolicy` com uma decisão de avaliação: `allowed`, `explicitDeny` ou `implicitDeny`. Para cada resposta que contém uma decisão

de avaliação `allowed`, a resposta inclui o nome da operação de API do AWS KMS específico permitido. Ela também inclui o ARN da chave do KMS que foi usada na avaliação, se houver.

Examinar concessões

Concessões são mecanismos avançados para especificar as permissões que você ou um serviço da AWS integrado ao AWS KMS pode usar para especificar como e quando uma chave do KMS pode ser usada. Concessões são associadas a uma chave do KMS, e cada concessão contém a entidade principal que recebe permissão para usar a chave do KMS e uma lista de operações que são permitidas. As concessões são uma alternativa para a política de chaves e são úteis para casos de uso específicos. Para ter mais informações, consulte Concessões no AWS KMS.

Para obter uma lista de concessões para uma chave KMS, use a AWS KMS ListGrantsoperação. É possível examinar as concessões de uma chave do KMS para determinar quem ou o quê tem acesso no momento para usar a chave do KMS por meio dessas concessões. Por exemplo, a seguir há uma representação JSON de uma concessão que foi obtida do comando list-grants na 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"}}
}]}
```

Para saber quem ou o quê tem acesso para usar a chave do KMS, procure o elemento `"GranteePrincipal"`. No exemplo anterior, o principal favorecido é um usuário de função assumida associado à instância do EC2 i-5d476fab. A infraestrutura do EC2 usa essa função para anexar o volume do EBS criptografado vol-5cccfb4e à instância. Nesse caso, a função da infraestrutura do EC2 tem permissão para usar a chave do KMS porque você já criou um volume do EBS criptografado protegido por essa chave do KMS. Anexe o volume a uma instância do EC2.

A seguir há outro exemplo de representação JSON de uma concessão que foi obtida do comando list-grants na AWS CLI. No exemplo a seguir, a entidade principal favorecido é outra Conta da AWS.

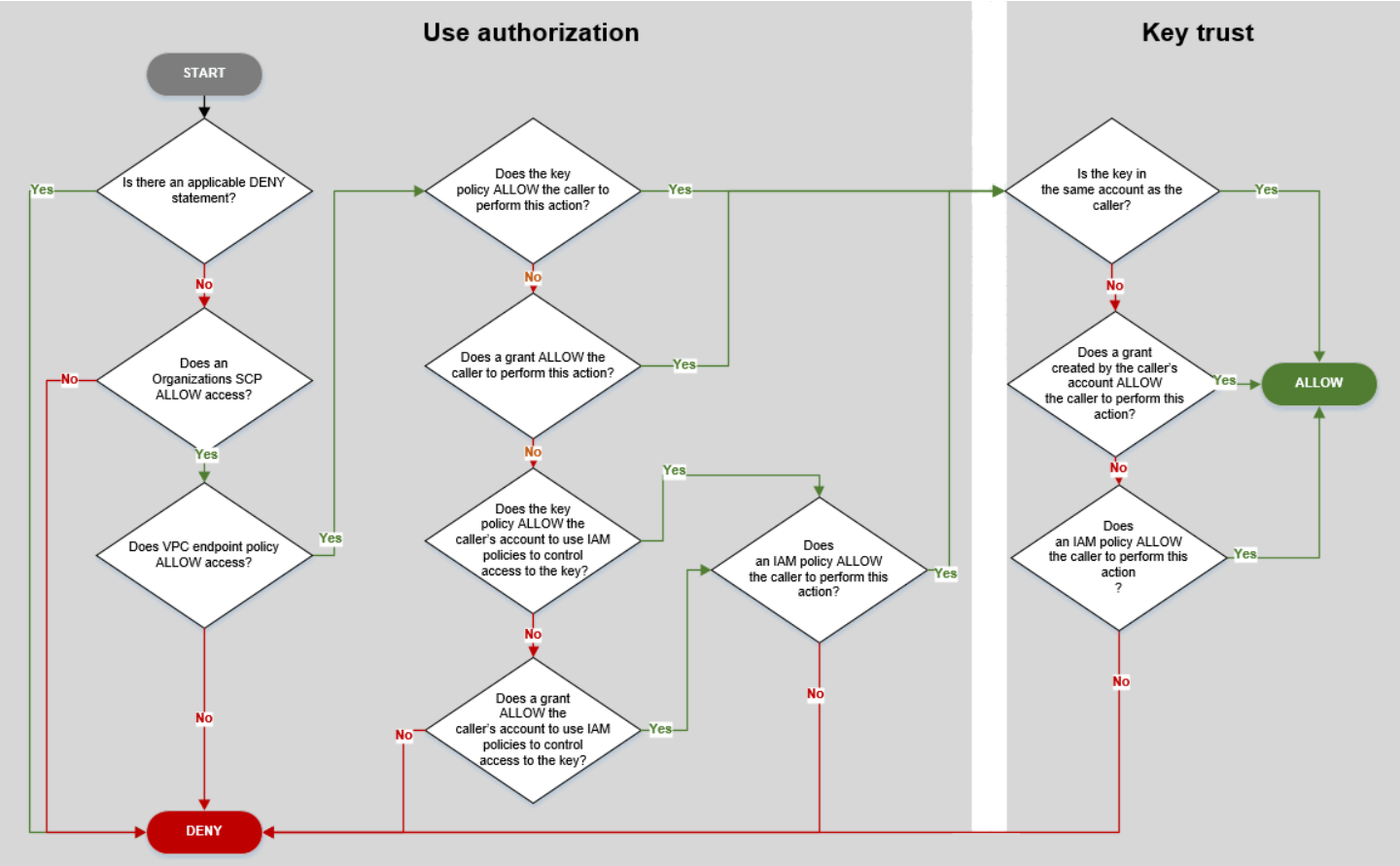
```
{"Grants": [{
  "Operations": ["Encrypt"],
  "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
  "Name": "",
  "GranteePrincipal": "arn:aws:iam::444455556666:root",
  "GrantId": "f271e8328717f8bde5d03f4981f06a6b3fc18bcae2da12ac38bd9186e7925d11",
  "IssuingAccount": "arn:aws:iam::111122223333:root",
  "CreationDate": 1.444151269E9
}]}
```

Solucionar problemas de acesso à chave

Ao autorizar o acesso a uma chave do KMS, o AWS KMS avalia o seguinte:

- A política de chaves associada à chave do KMS. A política de chaves é sempre definida na Conta da AWS e na região proprietária da chave do KMS.
- Todas as políticas do IAM que são vinculadas ao usuário ou ao perfil que realiza a solicitação. As políticas do IAM do que controlam o uso de uma chave do KMS pela entidade principal sempre são definidas naConta da AWS da entidade principal.
- Todas as concessões que se aplicam à chave do KMS.
- Outros tipos de políticas que podem se aplicar à solicitação para usar a chave do KMS, como políticas de controle de serviço do AWS Organizations e políticas de endpoint da VPC. Essas políticas são opcionais e permitem todas as ações por padrão, mas é possível usá-las para restringir permissões concedidas de outra forma às entidades principais.

O AWS KMS avalia esses mecanismos de política juntos para determinar se o acesso à chave do KMS é permitido ou negado. Para fazer isso, o AWS KMS usa um processo parecido com o descrito no fluxograma a seguir. O fluxograma a seguir fornece uma representação visual do processo de avaliação de política.



Esse fluxograma está dividido em duas partes. As partes parecem ser sequenciais, mas geralmente são avaliadas ao mesmo tempo.

- A autorização de uso determina se você tem permissão para usar uma chave do KMS com base em sua política de chaves, políticas do IAM, concessões e outras políticas aplicáveis.
- A confiança de chave determina se você deve confiar em uma chave do KMS que tem autorização para usar. Em geral, você confia nos recursos na sua da Conta da AWS. Porém, você também pode se sentir seguro em relação ao uso de chaves do KMS em outra Conta da AWS se uma concessão ou política do IAM na sua conta permitir que você use a chave do KMS.

Use esse fluxograma para descobrir por que um autor da chamada recebeu ou não permissão para usar uma chave do KMS. Ou use-o para avaliar suas políticas e concessões. Por exemplo, o fluxograma mostra que um autor de chamada pode ter acesso negado por uma instrução `DENY` explícita ou pela ausência de uma instrução `ALLOW` explícita na política de chaves, política do IAM ou concessão.

O fluxograma consegue explicar alguns cenários comuns de permissão.

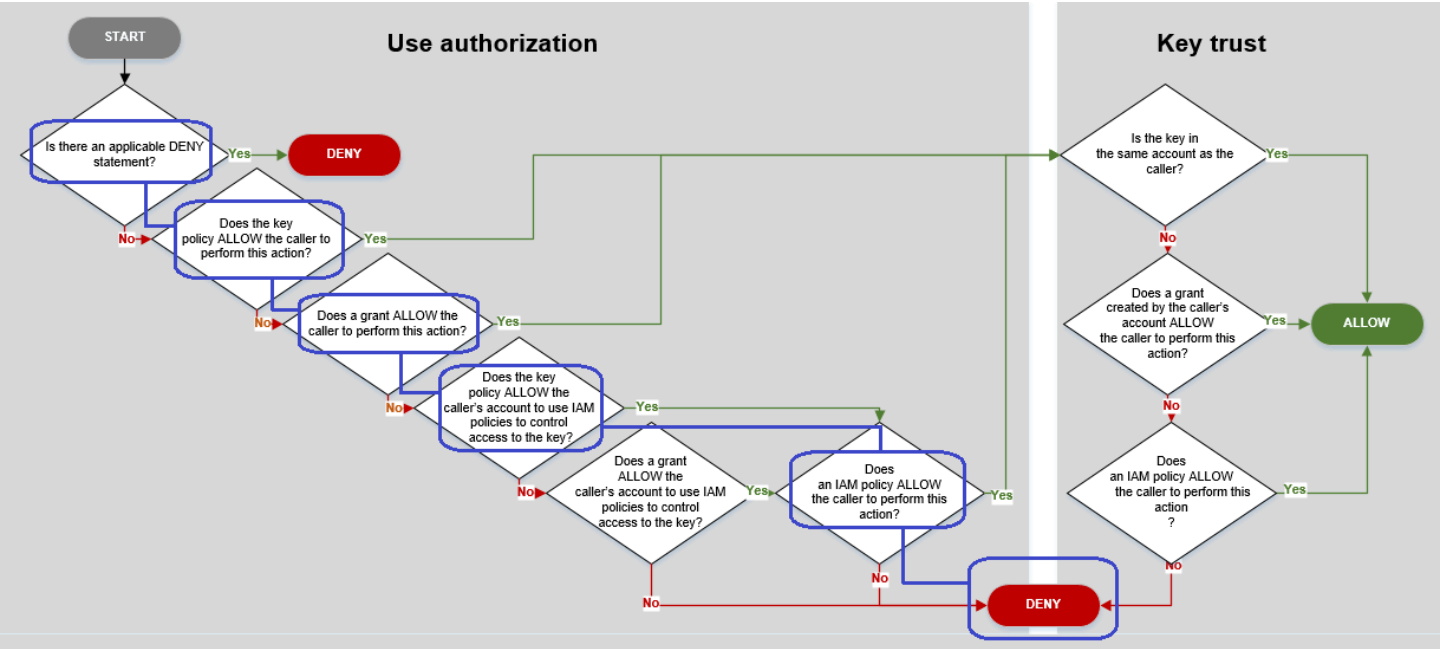
Exemplos de permissão

- Exemplo 1: é negado ao usuário o acesso a uma chave do KMS em sua Conta da AWS
- Exemplo 2: o usuário assume uma função com permissão para usar uma chave do KMS em outra Conta da AWS

Exemplo 1: é negado ao usuário o acesso a uma chave do KMS em sua Conta da AWS

Alice é um usuário do IAM na Conta da AWS 111122223333. Ela teve o acesso negado a uma chave do KMS na mesma Conta da AWS. Por que Alice não pode usar a chave do KMS?

Nesse caso, Alice teve o acesso negado à chave do KMS porque não há uma política de chaves, política do IAM ou concessão que dê a ela as permissões necessárias. A política de chaves da chave do KMS permite que a Conta da AWS use políticas do IAM para controlar o acesso à chave do KMS, mas nenhuma política do IAM concede a Alice permissão para usar a chave do KMS.



Considere as políticas relevantes para este exemplo.

- A chave do KMS que Alice deseja usar tem a política de chaves padrão. Essa política permite que a Conta da AWS que possui a chave do KMS use as políticas do IAM para controlar o acesso à chave do KMS. Esta política de chaves atende à condiçãoA política de chaves PERMITE que a conta dos chamadores usem políticas do IAM para controlar o acesso à chave? no fluxograma.

```
{
  "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" : "*"
  } ]
}
```

- No entanto, nenhuma política de chaves, política do IAM ou concessão permite que Alice use a chave do KMS. Portanto, é negada à Alice a permissão para usar a chave do KMS.

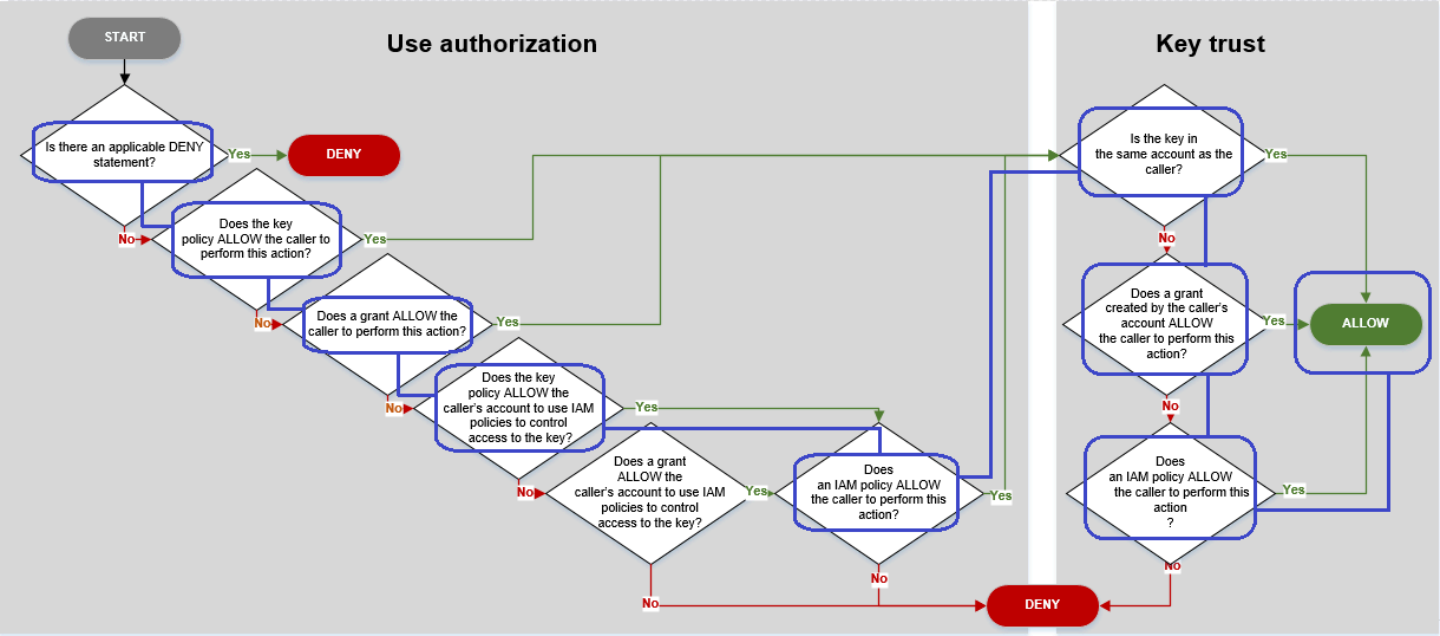
Exemplo 2: o usuário assume uma função com permissão para usar uma chave do KMS em outra Conta da AWS

Bob é um usuário na conta 1 (111122223333). Ele tem permissão para usar uma chave do KMS na conta 2 (444455556666) em operações de criptografia. Como isso é possível?

> **Tip**
>
> Ao avaliar permissões entre contas, lembre-se de que a política de chaves é especificada na conta da chave do KMS. A política do IAM é especificada na conta do autor da chamada, mesmo quando ele está em uma conta diferente. Para obter detalhes sobre como fornecer acesso entre contas a chaves do KMS, consulte Permitir que usuários de outras contas usem uma chave do KMS.

- A política de chaves da chave do KMS permite que a conta 2 use políticas do IAM para controlar o acesso à chave do KMS.
- A política de chaves da chave do KMS na conta 2 permite que a conta 1 use a chave do KMS em operações de criptografia. No entanto, a conta 1 deve usar políticas do IAM para conceder às suas entidades principais acesso à chave do KMS.

- Uma política do IAM na conta 1 permite que a função `Engineering` use a chave do KMS na conta 2 para operações de criptografia.
- Bob, um usuário na conta 1, tem permissão para assumir a função `Engineering`.
- Bob pode confiar nessa chave do KMS, pois, mesmo que ela não esteja na conta dele, uma política do IAM na conta dele concede uma permissão explícita para usar essa chave do KMS.



Considere as políticas que permitem que Bob, um usuário na conta 1, use a chave do KMS na conta 2.

- A política de chaves da chave do KMS permite que a conta 2 (444455556666, a conta que possui a chave do KMS) use políticas do IAM para controlar o acesso à chave do KMS. Essa política de chaves também permite que a conta 1 (111122223333) use a chave do KMS em operações de criptografia (especificadas no elemento `Action` da instrução de política). No entanto, ninguém na conta 1 pode usar a chave do KMS na conta 2 até que conta 1 defina políticas do IAM que concedam às entidades principais acesso à chave do KMS.

  No fluxograma, essa política de chaves na conta 2 atende à condição A política de chaves PERMITE que a conta do autor da chamada use políticas do IAM para controlar o acesso à chave?.

```
{
    "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": "*"
        }
    ]
}
```

- Uma política do IAM na Conta da AWS (conta 1, 111122223333) do autor da chamada concede à entidade principal a permissão para realizar operações de criptografia usando a chave do KMS na conta 2 (444455556666). O elemento `Action` concede à entidade principal as mesmas permissões que a política de chaves na conta 2 concedeu à conta 1. Para dar essas permissões à função `Engineering` na conta 1, essa política em linha está incorporada na função `Engineering`.

  Políticas do IAM entre contas como essa são efetivas somente quando a política de chaves para a chave do KMS na conta 2 concede à conta 1 permissão para usar a chave do KMS. Além disso, a conta 1 só pode conceder aos seus principais permissão para executar as ações que a política de chaves atribuiu à conta.

No fluxograma, isso atende à condição Uma política do IAM permite que o autor da chamada realize essa ação?.

```
{
    "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"
            ]
        }
    ]
}
```

- O último elemento exigido é a definição da função `Engineering` na conta 1. O `AssumeRolePolicyDocument` na função permite que Bob assuma a função `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 permissões

Essa tabela foi criada para ajudar você a entender AWS KMS as permissões para que você possa controlar o acesso aos seus AWS KMS recursos. As definições dos cabeçalhos das colunas aparecem abaixo da tabela.

Você também pode aprender sobre AWS KMS permissões no AWS Key Management Service tópico Ações, recursos e chaves de condição do Service Authorization Reference. No entanto, esse tópico não lista todas as chaves de condição que você pode usar para refinar cada permissão.

> **Note**
>
> Talvez seja necessário rolar horizontalmente ou verticalmente para ver todos os dados da tabela.

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
CancelKeyDeletion `kms:CancelKeyDeletion`	Política de chave	Não	Chave do KMS	Condições para operações de chave do KMS: kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
				kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases aws:ResourceTag/tag-key (chave de condição AWS global) kms: ViaService
ConnectCustomKeyStore `kms:ConnectCustomKeyStore`	Política do IAM	Não	*	kms: CallerAccount

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
CreateAlias `kms:CreateAlias` Para usar essa operação, o chamador precisa da permissão `kms:CreateAlias` em dois recursos: • O alias (em uma política do IAM) • A chave do KMS (em uma política de chaves) Para obter detalhes, consulte Controlar o acesso a aliases.	Política do IAM (para o alias)	Não	Alias	Nenhum (quando controlar o acesso ao alias)
	Política de chaves (para a chave do KMS)	Não	Chave do KMS	Condições para operações de chave do KMS: kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases aws:ResourceTag/tag-key (chave de condição AWS global) kms: ViaService
CreateCustomKeyStore `kms:CreateCustomKeyStore`	Política do IAM	Não	*	kms: CallerAccount

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
CreateGrant `kms:CreateGrant`	Política de chave	Sim	Chave do KMS	Condições para contexto de criptografia: kms:EncryptionContext: chave de contexto kms: EncryptionContextKeys Condições de concessão: kms: GrantConstraintType kms: GranteePrincipal kms: GrantIsForAWSResource kms: GrantOperations kms: RetiringPrincipal Condições para operações de chave do KMS: kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
				kms: MultiRegionKeyType kms: ResourceAliases aws:ResourceTag/tag-key (chave de condição AWS global) kms: ViaService

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
CreateKey `kms:CreateKey`	Política do IAM	Não	*	kms: BypassPolicyLockoutSafetyCheck kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ViaService aws:RequestTag/tag-key (chave de condição AWS global) aws:ResourceTag/tag-key (chave de condição AWS global) aws: TagKeys (chave de condição AWS global)

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
Decrypt `kms:Decrypt`	Política de chave	Sim	Chave do KMS	Condições para operações criptográficas kms: EncryptionAlgorithm kms: RequestAlias Condições para contexto de criptografia: kms:EncryptionContext: chave de contexto kms: EncryptionContextKeys Condições para operações de chave do KMS: kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
				aws:ResourceTag/tag-key (chave de condição AWS global) kms: ViaService
DeleteAlias `kms:DeleteAlias` Para usar essa operação, o chamador precisa da permissão `kms:DeleteAlias` em dois recursos: • O alias (em uma política do IAM) • A chave do KMS (em uma política de chaves) Para obter detalhes, consulte Controlar o acesso a aliases.	Política do IAM (para o alias)	Não	Alias	Nenhum (quando controlar o acesso ao alias)
	Política de chaves (para a chave do KMS)	Não	Chave do KMS	Condições para operações de chave do KMS: kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases aws:ResourceTag/tag-key (chave de condição AWS global) kms: ViaService

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
DeleteCustomKeyStore `kms:DeleteCustomKeyStore`	Política do IAM	Não	*	kms: CallerAccount
DeleteImportedKeyMaterial `kms:DeleteImportedKeyMaterial`	Política de chave	Não	Chave do KMS	Condições para operações de chave do KMS: kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases aws:ResourceTag/tag-key (chave de condição AWS global) kms: ViaService
DescribeCustomKeyStores `kms:DescribeCustomKeyStores`	Política do IAM	Não	*	kms: CallerAccount

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
DescribeKey `kms:DescribeKey`	Política de chave	Sim	Chave do KMS	Condições para operações de chave do KMS: kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases aws:ResourceTag/tag-key (chave de condição AWS global) kms: ViaService Outras condições: kms: RequestAlias

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
DisableKey `kms:DisableKey`	Política de chave	Não	Chave do KMS	Condições para operações de chave do KMS: kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases aws:ResourceTag/tag-key (chave de condição AWS global) kms: ViaService

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
DisableKeyRotation `kms:DisableKeyRotation`	Política de chave	Não	Chave do KMS	Condições para operações de chave do KMS: kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases aws:ResourceTag/tag-key (chave de condição AWS global) kms: ViaService
DisconnectCustomKeyStore `kms:DisconnectCustomKeyStore`	Política do IAM	Não	*	kms: CallerAccount

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
EnableKey `kms:EnableKey`	Política de chave	Não	Chave do KMS	Condições para operações de chave do KMS: kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases aws:ResourceTag/tag-key (chave de condição AWS global) kms: ViaService

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
EnableKeyRotation `kms:EnableKeyRotation`	Política de chave	Não	Chave do KMS (somente simétrica)	Condições para operações de chave do KMS: kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases aws:ResourceTag/tag-key (chave de condição AWS global) kms: ViaService Condições de rotação automática de chaves: kms: RotationPeriodInDays

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
Encrypt `kms:Encrypt`	Política de chave	Sim	Chave do KMS	Condições para operações criptográficas kms: EncryptionAlgorithm kms: RequestAlias Condições para contexto de criptografia: kms:EncryptionContext: chave de contexto kms: EncryptionContextKeys Condições para operações de chave do KMS: kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
				aws:ResourceTag/tag-key (chave de condição AWS global) kms: ViaService

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
GenerateDataKey `kms:GenerateDataKey`	Política de chave	Sim	Chave do KMS (somente simétrica)	Condições para operações criptográficas kms: EncryptionAlgorithm kms: RequestAlias Condições para contexto de criptografia: kms:EncryptionContext: chave de contexto kms: EncryptionContextKeys Condições para operações de chave do KMS: kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
				aws:ResourceTag/tag-key (chave de condição AWS global) kms: ViaService

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
GenerateDataKeyPair `kms:GenerateDataKeyPair`	Política de chave	Sim	Chave do KMS (somente simétrica) Gera um par de chaves de dados assimétricas que é protegido por uma chave do KMS de criptografia simétrica.	Condições para pares de chaves de dados: kms: DataKeyPairSpec Condições para operações criptográficas kms: EncryptionAlgorithm kms: RequestAlias Condições para contexto de criptografia: kms:EncryptionContext: chave de contexto kms: EncryptionContextKeys Condições para operações de chave do KMS: kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
				kms: MultiRegionKeyType kms: ResourceAliases aws:ResourceTag/tag-key (chave de condição AWS global) kms: ViaService

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
GenerateDataKeyPairWithoutPlaintext `kms:GenerateDataKeyPairWithoutPlaintext`	Política de chave	Sim	Chave do KMS (somente simétrica) Gera um par de chaves de dados assimétricas que é protegido por uma chave do KMS de criptografia simétrica.	Condições para pares de chaves de dados: kms: DataKeyPairSpec Condições para operações criptográficas kms: EncryptionAlgorithm kms: RequestAlias Condições para contexto de criptografia: kms:EncryptionContext: chave de contexto kms: EncryptionContextKeys Condições para operações de chave do KMS: kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
				kms: MultiRegionKeyType kms: ResourceAliases aws:ResourceTag/tag-key (chave de condição AWS global) kms: ViaService

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
GenerateDataKeyWithoutPlaintext `kms:GenerateDataKeyWithoutPlaintext`	Política de chave	Sim	Chave do KMS (somente simétrica)	Condições para operações criptográficas kms: EncryptionAlgorithm kms: RequestAlias Condições para contexto de criptografia: kms:EncryptionContext: chave de contexto kms: EncryptionContextKeys Condições para operações de chave do KMS: kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
				aws:ResourceTag/tag-key (chave de condição AWS global) kms: ViaService
GenerateMac `kms:GenerateMac`	Política de chave	Sim	Chave do KMS	Condições para operações de chave do KMS: kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases aws:ResourceTag/tag-key (chave de condição AWS global) kms: ViaService Condições para operações criptográficas: kms: MacAlgorithm kms: RequestAlias

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
GenerateRandom `kms:GenerateRandom`	Política do IAM	N/D	*	Nenhum
GetKeyPolicy `kms:GetKeyPolicy`	Política de chave	Não	Chave do KMS	Condições para operações de chave do KMS: kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases aws:ResourceTag/tag-key (chave de condição AWS global) kms: ViaService

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
GetKeyRotationStatus `kms:GetKeyRotationStatus`	Política de chave	Sim	Chave do KMS (somente simétrica)	Condições para operações de chave do KMS: kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases aws:ResourceTag/tag-key (chave de condição AWS global) kms: ViaService

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
GetParametersForImport `kms:GetParametersForImport`	Política de chave	Não	Chave do KMS	kms: WrappingAlgorithm kms: WrappingKeySpec Condições para operações de chave do KMS: kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases aws:ResourceTag/tag-key (chave de condição AWS global) kms: ViaService

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
GetPublicKey `kms:GetPublicKey`	Política de chave	Sim	Chave do KMS (somente assimétrica)	Condições para operações de chave do KMS: kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases aws:ResourceTag/tag-key (chave de condição AWS global) kms: ViaService Outras condições: kms: RequestAlias

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
ImportKeyMaterial `kms:ImportKeyMaterial`	Política de chave	Não	Chave do KMS	Condições para operações de chave do KMS: kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases aws:ResourceTag/tag-key (chave de condição AWS global) kms: ViaService Outras condições: kms: ExpirationModel kms: ValidTo
ListAliases `kms:ListAliases`	Política do IAM	Não	*	Nenhum

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
ListGrants `kms:ListGrants`	Política de chave	Sim	Chave do KMS	Condições para operações de chave do KMS: kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases aws:ResourceTag/tag-key (chave de condição AWS global) kms: ViaService Outras condições: kms: GrantIsForAWSResource

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
ListKeyPolicies `kms:ListKeyPolicies`	Política de chave	Não	Chave do KMS	Condições para operações de chave do KMS: kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases aws:ResourceTag/tag-key (chave de condição AWS global) kms: ViaService

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
ListKeyRotations `kms:ListKeyRotations`	Política de chave	Não	Chave do KMS (somente simétrica)	Condições para operações de chave do KMS: kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases aws:ResourceTag/tag-key (chave de condição AWS global) kms: ViaService
ListKeys `kms:ListKeys`	Política do IAM	Não	*	Nenhum

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
ListResourceTags `kms:ListResourceTags`	Política de chave	Não	Chave do KMS	Condições para operações de chave do KMS: kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases aws:ResourceTag/tag-key (chave de condição AWS global) kms: ViaService

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
ListRetirableGrants `kms:ListRetirableGrants`	Política do IAM	A entidade principal especificada deve estar na conta local, mas a operação retorna concessões em todas as contas.	*	Nenhum

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
PutKeyPolicy `kms:PutKeyPolicy`	Política de chave	Não	Chave do KMS	Condições para operações de chave do KMS: kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases aws:ResourceTag/tag-key (chave de condição AWS global) kms: ViaService Outras condições: kms: BypassPolicyLockoutSafetyCheck

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição

ReEncrypt
 	
`kms:ReEncryptFrom`
 	
`kms:ReEncryptTo`
 	
Para usar essa operação, o autor da chamada precisa de permissão em duas chaves do KMS:
 	
• `kms:ReEncryptFrom` na chave do KMS usada para descriptografar
• `kms:ReEncryptTo` na chave do KMS usada para criptografar
	Política de chave	Sim	Chave do KMS	Condições para operações criptográficas
				
				kms: EncryptionAlgorithm
				
				kms: RequestAlias
				
				Condições para contexto de criptografia:
				
				kms:EncryptionContext: chave de contexto
				
				kms: EncryptionContextKeys
				
				Condições para operações de chave do KMS:
				
				kms: CallerAccount
				
				kms: KeySpec
				
				kms: KeyUsage
				
				kms: KeyOrigin
				
				kms: MultiRegion
				
				kms: MultiRegionKeyType
				
				kms: ResourceAliases

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
				aws:ResourceTag/tag-key (chave de condição AWS global) kms: ViaService Outras condições: kms: ReEncryptOnSameKey

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
ReplicateKey `kms:ReplicateKey` Para usar essa operação, o autor da chamada precisa das seguintes permissões: • `kms:ReplicateKey` na chave primária de várias regiões • `kms:CreateKey` em uma política do IAM na região de réplica	Política de chave	Não	Chave do KMS	Condições para operações de chave do KMS: kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases aws:ResourceTag/tag-key (chave de condição AWS global) kms: ViaService Outras condições: kms: ReplicaRegion

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
RetireGrant `kms:RetireGrant` A permissão para retirar uma concessão é determinada principal mente pela concessão. Uma política por si só não pode permitir o acesso a essa operação. Para ter mais informações, consulte Retirar e revogar concessões.	Política do IAM (Essa permissão não é eficaz em uma política de chave.)	Sim	Chave KMS	kms: ResourceAliases aws:ResourceTag/tag-key (chave de condição AWS global)

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
RevokeGrant `kms:RevokeGrant`	Política de chave	Sim	Chave do KMS	Condições para operações de chave do KMS: kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases aws:ResourceTag/tag-key (chave de condição AWS global) kms: ViaService Outras condições: kms: GrantIsForAWSResource

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
RotateKeyOnDemand `kms:RotateKeyOnDemand`	Política de chave	Não	Chave do KMS (somente simétrica)	Condições para operações de chave do KMS: kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases aws:ResourceTag/tag-key (chave de condição AWS global) kms: ViaService

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
ScheduleKeyDeletion `kms:ScheduleKeyDeletion`	Política de chave	Não	Chave do KMS	Condições para operações de chave do KMS: kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases aws:ResourceTag/tag-key (chave de condição AWS global) kms: ViaService

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
Sign `kms:Sign`	Política de chave	Sim	Chave do KMS (somente assimétrica)	Condições para assinatura e verificação: kms: MessageType kms: RequestAlias kms: SigningAlgorithm Condições para operações de chave do KMS: kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases aws:ResourceTag/tag-key (chave de condição AWS global) kms: ViaService

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
TagResource `kms:TagResource`	Política de chave	Não	Chave do KMS	Condições para operações de chave do KMS: kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases aws:ResourceTag/tag-key (chave de condição AWS global) kms: ViaService Condições para marcação: aws:RequestTag/tag-key (chave de condição AWS global) aws: TagKeys (chave de condição AWS global)

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
UntagResource `kms:UntagResource`	Política de chave	Não	Chave do KMS	Condições para operações de chave do KMS: kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases aws:ResourceTag/tag-key (chave de condição AWS global) kms: ViaService Condições para marcação: aws:RequestTag/tag-key (chave de condição AWS global) aws: TagKeys (chave de condição AWS global)

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
UpdateAlias `kms:UpdateAlias` Para usar essa operação, o chamador precisa da permissão `kms:UpdateAlias` em três recursos: • O alias • A chave do KMS atualmente associada • A chave do KMS recém-associada Para obter detalhes, consulte Controlar o acesso a aliases.	Política do IAM (para o alias)	Não	Alias	Nenhum (quando controlar o acesso ao alias)
	Política de chaves (para as chaves do KMS)	Não	Chave do KMS	Condições para operações de chave do KMS: kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases aws:ResourceTag/tag-key (chave de condição AWS global) kms: ViaService
UpdateCustomKeyStore `kms:UpdateCustomKeyStore`	Política do IAM	Não	*	kms: CallerAccount

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
UpdateKeyDescription `kms:UpdateKeyDescription`	Política de chave	Não	Chave do KMS	Condições para operações de chave do KMS: kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases aws:ResourceTag/tag-key (chave de condição AWS global) kms: ViaService

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
UpdatePrimaryRegion `kms:UpdatePrimaryRegion` Para usar essa operação, o autor da chamada precisa da permissão `kms:UpdatePrimaryRegion` na chave primária de várias regiões que se tornará uma chave de réplica e também na chave de réplica de várias regiões que se tornará a chave primária.	Política de chave	Não	Chave do KMS	Condições para operações de chave do KMS: kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases aws:ResourceTag/tag-key (chave de condição AWS global) kms: ViaService Outras condições kms: PrimaryRegion

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
Verificar `kms:Verify`	Política de chave	Sim	Chave do KMS (somente assimétrica)	Condições para assinatura e verificação: kms: MessageType kms: RequestAlias kms: SigningAlgorithm Condições para operações de chave do KMS: kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases aws:ResourceTag/tag-key (chave de condição AWS global) kms: ViaService

Ações e permissões	Tipo de política	Uso entre contas	Recursos (para políticas do IAM)	AWS KMS chaves de condição
VerifyMac `kms:VerifyMac`	Política de chave	Sim	Chave do KMS	Condições para operações de chave do KMS: kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases aws:ResourceTag/tag-key (chave de condição AWS global) kms: ViaService Condições para operações criptográficas: kms: MacAlgorithm kms: RequestAlias

Descrições das colunas

As colunas nesta tabela fornecem as seguintes informações:

- Ações e permissões listam cada operação da AWS KMS API e a permissão que permite a operação. Você especifica a operação no elemento `Action` de uma instrução de política.
- Tipo de política indica se a permissão pode ser usada em uma política de chaves ou política do IAM.

  Política de chaves significa que você pode especificar a permissão na política de chaves. Quando a política de chaves contém a instrução de política que permite políticas do IAM, você pode especificar as permissões em uma política do IAM.

  Política do IAM significa que você pode especificar a permissão apenas em uma política do IAM.
- Uso entre contas mostra as operações que os usuários autorizados podem executar em recursos em uma Conta da AWS diferente.

  Um valor de Yes (Sim) significa que as entidades principais podem executar a operação em recursos em uma Conta da AWS diferente.

  Um valor de No (Não) significa que as entidades principais podem executar a operação somente em recursos da própria Conta da AWS.

  Se você conceder a uma entidade principal em uma conta diferente uma permissão que não pode ser usada em um recurso entre contas, essa permissão não será efetiva. Por exemplo, se você der TagResource permissão a um principal em uma conta diferente kms: para uma chave KMS em sua conta, as tentativas dele de marcar a chave KMS em sua conta falharão.
- Recursos lista os AWS KMS recursos aos quais as permissões se aplicam. AWS KMS suporta dois tipos de recursos: uma chave KMS e um alias. Em uma política de chaves, o valor do elemento `Resource` é sempre `*`, o que indica a chave do KMS à qual a política de chaves está anexada.

  Use os valores a seguir para representar um AWS KMS recurso em uma política do IAM.

  Chave KMS

  Quando o recurso for uma chave do KMS, use seu ARN de chave. Para obter ajuda, consulte the section called “Como encontrar o ID e o ARN da chave”.

  `arn:`*`AWS_partition_name`*`:kms:`*`AWS_Region`*`:`*`AWS_account_ID`*`:key/`*`key_ID`*

  Por exemplo: .

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

Alias

Quando o recurso for um alias, use seu ARN do alias. Para obter ajuda, consulte the section called “Encontrar o nome e o ARN do alias”.

`arn:AWS_partition_name:kms:AWS_region:AWS_account_ID:alias/alias_name`

Por exemplo: .

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

***** (asterisco)

Quando a permissão não se aplicar a um recurso específico (chave do KMS ou alias), use um asterisco (`*`).

Em uma política do IAM para uma AWS KMS permissão, um asterisco no `Resource` elemento indica todos os AWS KMS recursos (chaves e aliases do KMS). Você também pode usar um asterisco no `Resource` elemento quando a AWS KMS permissão não se aplica a nenhuma chave ou alias KMS em particular. Por exemplo, ao permitir ou negar `kms:CreateKey` ou ao permitir `kms:ListKeys`, é possível definir o elemento `Resource` como `*` ou como uma variação específica da conta, por exemplo, `arn:AWS_partition_name:kms:AWS_region:AWS_account_ID:*`.

- AWS KMS as chaves de AWS KMS condição listam as chaves de condição que você pode usar para controlar o acesso à operação. Especifique as condições no elemento `Condition` de uma política. Para ter mais informações, consulte AWS KMS chaves de condição. Essa coluna também inclui chaves de condição AWS globais que são suportadas por AWS KMS, mas não por todos os AWS serviços.

Testar suas permissões

Para usar o AWS KMS, você deve ter credenciais que a AWS possa usar para autenticar suas solicitações de API. As credenciais devem incluir permissões para acessar chaves KMS e aliases. As permissões são determinadas pelas política de chave, políticas do IAM, concessões e controles de acesso entre contas. Além de controlar o acesso às chaves KMS, é possível controlar o acesso ao seu CloudHSM e aos seus repositórios de chaves personalizados.

É possível especificar o parâmetro da API `DryRun` para verificar se você tem as permissões necessárias para usar as chaves do AWS KMS. Também é possível usar `DryRun` para verificar

se os parâmetros de solicitação em uma chamada de API do AWS KMS estão especificados corretamente.

Tópicos

- Qual é o DryRun parâmetro?
- Especificando DryRun com a API

Qual é o DryRun parâmetro?

`DryRun` é um parâmetro de API opcional que você especifica para verificar se as chamadas da API do AWS KMS serão bem-sucedidas. Use `DryRun` para testar sua chamada de API, antes de realmente fazer a chamada para o AWS KMS. É possível verificar o seguinte:

- Que você tem as permissões necessárias para usar as chaves do AWS KMS.
- Que você especificou os parâmetros na chamada corretamente.

AWS KMS oferece suporte ao uso do parâmetro `DryRun` em determinadas ações da API:

- CreateGrant
- Decrypt
- Encrypt
- GenerateDataKey
- GenerateDataKeyPair
- GenerateDataKeyPairWithoutPlaintext
- GenerateDataKeyWithoutPlaintext
- GenerateMac
- ReEncrypt
- RetireGrant
- RevokeGrant
- Sign
- Verificar
- VerifyMac

O uso do parâmetro `DryRun` incorrerá em cobranças e será cobrado como uma solicitação de API padrão. Para obter mais informações sobre os preços do AWS KMS, consulte Definição de preço do AWS Key Management Service.

Todas as solicitações de API que usam o parâmetro `DryRun` se aplicam à cota de solicitações da API e podem resultar em uma exceção de controle de utilização se você exceder a cota de solicitação da API. Por exemplo, chamar Decrypt com `DryRun` ou sem `DryRun` conta na mesma cota de operações criptográficas. Para saber mais, consulte Solicitações de AWS KMS limitação.

Toda chamada para uma operação de API do AWS KMS é capturada como um evento e gravada em um log do AWS CloudTrail. A saída de qualquer operação que especifique o `DryRun` parâmetro aparece no seu CloudTrail registro. Para ter mais informações, consulte Registrando chamadas de AWS KMS API com AWS CloudTrail.

Especificando DryRun com a API

Para usar `DryRun`, especifique o parâmetro `–dry-run` nos comandos AWS CLI e chamadas de API do AWS KMS compatíveis com o parâmetro. Ao fazer isso, o AWS KMS verificará se sua chamada será bem-sucedida. As chamadas do AWS KMS que usam `DryRun` sempre falharão e retornarão uma mensagem com informações sobre o motivo pelo qual a chamada falhou. A mensagem pode incluir as seguintes exceções:

- `DryRunOperationException` - A solicitação seria bem-sucedida se `DryRun` não estivesse especificada.
- `ValidationException` - A solicitação falhou devido à especificação de um parâmetro de API incorreto.
- `AccessDeniedException` - Você não tem permissões para realizar a ação de API especificada no recurso KMS.

Por exemplo, o comando a seguir usa a CreateGrantoperação e cria uma concessão que permite que os usuários autorizados a assumir a `keyUserRole` função chamem a operação Decrypt em uma chave KMS simétrica especificada. O parâmetro `DryRun` está especificado.

```
$  aws kms create-grant \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --grantee-principal arn:aws:iam::111122223333:role/keyUserRole \
    --operations Decrypt \
    --dry-run
```

Chaves para fins especiais

O AWS Key Management Service (AWS KMS) oferece suporte vários tipos diferentes de chaves para diferentes usos.

Ao criar uma AWS KMS key, você recebe por padrão uma chave do KMS de criptografia simétrica. No AWS KMS, uma chave do KMS de criptografia simétrica representa uma chave de criptografia AES-GCM de 256 bits que é usada para criptografia e descriptografia, exceto nas regiões da China, em que ela representa uma chave simétrica de 128 bits que usa a criptografia SM4. O material de chave simétrica nunca sai descriptografado do AWS KMS. A menos que sua tarefa exija explicitamente criptografia assimétrica ou chaves de Hash-based message authentication code (HMAC – Código de autenticação de mensagem por hash), as chaves do KMS de criptografia simétrica, que nunca saem descriptografadas do AWS KMS, são uma boa opção. Além disso, os serviços da AWS que são integrados ao AWS KMS usam exclusivamente chaves do KMS de criptografia simétrica para criptografar seus dados. Esses serviços não fornecem suporte para criptografia com chaves do KMS assimétricas.

É possível usar uma chave do KMS de criptografia simétrica no AWS KMS para criptografar, descriptografar e recriptografar dados, gerar chaves de dados e pares de chaves de dados, além de gerar strings de bytes aleatórios. Você pode importar seu próprio material de chave para uma chave do KMS de criptografia simétrica e criar chaves do KMS de criptografia simétrica em armazenamentos personalizados de chaves. Para acessar uma tabela comparativa das operações que você pode executar em chaves do KMS simétricas e assimétricas, consulte Referência de tipos de chaves.

O AWS KMS também é compatível com os seguintes tipos de chaves do KMS de finalidade especial:

- Chaves RSA assimétricas para criptografia da chave pública
- Chaves RSA assimétricas e ECC para assinatura e verificação
- Chaves SM2 assimétricas (somente nas regiões da China) para criptografia de chave pública ou assinatura e verificação
- Chaves de HMAC para gerar e verificar códigos de autenticação de mensagem por hash
- Chaves de várias regiões (simétricas e assimétricas) que funcionam como cópias da mesma chave em diferentes Regiões da AWS
- Chaves com material de chave importado fornecido por você

- Chaves em um armazenamento de chaves personalizado com o suporte de um cluster do AWS CloudHSM ou de um gerenciador de chaves externas fora da AWS.

Escolha de um tipo de chave do KMS

O AWS KMS é compatível com vários tipos de chaves do KMS: chaves de criptografia simétrica, chaves de HMAC simétrica, chaves de criptografia assimétrica e chaves de assinatura assimétrica.

As chaves do KMS diferem porque contêm diferentes materiais criptográficos de chave.

- Chave do KMS de criptografia simétrica: representa uma única chave de criptografia AES-GCM de 256 bits, exceto nas regiões da China, em que ela representa uma chave de criptografia SM4 de 128 bits. O material de chave simétrica nunca sai descriptografado do AWS KMS. Para usar a chave do KMS de criptografia simétrica, é necessário chamar o AWS KMS.

  As chaves de criptografia simétrica, que são as chaves padrão do KMS, são ideais para a maioria dos usos. Se você precisar de uma chave do KMS para proteger seus dados em um AWS service (Serviço da AWS), use uma chave de criptografia simétrica, a menos que receba instruções para usar outro tipo de chave.
- Chave do KMS assimétrica: representa uma chave pública e um par de chaves privadas matematicamente relacionados que podem ser usados para criptografar e descriptografar ou para assinar e verificar, mas não ambos. A chave privada nunca deixa o AWS KMS descriptografado. É possível usar a chave pública no AWS KMS chamando as operações de API do AWS KMS ou baixando a chave pública e usando-a fora do AWS KMS.
- Chave do KMS de HMAC (simétrica): representa uma chave simétrica de comprimento variável que é usada para gerar e verificar códigos de autenticação de mensagem por hash. O material de chave em uma chave do KMS de HMAC nunca sai descriptografado do AWS KMS. Para usar sua chave do KMS de HMAC, é necessário chamar o AWS KMS.

O tipo de chave do KMS criada depende em grande parte de como você planeja usar a chave do KMS e dos requisitos de segurança e de autorização. Ao criar sua chave do KMS, lembre-se de que a configuração criptográfica da chave do KMS, incluindo sua especificação de chave e uso de chave, é estabelecida ao criar a chave do KMS e não pode ser alterada.

Use as orientações a seguir para determinar o tipo de chave do KMS necessário com base no seu caso de uso.

Criptografar e descriptografar dados

Use uma chave do KMS simétrica para a maioria dos casos de uso que exigem criptografia e descriptografia dos dados. O algoritmo de criptografia simétrica usado pelo AWS KMS é rápido, eficiente e garante a confidencialidade e a autenticidade dos dados. Ele oferece suporte à criptografia autenticada com dados adicionais autenticados (ADD), definidos como um contexto de criptografia. Esse tipo de chave do KMS exige que o remetente e o destinatário dos dados criptografados tenham credenciais válidas da AWS para chamar o AWS KMS.

Se o seu caso de uso exige criptografia fora do AWS por usuários que não podem chamar o AWS KMS, as chaves do KMS assimétricas são uma boa escolha. Você pode distribuir a parte pública da chave do KMS assimétrica para permitir que esses usuários criptografem dados. Além disso, as aplicações que precisam descriptografar esses dados podem usar a chave privada da chave do KMS assimétrica no AWS KMS.

Assinar mensagens e verificar assinaturas

Para assinar mensagens e verificar assinaturas, é necessário usar uma chave do KMS assimétrica. É possível usar uma chave do KMS com uma especificação de chave que representa um par de chaves RSA, um par de chaves de curva elíptica (ECC) ou um par de chaves SM2 (somente nas regiões da China). A especificação de chave escolhida é determinada pelo algoritmo de assinatura que você deseja usar. Os algoritmos de assinatura ECDSA compatíveis com os pares de chaves ECC são recomendados em vez dos algoritmos de assinatura RSA. No entanto, pode ser necessário usar uma especificação de chave e um algoritmo de assinatura específicos para oferecer suporte aos usuários que verificam assinaturas de forma externa à AWS.

Executar criptografia de chave pública

Para executar a criptografia da chave pública, é necessário usar uma chave do KMS assimétrica com uma especificação de chave RSA ou uma especificação de chave SM2 (somente nas regiões da China). Para criptografar dados no AWS KMS com a chave pública de um par de chaves do KMS, use a operação Encrypt (Criptografar). Também é possível fazer download da chave pública e compartilhá-la com as partes que precisam criptografar dados fora do AWS KMS.

Ao baixar a chave pública de uma chave do KMS assimétrica, é possível usá-la fora do AWS KMS. No entanto, ela não está mais sujeita aos controles de segurança que protegem a chave do KMS no AWS KMS. Por exemplo, não é possível usar concessões ou políticas de chaves do AWS KMS para controlar o uso da chave pública. Também não é possível controlar se a chave é usada somente para criptografia e descriptografia usando os algoritmos de criptografia

compatíveis com o AWS KMS. Para obter mais detalhes, consulte Considerações especiais sobre o download de chaves públicas.

Para descriptografar dados que foram criptografados com a chave pública fora do AWS KMS, chame a operação Decrypt. Ocorrerá falha na operação do `Decrypt` se os dados tiverem sido criptografados em uma chave pública de uma chave do KMS com um uso de chave de `SIGN_VERIFY`. Também ocorrerá falha se eles tiverem sido criptografados usando um algoritmo não compatível com o AWS KMS para a especificação de chave selecionada. Para obter mais informações sobre especificações de chaves e algoritmos com suporte, consulte Especificações de chaves assimétricas.

Para evitar esses erros, qualquer pessoa que esteja usando uma chave pública fora do AWS KMS deve armazenar a configuração da chave. O AWS KMS console e a GetPublicKeyresposta fornecem as informações que você deve incluir ao compartilhar a chave pública.

Gerar e verificar códigos de HMAC

Para gerar e verificar códigos de autenticação de mensagem por hash, use uma chave do KMS de HMAC. Ao criar uma chave de HMAC no AWS KMS, o AWS KMS cria e protege o material de chave, garantindo que você use os algoritmos de Message authentication code (MAC – Código de autenticação de mensagem) corretos para sua chave. Também é possível usar os códigos de HMAC como números pseudo-aleatórios e para assinatura simétrica e tokenização em determinados cenários.

As chaves do KMS de HMAC são chaves simétricas. Ao criar uma chave do KMS de HMAC no console do AWS KMS, escolha o tipo de chave `Symmetric`.

Usar com serviços da AWS

Para criar uma chave do KMS para uso com um serviço da AWS integrado ao AWS KMS, consulte a documentação do serviço. Os serviços da AWS que criptografam seus dados exigem uma chave do KMS de criptografia simétrica.

Além dessas considerações, as operações criptográficas em chaves do KMS com diferentes especificações de chave têm preços e cotas de solicitação diferentes. Para obter mais informações sobre a definição de preço do AWS KMS, consulte Definição de preço do AWS Key Management Service. Para obter mais informações sobre cotas de solicitações, consulte Cotas de solicitações.

Selecionar o uso de chave

O uso de chave de uma chave do KMS determina se a chave do KMS será usada para criptografia e descriptografia ou para assinatura e verificação ou para geração e verificação de etiquetas de HMAC. Cada chave do KMS pode ter apenas um uso. O uso de uma chave do KMS para mais de um tipo de operação torna o produto de todas as operações mais vulnerável a ataques.

Conforme apresentado na tabela a seguir, as chaves do KMS de criptografia simétrica só podem ser usadas para criptografia e descriptografia. As chaves do KMS de HMAC só podem ser usadas para gerar e verificar códigos de HMAC. As chaves do KMS de curva elíptica (ECC) podem ser usadas somente para assinatura e verificação. Você só precisa decidir sobre um uso de chave para chaves do KMS RSA.

Uso de chave válido para tipos de chaves do KMS

Tipo de chave do KMS	Criptografar e descriptografar ENCRYPT_DECRYPT	Assinar e verificar SIGN_VERIFY	Gerar e verificar MAC GENERATE_VERIFY_MAC
Chaves do KMS de criptografia simétrica	✓	⊗	⊗
Chaves do KMS de HMAC (simétrica)	⊗	⊗	✓
Chaves do KMS assimétricas com pares de chaves RSA	✓	✓	⊗
Chaves do KMS assimétricas com pares de chaves de ECC	⊗	✓	⊗
Chaves do KMS assimétricas com pares de chaves SM2	✓	✓	⊗

Tipo de chave do KMS	Criptografar e descriptografar ENCRYPT_DECRYPT	Assinar e verificar SIGN_VERIFY	Gerar e verificar MAC GENERATE_VERIFY_MAC
(somente nas regiões da China)			

No console do AWS KMS, primeiro você escolhe o tipo de chave (simétrica ou assimétrica) e, em seguida, o uso de chave. O tipo de chave escolhido determina quais opções de uso de chave são exibidas. O uso de chave escolhido determina quais especificações de chave são exibidas, se for o caso.

Para escolher um uso de chave no console do AWS KMS:

- Para chaves do KMS de criptografia simétrica (padrão), escolha Encrypt and decrypt (Criptografar e descriptografar).
- Para chaves do KMS de HMAC, escolha Generate and verify MAC (Gerar e verificar MAC).
- Para chaves do KMS assimétricas com material de chave de Elliptic curve (ECC – Criptografia de curva elíptica), escolha Sign and verify (Assinar e verificar).
- Para chaves do KMS assimétricas com material de chave RSA, selecione Encrypt and decrypt (Criptografar e descriptografar) ou Sign and verify (Assinar e verificar).
- Para chaves do KMS assimétricas com material de chave SM2, selecione Encrypt and decrypt (Criptografar e descriptografar) ou Sign and verify (Assinar e verificar). A especificação de chave SM2 está disponível somente nas regiões da China.

Para permitir que os diretores criem chaves KMS somente para um determinado uso de chave, use a chave de condição kms: KeyUsage. Também é possível usar a chave de condição `kms:KeyUsage` para permitir que as entidades principais chamem operações de API para uma chave do KMS baseada em seu uso de chave. Por exemplo, apenas será possível conceder permissão para desabilitar uma chave do KMS se o seu uso de chave for SIGN_VERIFY.

Selecionar a especificação de chave

Ao criar uma chave do KMS assimétrica ou uma chave do KMS de HMAC, selecione sua especificação de chave. A especificação de chave, que é uma propriedade de cada AWS KMS key, representa a configuração criptográfica da sua chave do KMS. Você escolhe a especificação de chave ao criar a chave do KMS e não pode alterá-la. Se você tiver escolhido a especificação de chave errada, exclua a chave do KMS e crie outra.

> **Note**
>
> A especificação de chave para uma chave do KMS era conhecida como “especificação de chave mestra do cliente”. O `CustomerMasterKeySpec` parâmetro da CreateKeyoperação está obsoleto. Em vez disso, use o parâmetro `KeySpec`. A resposta das DescribeKeyoperações `CreateKey` e inclui um `CustomerMasterKeySpec` membro `KeySpec` e com o mesmo valor.

A especificação de chave determina se a chave do KMS é simétrica ou assimétrica, o tipo de material de chave na chave do KMS e os algoritmos de criptografia, algoritmos de assinatura ou algoritmos de MAC compatíveis com o AWS KMS para a chave do KMS. A especificação de chave escolhida normalmente é determinada pelo caso de uso e pelos requisitos regulatórios. No entanto, as operações criptográficas em chaves do KMS com especificações de chave diferentes são cobradas de maneira diferente e estão sujeitas a cotas diferentes. Para obter detalhes sobre os preços, consulte AWS Key Management Service Pricing (Preços do). Para obter mais informações sobre cotas de solicitações, consulte Cotas de solicitações.

Para determinar as principais especificações que os diretores da sua conta podem usar para chaves KMS, use a chave de condição kms:. KeySpec

O AWS KMS é compatível com as seguintes especificações de chave para chaves do KMS:

Especificações da chave de criptografia simétrica (padrão)

- SYMMETRIC_DEFAULT

Especificações de chave de HMAC

- HMAC_224
- HMAC_256
- HMAC_384

- HMAC_512

Especificações de chave RSA (criptografia e descriptografia ou assinatura e verificação)

- RSA_2048
- RSA_3072
- RSA_4096

Especificações da chave de curva elíptica

- Pares de chaves de curva elíptica assimétricas recomendadas pelo NIST (assinatura e verificação)
  - ECC_NIST_P256 (secp256r1)
  - ECC_NIST_P384 (secp384r1)
  - ECC_NIST_P521 (secp521r1)
- Outros pares de chaves de curva elíptica assimétricas (assinatura e verificação)
  - ECC_SECG_P256K1 (secp256k1), normalmente usado para criptomoedas.

Especificação de chave SM2 (criptografia e descriptografia ou assinatura e verificação)

- SM2 (somente nas regiões da China)

Chaves assimétricas no AWS KMS

O AWS KMS é compatível com chaves do KMS assimétricas que representam pares de chaves pública e privada RSA, de curva elíptica (ECC) ou SM2 (somente nas regiões da China) matematicamente relacionados. Esses pares de chaves são gerados em módulos de segurança de hardware do AWS KMS certificados sob o Programa de validação de módulos criptográficos FIPS 140-2, exceto nas regiões China (Pequim) e China (Ningxia). A chave privada nunca deixa os HSMs do AWS KMS descriptografadas. Você pode baixa a chave pública para distribuição e usá-la fora do AWS. É possível usar chaves do KMS assimétricas para criptografia e descriptografia ou para assinatura e verificação, mas não para ambos.

É possível criar e gerenciar as chaves do KMS assimétricas na sua Conta da AWS, incluindo configurar políticas de chaves, políticas do IAM e concessões que controlam o acesso às chaves do KMS, além de habilitar e desabilitar as chaves do KMS, criar tags e aliases e excluir chaves do KMS. E você pode auditar todas as operações que usam ou gerenciam chaves do KMS na AWS em logs do AWS CloudTrail.

O AWS KMS também fornece pares de chaves de dados assimétricas que foram desenvolvidos para serem usados para criptografia no lado do cliente fora do AWS KMS. A chave privada em um par de chaves de dados assimétricas são protegidas por uma chave do KMS de criptografia simétrica no AWS KMS.

Este tópico explica como as chaves do KMS assimétricas funcionam, suas diferenças em relação a outras chaves do KMS e como decidir o tipo de chave do KMS de que você precisa para proteger seus dados. Ele também explica como pares de chaves de dados assimétricas funcionam e como usá-los fora do AWS KMS.

Regiões

Chaves do KMS assimétricas e pares de chaves de dados assimétricos têm suporte em todas as Regiões da AWS para as quais o AWS KMS oferece suporte.

Saiba mais

- Para criar chaves do KMS assimétricas, consulte Criar chaves do KMS assimétricas. Para criar chaves do KMS de criptografia simétrica, consulte Criar chaves.
- Para criar chaves do KMS assimétricas de várias regiões, consulte Criar chaves de várias regiões.
- Para descobrir se uma chave do KMS é simétrica ou assimétrica, consulte Identificar chaves do KMS assimétricas.
- Para acessar uma tabela que compara as operações de API do AWS KMS que se aplicam a cada tipo de chave do KMS, consulte the section called “Referência de tipos de chaves”.
- Para controlar o acesso às especificações da chave, o uso da chave, os algoritmos de criptografia e os algoritmos de assinatura que as entidades principais na sua conta podem usar para chaves do KMS, consulte the section called “AWS KMS chaves de condição”.
- Para saber mais sobre as cotas de solicitação que se aplicam aos diferentes tipos de chaves do KMS, consulte the section called “Cotas de solicitações”.
- Para saber como assinar mensagens e verificar assinaturas com chaves do KMS assimétricas, consulte Assinatura digital com o novo recurso de chaves assimétricas do AWS KMS no Blog de segurança da AWS.

Tópicos

- Chaves do KMS assimétricas
- Criar chaves do KMS assimétricas
- Fazer download de chaves públicas

- Identificar chaves do KMS assimétricas
- Especificações de chave assimétrica

Chaves do KMS assimétricas

É possível criar uma chave do KMS assimétrica no AWS KMS. Uma chave do KMS assimétrica representa um par de chave pública e chave privada matematicamente relacionadas. É possível dar a chave privada para qualquer pessoa, mesmo se ela não for confiável, mas a chave privada deve ser mantida em segredo.

Em uma chave do KMS assimétrica, a chave privada é criada no AWS KMS e nunca deixa o AWS KMS descriptografada. Para usar a chave privada, é necessário chamar o AWS KMS. É possível usar a chave pública no AWS KMS chamando as operações de API do AWS KMS. Ou é possível fazer download da chave pública e usá-la fora do AWS KMS.

Se o seu caso de uso exige criptografia fora do AWS por usuários que não podem chamar o AWS KMS, as chaves do KMS assimétricas são uma boa escolha. No entanto, se estiver criando uma chave do KMS para criptografar os dados armazenados ou gerenciados em um serviço da AWS, use uma chave do KMS de criptografia simétrica. Os serviços da AWS que são integrados ao AWS KMS usam chaves do KMS de criptografia simétrica para criptografar seus dados. Esses serviços não fornecem suporte para criptografia com chaves do KMS assimétricas.

O AWS KMS é compatível com três tipos de chaves do KMS assimétricas.

- Chaves do KMS RSA: uma chave do KMS com um par de chaves RSA para criptografia de descriptografia ou assinatura e verificação (mas não ambos). O AWS KMS oferece suporte a vários comprimentos de chave para requisitos de segurança diversificados.
- Chaves do KMS de curva elíptica (ECC): uma chave do KMS com um par de chaves de curva elíptica para assinatura e verificação. O AWS KMS oferece suporte a várias curvas comumente utilizadas.
- Chaves do KMS SM2 (somente regiões da China): uma chave do KMS com um par de chaves SM2 para criptografia e descriptografia ou para assinatura e verificação (mas não ambos).

Para obter ajuda na escolha da sua configuração de chave assimétrica, consulte Escolha de um tipo de chave do KMS. Para obter detalhes técnicos sobre os algoritmos de criptografia e assinatura compatíveis com o AWS KMS para chaves do KMS RSA, consulte Especificações de chaves RSA. Para obter detalhes técnicos sobre os algoritmos de assinatura compatíveis com o AWS KMS para

chaves do KMS ECC, consulte Especificações de chaves de curva elíptica. Para obter detalhes técnicos sobre os algoritmos de criptografia e de assinatura compatíveis com o AWS KMS para chaves SM2 do KMS (somente para regiões da China), consulte Especificações da chave SM2.

Para acessar uma tabela comparando as operações que podem ser executadas em chaves do KMS simétricas e assimétricas, consulte Comparar chaves do KMS simétricas e assimétricas. Para obter ajuda para determinar se uma chave do KMS é simétrica ou assimétrica, consulte Identificar chaves do KMS assimétricas.

Regiões

Chaves do KMS assimétricas e pares de chaves de dados assimétricos têm suporte em todas as Regiões da AWS para as quais o AWS KMS oferece suporte.

Criar chaves do KMS assimétricas

Você pode criar chaves KMS assimétricas no AWS KMS console, usando a CreateKeyAPI ou usando um modelo. AWS CloudFormation Uma chave do KMS assimétrica representa um par de chaves pública e privada que pode ser usado para criptografia ou assinatura. A chave privada permanece no AWS KMS. Para baixar a chave pública para uso fora do AWS KMS, consulte Fazer download de chaves públicas.

Ao criar uma chave do KMS para criptografar dados que você armazena ou gerencia em um serviço da AWS, use uma chave do KMS de criptografia simétrica. Os serviços da AWS que têm integração com o AWS KMS não são compatíveis com chaves do KMS assimétricas. Para ajudar a decidir se você vai criar uma chave do KMS simétrica ou assimétrica, consulte Escolha de um tipo de chave do KMS.

Para obter informações sobre as permissões necessárias para criar chaves do KMS, consulte Permissões para criar chaves do KMS.

Tópicos

- Criar chaves do KMS assimétricas (console)
- Criar chaves do KMS assimétricas (API do AWS KMS)

Criar chaves do KMS assimétricas (console)

É possível usar o AWS Management Console para criar AWS KMS keys (chaves do KMS) assimétricas. Cada chave do KMS assimétrica representa um par de chaves pública e privada.

> **Important**
>
> Não inclua informações confidenciais ou sigilosas no alias, na descrição ou nas tags. Esses campos podem aparecer em texto simples em CloudTrail registros e outras saídas.

1. Faça login no AWS Management Console e abra o console do AWS Key Management Service (AWS KMS) em https://console.aws.amazon.com/kms.
2. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.
3. No painel de navegação, escolha Customer managed keys (Chaves gerenciadas pelo cliente).
4. Escolha Create key (Criar chave).
5. Para criar uma chave do KMS assimétrica, em Key type (Tipo de chave), selecione Asymmetric (Assimétrica).

   Para obter informações sobre como criar uma chave do KMS de criptografia simétrica no console do AWS KMS, consulte Criar chaves do KMS de criptografia simétrica (console).
6. Para criar uma chave do KMS assimétrica para assinar mensagens e verificar assinaturas, em Key usage (Uso de chaves), selecione Encrypt and decrypt (Criptografar e descriptografar). Ou, para criar uma chave do KMS assimétrica para assinar mensagens e verificar assinaturas, em Key usage (Uso de chave), selecione Sign and verify (Assinar e verificar).

   Para ajudar a escolher um valor de uso de chave, consulte Selecionar o uso de chave.
7. Escolha uma especificação (Especificação da chave) para a chave do KMS assimétrica.

   Geralmente a especificação de chave escolhida é determinada por requisitos regulatórios, de segurança ou de negócios. Ela também pode ser influenciada pelo tamanho das mensagens que você precisa criptografar ou assinar. Em geral, chaves de criptografia maiores são mais resistentes a ataques de força bruta.

   Para ajudar para escolher uma especificação de chave, consulte Selecionar a especificação de chave.
8. Escolha Próximo.
9. Digite um alias para a chave do KMS. O nome do alias não pode começar com **`aws/`**. O prefixo **`aws/`** é reservado pela Amazon Web Services para representar as Chaves gerenciadas pela AWS na sua conta.

Um alias é um nome amigável que você pode usar para identificar a chave do KMS no console e em algumas APIs do AWS KMS. Recomendamos que você escolha um alias que indique o tipo de dados que pretende proteger ou a aplicação a ser usada com a chave do KMS.

Aliases são necessários ao criar uma chave do KMS no AWS Management Console. Você não pode especificar um alias ao usar a CreateKeyoperação, mas pode usar o console ou a CreateAliasoperação para criar um alias para uma chave KMS existente. Para obter detalhes, consulte Usar aliases.

10. (Opcional) Digite uma descrição para a chave do KMS.

    Insira uma descrição que explique o tipo de dados que você planeja proteger ou a aplicação que planeja usar com a chave do KMS.

    Você pode adicionar uma descrição agora ou atualizá-la a qualquer momento, a não ser que o estado da chave seja `Pending Deletion` ou `Pending Replica Deletion`. Para adicionar, alterar ou excluir a descrição de uma chave gerenciada pelo cliente existente, edite a descrição na operação AWS Management Console ou use a UpdateKeyDescriptionoperação.

11. (Opcional) Digite uma chave de tag e um valor de tag opcional. Para adicionar mais de uma etiqueta à chave do KMS, selecione Add tag (Adicionar etiqueta).

    Ao adicionar tags aos recursos da AWS, a AWS gera um relatório de alocação de custos com utilização e custos agrupados por tags. Etiquetas também podem ser utilizadas para controlar o acesso a uma chave do KMS. Para informações sobre marcação de chaves do KMS, consulte Marcar chaves com tags e ABAC para AWS KMS.

12. Escolha Próximo.

13. Selecione os usuários e as funções do IAM que podem administrar a chave do KMS.

> **Note**
>
> Esta política de chave concede controle total dessa chave do KMS à Conta da AWS. Ela permite que os administradores de conta usem políticas do IAM para conceder a outras entidades principais a permissão para gerenciar a chave do KMS. Para obter detalhes, consulte the section called “Política de chaves padrão”.
> As práticas recomendadas do IAM não encorajam o uso de usuários do IAM com credenciais de longo prazo. Sempre que possível, use os perfis do IAM, por fornecerem

credenciais temporárias. Para obter detalhes, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

14. (Opcional) Para evitar que os usuários e funções do IAM selecionados excluam essa chave do KMS, na seção Key deletion (Exclusão de chaves) na parte inferior da página, desmarque a caixa de seleção Allow key administrators to delete this key (Permitir que os administradores de chaves excluam essa chave).
15. Escolha Próximo.
16. Selecione os usuários e as funções do IAM que podem usar a chave do KMS para operações de criptografia.

> **Note**
>
> Esta política de chave concede controle total dessa chave do KMS à Conta da AWS. Ela permite que os administradores de conta usem políticas do IAM para conceder a outras entidades principais a permissão para usar a chave do KMS em operações de criptografia. Para obter detalhes, consulte the section called “Política de chaves padrão”. As práticas recomendadas do IAM não encorajam o uso de usuários do IAM com credenciais de longo prazo. Sempre que possível, use os perfis do IAM, por fornecerem credenciais temporárias. Para obter detalhes, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

17. (Opcional) Você pode permitir que outras Contas da AWS usem essa chave do KMS para operações de criptografia. Para fazer isso, na parte inferior da página na seção Other Contas da AWS (Outras), escolha Add another Conta da AWS (Adicionar outra) e insira o número de identificação da Conta da AWS de uma conta externa. Para adicionar várias contas externas, repita essa etapa.

> **Note**
>
> Para permitir que as entidades principais de contas externas usem a chave do KMS, os administradores da conta externa devem criar políticas do IAM que forneçam essas permissões. Para ter mais informações, consulte Permitir que usuários de outras contas usem uma chave do KMS.

18. Escolha Próximo.

19. Revise as configurações que você escolheu. Ainda é possível voltar e alterar todas as configurações.
20. Selecione Finish (Concluir) para criar a chave do KMS.

Criar chaves do KMS assimétricas (API do AWS KMS)

Você pode usar a CreateKeyoperação para criar uma assimétricaAWS KMS key. Estes exemplos usam a AWS Command Line Interface (AWS CLI), mas você pode usar qualquer linguagem de programação compatível.

Ao criar uma chave do KMS assimétrica, você deve especificar o parâmetro `KeySpec`, que determina o tipo de chaves que criado. Além disso, é necessário especificar um valor `KeyUsage` de ENCRYPT_DECRYPT ou SIGN_VERIFY. Não é possível alterar essas propriedades depois que a chave do KMS é criada.

A `CreateKey` operação não permite que você especifique um alias, mas você pode usar a CreateAliasoperação para criar um alias para sua nova chave KMS.

> **Important**
>
> Não inclua informações confidenciais ou sigilosas nos campos `Description` ou `Tags`. Esses campos podem aparecer em texto simples em CloudTrail registros e outras saídas.

O exemplo a seguir usa a operação `CreateKey` para criar uma chave do KMS assimétrica de chaves RSA de 4.096 bits projetada para criptografia de chave pública.

```
$ 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
    }
}
```

O comando de exemplo a seguir cria uma chave KMS assimétrica que representa um par de chaves ECDSA usado para assinatura e verificação. Não é possível criar um par de chaves de curva elíptica para criptografia e descriptografia.

```
$ 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"
    }
}
```

Fazer download de chaves públicas

É possível visualizar, copiar e baixar a chave pública de um par de chaves do KMS assimétricas usando o AWS Management Console ou a API do AWS KMS. É necessário ter a permissão `kms:GetPublicKey` na chave do KMS assimétrica.

Cada par de chaves do KMS assimétricas consiste em uma chave privada que nunca sai do AWS KMS descriptografada e em uma chave pública que pode ser baixada e compartilhada.

Você pode compartilhar uma chave pública para permitir que outras pessoas criptografem dados fora do AWS KMS que você só pode descriptografar com a chave privada. Ou para permitir que outras pessoas verifiquem uma assinatura digital fora do AWS KMS que você gerou com a chave privada.

Ao usar a chave pública na sua chave do KMS assimétrica dentro do AWS KMS, você se beneficia da autenticação, autorização e registro em log que fazem parte de cada operação do AWS KMS. Você também reduz o risco de criptografar dados que não podem ser descriptografados. Esses recursos não têm efeito fora do AWS KMS. Para obter detalhes, consulte Considerações especiais sobre o download de chaves públicas.

> **Tip**
>
> Está procurando por chaves de dados ou chaves SSH? Este tópico explica como gerenciar chaves assimétricas no AWS Key Management Service, onde a chave privada não é exportável. Para pares de chaves de dados exportáveis em que a chave privada é protegida por uma chave KMS de criptografia simétrica, consulte. GenerateDataKeyPair Para obter ajuda com o download da chave pública associada a uma instância do Amazon EC2, consulte Recuperação da chave pública no Guia do usuário do Amazon EC2 para instâncias do Linux e no Guia do usuário do Amazon EC2 para instâncias do Windows.

Tópicos

- Considerações especiais sobre o download de chaves públicas
- Baixar uma chave pública (console)
- Baixar uma chave pública (API do AWS KMS)

Considerações especiais sobre o download de chaves públicas

Para proteger suas chaves do KMS, o AWS KMS fornece controles de acesso, criptografia autenticada e logs detalhados de cada operação. O AWS KMS também permite evitar o uso de chaves do KMS de maneira temporária ou permanente. Por fim, as operações do AWS KMS são projetadas para minimizar o risco de criptografar dados que não podem ser descriptografados. Esses recursos não estão disponíveis quando você usa chaves públicas obtidas por download fora do AWS KMS.

Autorização

As políticas de chaves e as políticas do IAM que controlam o acesso à chave do KMS no AWS KMS não têm efeito nas operações realizadas fora da AWS. Qualquer usuário que possa obter a chave pública pode usá-lo fora do AWS KMS, mesmo que não tenha permissão para criptografar dados ou verificar assinaturas com a chave do KMS.

Restrições de uso da chave

As principais restrições de uso não têm efeito fora do AWS KMS. Se você chamar a operação Encrypt com uma chave do KMS que tenha um `KeyUsage` de `SIGN_VERIFY`, a operação do AWS KMS falhará. Porém, se você criptografar dados fora do AWS KMS com uma chave pública de uma chave do KMS com um `KeyUsage` de `SIGN_VERIFY`, os dados não poderão ser descriptografados.

Restrições de algoritmo

As restrições aos algoritmos de criptografia e de assinatura compatíveis com o AWS KMS não têm efeito fora do AWS KMS. Se você criptografar dados com a chave pública de uma chave do KMS fora do AWS KMS e usar um algoritmo de criptografia não compatível com o AWS KMS, os dados não poderão ser descriptografados.

Desabilitar e excluir chaves do KMS

As ações que você pode tomar para evitar o uso da chave do KMS em uma operação criptográfica dentro do AWS KMS não impedem ninguém de usar a chave pública fora do AWS KMS. Por exemplo, desabilitar uma chave do KMS, programar a exclusão de uma chave do KMS, excluir uma chave do KMS ou excluir o material de chave de uma chave do KMS não têm efeito em uma chave pública fora do AWS KMS. Se você excluir uma chave do KMS assimétrica ou se excluir ou perder seu material de chave, os dados criptografados com uma chave pública fora do AWS KMS serão irrecuperáveis.

Registro em log

Os logs do AWS CloudTrail que gravam todas as operações do AWS KMS, incluindo solicitação, resposta, data, hora e usuário autorizado, não gravam o uso da chave pública fora do AWS KMS.

Verificação offline com pares de chaves SM2 (somente nas regiões da China)

Para verificar uma assinatura fora do AWS KMS com uma chave pública SM2, é necessário especificar o ID distintivo. Por padrão, o AWS KMS usa `1234567812345678` como o ID distintivo. Para obter mais informações, consulte Verificação offline com pares de chaves SM2 (somente nas regiões da China).

Baixar uma chave pública (console)

É possível usar o AWS Management Console para visualizar, copiar e baixar a chave pública de uma chave do KMS assimétrica na sua Conta da AWS. Para baixar a chave pública de uma chave do KMS assimétrica em uma Conta da AWS diferente, use a API do AWS KMS.

1. Faça login no AWS Management Console e abra o console do AWS Key Management Service (AWS KMS) em https://console.aws.amazon.com/kms.
2. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.
3. No painel de navegação, escolha Customer managed keys (Chaves gerenciadas pelo cliente).
4. Escolha o alias ou o ID de chave de uma chave do KMS assimétrica.
5. Selecione a guia Cryptographic configuration (Configuração criptográfica). Registre os valores dos campos Key spec (Especificação da chave), Key usage (Uso da chave) e Encryption algorithms (Algoritmos de criptografia) ou Signing Algorithms (Algoritmos de assinatura). Será necessário usar esses valores para usar a chave pública fora do AWS KMS. Compartilhe essas informações ao compartilhar a chave pública.
6. Selecione a guia Public key (Chave pública).
7. Para copiar a chave pública para a área de transferência, selecione Copy (Copiar). Para fazer download da chave pública em um arquivo, selecione Download (Fazer download).

Baixar uma chave pública (API do AWS KMS)

A GetPublicKeyoperação retorna a chave pública em uma chave KMS assimétrica. Ela também retorna informações críticas que você precisa para usar a chave pública corretamente fora do AWS

KMS, incluindo o uso de chave e os algoritmos de criptografia. Salve esses valores e compartilhe-os sempre que compartilhar a chave pública.

Os exemplos nesta seção usam a AWS Command Line Interface (AWS CLI), mas você pode usar qualquer linguagem de programação compatível.

Para especificar uma chave do KMS, use seu ID de chave, ARN de chave, nome de alias ou ARN de alias. Ao usar um nome de alias, use alias/ como prefixo dele. Para especificar uma chave do KMS em outra Conta da AWS, é necessário usar o ARN da chave ou o ARN do alias.

Antes de executar esse comando, substitua o nome de alias de exemplo por um identificador válido para a chave do KMS. Para executar esse comando, é necessário ter as permissões `kms:GetPublicKey` na chave do 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..."
}
```

Identificar chaves do KMS assimétricas

Para determinar se uma chave do KMS específica é uma chave do KMS assimétrica, localize o tipo de chave ou a especificação da chave. É possível usar o console do AWS KMS ou a API do AWS KMS.

Alguns desses métodos também mostram outros aspectos da configuração criptográfica de uma chave do KMS, incluindo o uso da chave e os algoritmos de criptografia ou assinatura com suporte pela chave do KMS. Você pode visualizar a configuração criptográfica de uma chave do KMS existente, mas não pode alterá-la.

Para obter informações gerais sobre como visualizar chaves do KMS, incluindo classificar, filtrar e escolher colunas para a exibição no console, consulte Visualizar chaves do KMS no console.

Tópicos

- Encontrar o tipo de chave na tabela de chaves do KMS
- Encontrar o tipo de chave na página de detalhes
- Encontrar a especificação da chave usando a API do AWS KMS

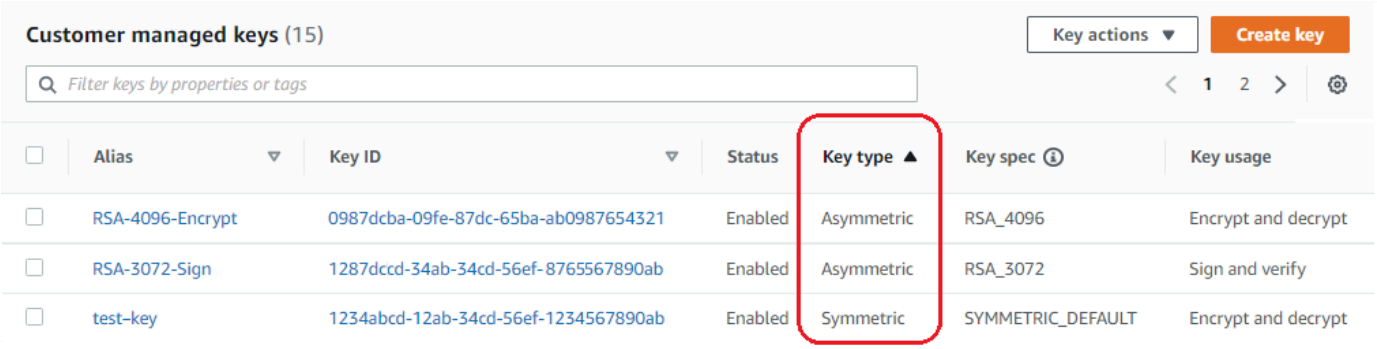
Encontrar o tipo de chave na tabela de chaves do KMS

No console do AWS KMS, a coluna Key type (Tipo de chave) mostra se cada chave do KMS é simétrica ou assimétrica. É possível adicionar uma coluna Key type (Tipo de chave) à tabela de chaves do KMS nas páginas Customer managed keys (Chaves gerenciadas pelo cliente) ou Chaves gerenciadas pela AWS no console.

Para identificar chaves do KMS simétricas e assimétricas na tabela de chaves do KMS, use o procedimento a seguir.

1. Abra o console do AWS KMS em https://console.aws.amazon.com/kms.
2. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.
3. Para exibir as chaves em sua conta que você cria e gerencia, no painel de navegação, escolha Customer managed keys (Chaves gerenciadas de cliente). Para visualizar as chaves na sua conta que a AWS cria e gerencia para você, no painel de navegação, escolha AWS managed keys (Chaves gerenciadas pela AWS).
4. A coluna Key type (Tipo de chave) mostra se cada chave do KMS é simétrica ou assimétrica. Também é possível classificar e filtrar pelo valor de Key type (Tipo de chave).

   Se a coluna Key type (Tipo de chave) não aparecer na tabela de chaves do KMS, selecione o ícone de engrenagem no canto superior direito da página, selecione Key type (Tipo de chave) e Confirm (Confirmar). Também é possível adicionar as colunas Key spec (Especificação da chave) e Key usage (Uso da chave).



Encontrar o tipo de chave na página de detalhes

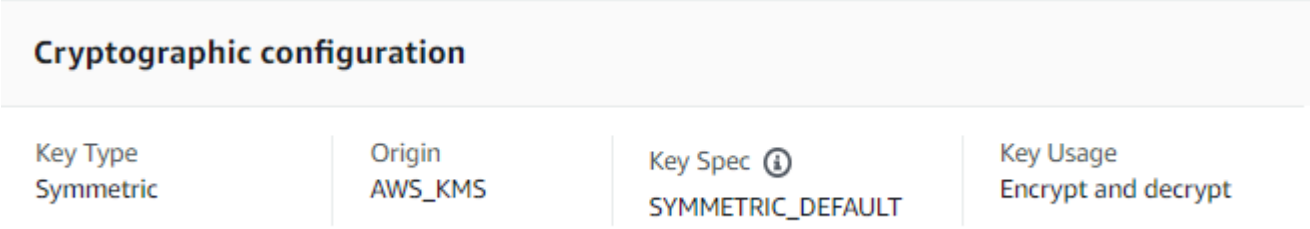
No console do AWS KMS, a página de detalhes de cada chave do KMS inclui uma seção Cryptographic Configuration (Configuração criptográfica) que exibe o tipo de chave (simétrica ou assimétrica) e outros detalhes criptográficos da chave do KMS.

Para identificar chaves do KMS simétricas e assimétricas na página de detalhes de uma chave do KMS, use o procedimento a seguir.

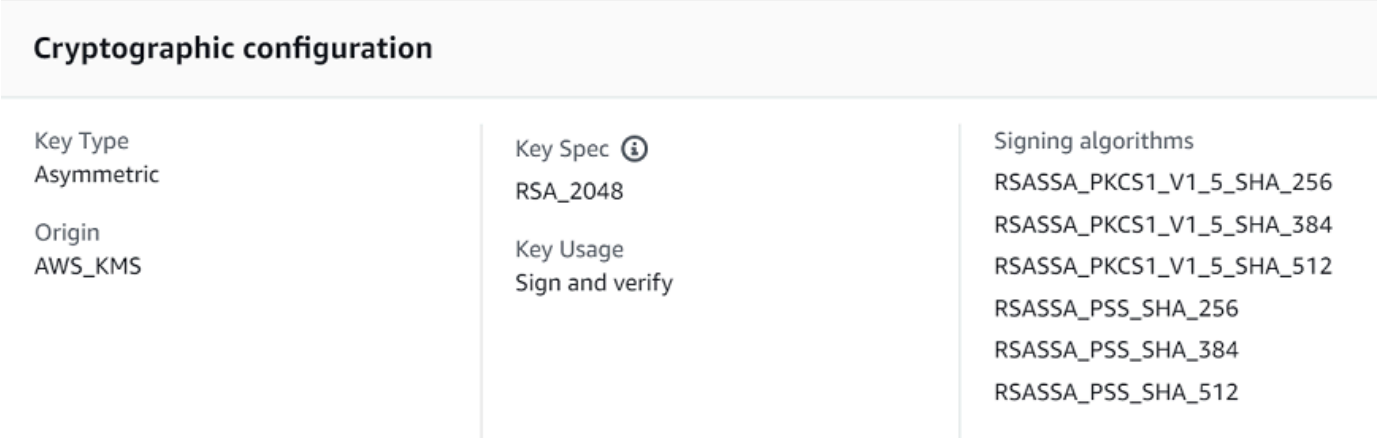
1. Abra o console do AWS KMS em https://console.aws.amazon.com/kms.
2. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.
3. Para exibir as chaves em sua conta que você cria e gerencia, no painel de navegação, escolha Customer managed keys (Chaves gerenciadas de cliente). Para visualizar as chaves na sua conta que a AWS cria e gerencia para você, no painel de navegação, escolha AWS managed keys (Chaves gerenciadas pela AWS).
4. Escolha o alias ou ID de chave de uma chave do KMS.
5. Selecione a guia Cryptographic configuration (Configuração criptográfica). As guias estão abaixo da seção General configuration (Configuração geral).

   A seção Cryptographic Configuration (Configuração criptográfica) inclui o Key Type (Tipo de chave), que indica se ela é simétrica ou assimétrica. Ela também exibe outros detalhes sobre a chave do KMS, incluindo o Key Usage (Uso da chave), que informa se uma chave do KMS pode ser usada para criptografia e descriptografia ou para assinatura e verificação. Para chaves do KMS assimétricas, ela exibe os algoritmos de criptografia ou os algoritmos de assinatura compatíveis com a chave do KMS.

   Por exemplo, veja a seguir um exemplo da guia Cryptographic configuration (Configuração criptográfica) de uma chave do KMS de criptografia simétrica.



   Veja a seguir um exemplo da guia Cryptographic Configuration (Configuração criptográfica) de uma chave do KMS RSA assimétrica que é usada para assinatura e verificação.



Encontrar a especificação da chave usando a API do AWS KMS

Para determinar se uma chave KMS é simétrica ou assimétrica, use a operação. DescribeKey O campo `KeySpec` na resposta contém a especificação da chave da chave do KMS. Para uma chave do KMS de criptografia simétrica, o valor de `KeySpec` é `SYMMETRIC_DEFAULT`. Outros valores indicam uma chave do KMS assimétrica ou uma chave do KMS de HMAC.

> **Note**
>
> O membro `CustomerMasterKeySpec` é defasado. Em seu lugar, use `KeySpec`. Para evitar alterações súbitas, a resposta `DescribeKey` inclui os membros `KeySpec` e `CustomerMasterKeySpec` com o mesmo valor.

Por exemplo, `DescribeKey` retorna a seguinte resposta para uma chave do KMS de criptografia simétrica. O valor de `KeySpec` é `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"
    ]
  }
}
```

A resposta `DescribeKey` para uma chave do KMS RSA assimétrica usada para assinatura e verificação é semelhante a este exemplo. O valor `KeySpec` é`RSA_2048`, e `KeyUsage` é `SIGN_VERIFY`. O elemento `SigningAlgorithms` lista os algoritmos de assinatura válidos para a chave do 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"
    ]
  }
}
```

Especificações de chave assimétrica

Os tópicos a seguir fornecem informações técnicas sobre as especificações de chave com as quais o AWS KMS tem compatibilidade para chaves do KMS assimétricas. As informações sobre a especificação de chave SYMMETRIC_DEFAULT para chaves de criptografia simétrica estão incluídas para comparação.

Tópicos

- Especificações da chave RSA
- Especificações da chave de curva elíptica
- Especificação de chave SM2 (somente nas regiões da China)
- Especificação da chave SYMMETRIC_DEFAULT

Especificações da chave RSA

Quando uma especificação de chave RSA é usada, o AWS KMS cria uma chave do KMS simétrica com um par de chaves RSA. A chave privada nunca deixa o AWS KMS descriptografado. É possível usar a chave pública no AWS KMS ou fazer download da chave pública para usar fora do AWS KMS.

> **Warning**
>
> Ao criptografar dados fora do AWS KMS, certifique-se de que você pode descriptografar o texto cifrado. Se você usar a chave pública de uma chave do KMS que foi excluída do AWS KMS, a chave pública de uma chave do KMS configurada para assinatura e verificação ou um algoritmo de criptografia não compatível com a chave do KMS, os dados se tornarão irrecuperáveis.

No AWS KMS, é possível usar chaves do KMS assimétricas com pares de chaves RSA para criptografia e descriptografia ou para assinatura e verificação, mas não para ambos. Essa propriedade, conhecida como uso de chave, é determinada separadamente da especificação de chave, mas você deve tomar essa decisão antes de escolher uma especificação de chave.

O AWS KMS oferece suporte às seguintes especificações de chave para criptografia e descriptografia ou para assinatura e verificação:

- RSA_2048

- RSA_3072
- RSA_4096

As especificações de chave RSA diferem no tamanho da chave RSA em bits. A especificação da chave RSA escolhida deve ser determinada pelos padrões de segurança ou pelos requisitos da tarefa. Em geral, use a maior chave que seja prática e acessível para sua tarefa. As operações criptográficas em chaves do KMS com diferentes especificações de chave RSA são cobradas de maneira diferente. Para obter informações sobre a definição de preço do AWS KMS, consulte Definição de preço do serviço de gerenciamento de chaves da AWS. Para obter mais informações sobre cotas de solicitações, consulte Cotas de solicitações.

Especificações de chave RSA para criptografia e descriptografia

Quando uma chave do KMS RSA assimétrica é usada para criptografia e descriptografia, você criptografa com a chave pública e descriptografa com a chave privada. Quando a operação `Encrypt` é chamada no AWS KMS para uma chave do KMS RSA, o AWS KMS usa a chave pública no par de chaves RSA e o algoritmo de criptografia especificado para criptografar seus dados. Para descriptografar o texto cifrado, chame a operação `Decrypt` e especifique a mesma chave do KMS e o mesmo algoritmo de criptografia. O AWS KMS usará a chave privada no par de chaves RSA para descriptografar seus dados.

Também é possível fazer download da chave pública e usá-la para criptografar dados fora do AWS KMS. Certifique-se de usar um algoritmo de criptografia compatível com o AWS KMS para chaves do KMS RSA. Para descriptografar o texto cifrado, chame a função `Decrypt` com a mesma chave do KMS e o mesmo algoritmo de criptografia.

O AWS KMS é compatível com dois algoritmos de criptografia para chaves do KMS com especificações de chave RSA. Esses algoritmos, que são definidos no PKCS nº 1 v2.2, diferem na função de hash que usam internamente, No AWS KMS, os algoritmos RSAES_OAEP sempre usam a mesma função de hash para finalidades de hash e para a função de geração de máscara (MGF1). É obrigatório especificar um algoritmo de criptografia ao chamar as operações Encrypt e Decrypt. É possível escolher um algoritmo diferente para cada solicitação.

Algoritmos de criptografia compatíveis com especificações de chave RSA

Algoritmo de criptografia	Descrição do algoritmo
RSAES_OAEP_SHA_1	PKCS nº 1 v2.2, Seção 7.1. Criptografia RSA com padding OAEP usando SHA-1 para a

Algoritmo de criptografia	Descrição do algoritmo
	função de hash e a função de geração de máscara MGF1 com um rótulo vazio.
RSAES_OAEP_SHA_256	PKCS nº 1, Seção 7.1. Criptografia RSA com padding OAEP usando SHA-256 para a função de hash e a função de geração de máscara MGF1 com um rótulo vazio.

Não é possível configurar uma chave do KMS para usar um algoritmo de criptografia específico. No entanto, você pode usar a condição kms: EncryptionAlgorithm policy para especificar os algoritmos de criptografia que os principais podem usar com a chave KMS.

Para obter os algoritmos de criptografia de uma chave KMS, visualize a configuração criptográfica da chave KMS no AWS KMS console ou use a operação. DescribeKey AWS KMStambém fornece a especificação da chave e os algoritmos de criptografia quando você baixa sua chave pública, seja no AWS KMS console ou usando a GetPublicKeyoperação.

Você pode escolher uma especificação de chave RSA com base no tamanho dos dados do texto não criptografado que pode ser criptografado em cada solicitação. A tabela a seguir mostra o tamanho máximo, em bytes, do texto não criptografado que pode ser criptografado em uma única chamada para a operação Encrypt. Os valores diferem de acordo com a especificação de chave e com o algoritmo de criptografia. Para fins comparativos, é possível usar uma chave do KMS de criptografia simétrica para criptografar até 4.096 bytes de uma vez.

Para calcular o tamanho máximo do texto não criptografado em bytes para esses algoritmos, use a seguinte fórmula: (*tamanho_da_chave_em_bits*/8) - (2 * *tamanho_de_hash_em_bits*/8) - 2. Por exemplo, para RSA_2048 com SHA-256, o tamanho máximo de texto não criptografado em bytes é de (2048/8) - (2 * 256/8) -2 = 190.

Tamanho máximo de texto não criptografado (em bytes) em uma operação Encrypt

	Algoritmo de criptografia	
Especificação da chave	RSAES_OAEP_SHA_1	RSAES_OAEP_SHA_256
RSA_2048	214	190

	Algoritmo de criptografia	
Especificação da chave	RSAES_OAEP_SHA_1	RSAES_OAEP_SHA_256
RSA_3072	342	318
RSA_4096	470	446

Especificações de chave RSA para assinatura e verificação

Quando uma chave do KMS RSA assimétrica é usada para assinatura e verificação, você gera a assinatura para uma mensagem com uma chave privada e verifica a assinatura com a chave pública.

Quando você chama a operação `Sign` no AWS KMS para uma chave do KMS assimétrica, o AWS KMS usa a chave privada no par de chaves RSA, a mensagem e o algoritmo de assinatura especificado para gerar uma assinatura. Para verificar a assinatura, chame a operação Verify. Especifique a assinatura, a mesma chave do KMS, a mesma mensagem e o mesmo algoritmo de assinatura. O AWS KMS usará a chave pública no par de chaves RSA para verificar a assinatura. Também é possível fazer download da chave pública e usá-la para verificar a assinatura fora do AWS KMS.

O AWS KMS oferece suporte aos algoritmos de assinatura a seguir para todas as chaves do KMS com uma especificação de chave RSA. É obrigatório especificar um algoritmo de assinatura ao chamar as operações Sign e Verify. É possível escolher um algoritmo diferente para cada solicitação. Ao assinar com pares de chaves RSA, os algoritmos RSASSA-PSS são preferidos. Incluímos algoritmos RSASSA-PKCS1-v1_5 para compatibilidade com aplicações existentes.

Algoritmos de assinatura compatíveis com especificações de chave RSA

Algoritmo de assinatura	Descrição do algoritmo
RSASSA_PSS_SHA_256	PKCS nº 1 v2.2, Seção 8.1, assinatura RSA com padding PSS usando SHA-256 para a função de resumo de mensagens e para a função de geração de máscara MGF1 com um sal de 256 bits.
RSASSA_PSS_SHA_384	PKCS nº 1 v2.2, Seção 8.1, assinatura RSA com padding PSS usando SHA-384 para o a

Algoritmo de assinatura	Descrição do algoritmo
	função de resumo de mensagens e a função de geração de máscara MGF1 com um sal de 384 bits
RSASSA_PSS_SHA_512	PKCS nº 1 v2.2, Seção 8.1, assinatura RSA com padding PSS usando SHA-512 para a função de resumo de mensagens e a função de geração de máscara MGF1 com um sal de 512 bits
RSASSA_PKCS1_V1_5_SHA_256	PKCS nº 1 v2.2, Seção 8.2, assinatura RSA com PKCS nº 1 v1.5 padding e SHA-256
RSASSA_PKCS1_V1_5_SHA_384	PKCS nº 1 v2.2, Seção 8.2, assinatura RSA com PKCS nº 1 v1.5 padding e SHA-384
RSASSA_PKCS1_V1_5_SHA_512	PKCS nº 1 v2.2, Seção 8.2, assinatura RSA com PKCS nº 1 v1.5 padding e SHA-512

Não é possível configurar uma chave do KMS para usar algoritmos de assinatura específicos. No entanto, você pode usar a condição kms: SigningAlgorithm policy para especificar os algoritmos de assinatura que os diretores podem usar com a chave KMS.

Para obter os algoritmos de assinatura de uma chave KMS, visualize a configuração criptográfica da chave KMS no AWS KMS console ou usando a operação. DescribeKey AWS KMStambém fornece a especificação da chave e os algoritmos de assinatura quando você baixa sua chave pública, seja no AWS KMS console ou usando a GetPublicKeyoperação.

Especificações da chave de curva elíptica

Quando uma especificação de chave de curva elíptica (ECC) é usada, o AWS KMS cria uma chave do KMS assimétrica com um par de chaves de ECC para assinatura e verificação. A chave privada que gera a assinatura nunca deixa o AWS KMS descriptografada. É possível usar a chave pública para verificar assinaturas no AWS KMS ou fazer download da chave pública para usar fora do AWS KMS.

O AWS KMS é compatível com especificações de chave de ECC a seguir para chaves do KMS assimétricas.

- Pares de chaves de curva elíptica assimétricas recomendadas pelo NIST (assinatura e verificação)
  - ECC_NIST_P256 (secp256r1)
  - ECC_NIST_P384 (secp384r1)
  - ECC_NIST_P521 (secp521r1)
- Outros pares de chaves de curva elíptica assimétricas (assinatura e verificação)
  - ECC_SECG_P256K1 (secp256k1), normalmente usada para criptomoedas.

A especificação da chave ECC escolhida deve ser determinada pelos padrões de segurança ou pelos requisitos da tarefa. Em geral, use a curva com mais pontos que seja prática e acessível para sua tarefa.

Se você estiver criando uma chave do KMS assimétrica para usar com criptomoedas, use a especificação de chave ECC_SECG_P256K1. Também é possível usar essa especificação de chave para outros fins, mas ela é exigida para Bitcoin e para outras criptomoedas.

As chaves do KMS com especificações de chave de ECC diferentes são cobradas de maneira diferente e estão sujeitas a diferentes cotas de solicitações. Para obter mais informações sobre a definição de preço do AWS KMS, consulte Definição de preço do AWS Key Management Service. Para obter mais informações sobre cotas de solicitações, consulte Cotas de solicitações.

A tabela a seguir mostra os algoritmos de assinatura compatíveis com o AWS KMS para cada especificação de chave ECC. Não é possível configurar uma chave do KMS para usar algoritmos de assinatura específicos. No entanto, você pode usar a condição kms: SigningAlgorithm policy para especificar os algoritmos de assinatura que os diretores podem usar com a chave KMS.

Algoritmos de assinatura compatíveis para especificações de chave ECC

Especificação da chave	Algoritmo de assinatura	Descrição do algoritmo
ECC_NIST_P256	ECDSA_SHA_256	NIST FIPS 186-4, Seção 6.4, assinatura ECDSA usando a curva especificada pela chave e SHA-256 para o resumo de mensagens.

Especificação da chave	Algoritmo de assinatura	Descrição do algoritmo
ECC_NIST_P384	ECDSA_SHA_384	NIST FIPS 186-4, Seção 6.4, assinatura ECDSA usando a curva especificada pela chave e SHA-384 para o resumo de mensagens.
ECC_NIST_P521	ECDSA_SHA_512	NIST FIPS 186-4, Seção 6.4, assinatura ECDSA usando a curva especificada pela chave e SHA-512 para o resumo de mensagens.
ECC_SECG_P256K1	ECDSA_SHA_256	NIST FIPS 186-4, Seção 6.4, assinatura ECDSA usando a curva especificada pela chave e SHA-256 para o resumo de mensagens.

Especificação de chave SM2 (somente nas regiões da China)

A especificação de chave SM2 é uma especificação chave de curva elíptica definida dentro da série de especificações GM/T publicada pelo Office of State Commercial Cryptography Administration (OSCCA) da China. A especificação de chave SM2 está disponível somente nas regiões da China. Quando uma especificação de chave SM2 é usada, o AWS KMS cria uma chave do KMS simétrica com um par de chaves SM2. É possível usar esse par chaves SM2 no AWS KMS ou baixar a chave pública para usar fora do AWS KMS.

Ao contrário da especificação de chave ECC, chave do KMS SM2 pode ser usada para assinatura e verificação ou para criptografia e descriptografia. Você deve especificar o uso da chave ao criar a chave do KMS, e não será possível alterá-lo após a criação da chave.

O AWS KMS é compatível com os seguintes algoritmos de criptografia e assinatura SM2:

- Algoritmo de criptografia SM2PKE

  O SM2PKE é um algoritmo de criptografia baseado em curva elíptica definido pelo OSCCA no GM/T 0003.4-2012.

- Algoritmo de criptografia SM2DSA

  O SM2DSA é um algoritmo de assinatura baseado em curva elíptica definido pelo OSCCA em GM/T 0003.2-2012. O SM2DSA requer um ID distinto criptografado em hash com o algoritmo de hash SM3 e, em seguida, é combinado com a mensagem, ou o resumo da mensagem, que você transmitiu para o AWS KMS. Esse valor concatenado é então criptografado em hash e assinado pelo AWS KMS.

Operações offline com SM2 (somente nas regiões da China)

Você pode baixar a chave pública do seu par de chaves SM2 para uso em operações offline, ou seja, operações fora do AWS KMS. Porém, ao usar sua chave pública SM2 offline, talvez seja necessário fazer conversões e cálculos extras manualmente. Operações SM2DSA podem exigir que você forneça um ID distintivo ou calcule um resumo de mensagem. Operações de criptografia SM2PKE podem exigir que você converta a saída de texto cifrado bruto em um formato aceitável pelo AWS KMS.

Para ajudar com essas operações, a classe `SM2OfflineOperationHelper` para Java tem métodos que realizam as tarefas para você. Essa classe auxiliar pode ser usada como modelo para outros provedores criptográficos.

> **Important**
>
> O código de referência `SM2OfflineOperationHelper` foi projetado para ser compatível com o Bouncy Castle versão 1.68. Para obter ajuda com outras versões, entre em contato com bouncycastle.org.

Verificação offline com pares de chaves SM2 (somente nas regiões da China)

Para verificar uma assinatura fora do AWS KMS com uma chave pública SM2, é necessário especificar o ID distintivo. Quando você transmite uma mensagem bruta, `MessageType:RAW`, para a API Sign, o AWS KMS usa o ID distintivo padrão, `1234567812345678`, definido pelo OSCCA em GM/T 0009-2012. Você não pode especificar seu próprio ID de distinção no AWS KMS.

Porém, se estiver gerando um resumo de mensagens fora do AWS, você poderá especificar seu próprio ID distintivo e, em seguida, transmitir o resumo de mensagem, `MessageType:DIGEST`, para o AWS KMS assinar. Para isso, altere o valor de `DEFAULT_DISTINGUISHING_ID` na classe `SM2OfflineOperationHelper`. O ID distintivo especificado pode ser qualquer string de até 8.192 caracteres. Depois que o AWS KMS assinar o resumo de mensagem, você precisará desse resumo de mensagem ou da mensagem e do ID distintivo utilizados no cálculo do resumo para verificá-lo offline.

Classe **`SM2OfflineOperationHelper`**

No AWS KMS, as conversões de texto cifrado bruto e os cálculos de resumos de mensagem SM2DSA ocorrem automaticamente. Nem todos os provedores criptográficos implementam o SM2 da mesma maneira. Algumas bibliotecas, como a OpenSSL versões 1.1.1 e posteriores, realizam essas ações automaticamente. O AWS KMS confirma esse comportamento em testes com a OpenSSL versão 3.0. Use a seguinte classe `SM2OfflineOperationHelper` com bibliotecas, como a Bouncy Castle, que exigem que você faça essas conversões e cálculos manualmente.

A classe `SM2OfflineOperationHelper` fornece métodos para as seguintes operações:

- Cálculo de resumo de mensagem

  Para gerar um resumo de mensagem offline para uso em uma verificação offline ou para transmissão ao AWS KMS para assinatura, use o método `calculateSM2Digest`. O método `calculateSM2Digest` gera um resumo de mensagem com o algoritmo de hash SM3. A GetPublicKeyAPI retorna sua chave pública em formato binário. Você deve analisar a chave binária em um Java PublicKey. Forneça a chave pública analisada com a mensagem. O método combina automaticamente sua mensagem com o ID distintivo padrão, `1234567812345678`, mas você pode definir seu próprio ID distintivo alterando o valor de `DEFAULT_DISTINGUISHING_ID`.

- Verificar

  Para verificar uma assinatura offline, use o método `offlineSM2DSAVerify`. O método `offlineSM2DSAVerify` usa o resumo de mensagem calculado com base no ID distintivo especificado e a mensagem original fornecida para verificar a assinatura digital. A GetPublicKeyAPI retorna sua chave pública em formato binário. Você deve analisar a chave binária em um Java PublicKey. Forneça a chave pública analisada com a mensagem original e a assinatura que você deseja verificar. Para obter mais detalhes, consulte Verificação offline com pares de chaves SM2.

- Encrypt

  Para criptografar texto sem formatação offline, use o método `offlineSM2PKEEncrypt`. Ele garante que o texto cifrado esteja em um formato que o AWS KMS possa descriptografar. O método `offlineSM2PKEEncrypt` criptografa o texto simples e depois converte o texto cifrado bruto produzido por SM2PKE no formato ASN.1. A GetPublicKeyAPI retorna sua chave pública em formato binário. Você deve analisar a chave binária em um Java PublicKey. Forneça a chave pública analisada com o texto simples que você deseja criptografar.

  Se não tiver certeza de que a conversão é necessário, use a seguinte operação OpenSSL para testar o formato do texto cifrado. Se a operação falhar, significa que você precisa converter o texto cifrado no formato ASN.1.

  ```
  openssl asn1parse -inform DER -in ciphertext.der
  ```

Por padrão, a classe `SM2OfflineOperationHelper` usa o ID distintivo padrão, `1234567812345678`, ao gerar resumos de mensagens para operações 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");
    }
}
```

Especificação da chave SYMMETRIC_DEFAULT

A especificação de chave padrão, SYMMETRIC_DEFAULT, é a especificação de chave para chaves do KMS de criptografia simétrica. Ao selecionar o tipo de chave Symmetric (Simétrica) e o uso de chave Encrypt and decrypt (Criptografar e descriptografar) no console do AWS KMS, ele seleciona a especificação de chave `SYMMETRIC_DEFAULT`. Na CreateKeyoperação, se você não especificar um `KeySpec` valor, SYMMETRIC_DEFAULT será selecionado. Se você não tiver um motivo para usar uma especificação de chave diferente, SYMMETRIC_DEFAULT é uma boa escolha.

SYMMETRIC_DEFAULT atualmente representa AES-256-GCM, um algoritmo simétrico baseado no on Advanced Encryption Standard (AES) em Galois Counter Mode (GCM) com chaves de 256 bits, um padrão do setor para criptografia segura. O texto cifrado que esse algoritmo gera oferece suporte a dados adicionais autenticados (ADD), como um contexto de criptografia e o GCM fornece uma verificação de integridade adicional no texto cifrado. Para obter mais detalhes técnicos, consulte Detalhes criptográficos para AWS Key Management Service.

Os dados criptografados em AES-256-GCM está protegido agora e futuramente. Os criptógrafos consideram esse algoritmo como resistente a quânticos. Num futuro teórico, ataques de computação

quântica em grande escala em textos cifrados criados sob chaves AES-GCM de 256 bits reduzem a segurança efetiva da chave para 128 bits. No entanto, esse nível de segurança é suficiente para tornar inviáveis ataques de força bruta contra textos cifrados do AWS KMS.

A única exceção é aplicável às regiões da China, em que SYMMETRIC_DEFAULT representa uma chave simétrica de 128 bits que usa a criptografia SM4. Apenas é possível criar uma chave SM4 de 128 bits nas regiões da China. Uma chave do KMS AES-GCM de 256 bits não pode ser criada nas regiões da China.

É possível usar uma chave do KMS de criptografia simétrica no AWS KMS para criptografar, descriptografar e recriptografar dados, bem como para proteger as chaves de dados geradas e os pares de chaves de dados. Os serviços da AWS integrados ao AWS KMS usam chaves do KMS de criptografia simétrica para criptografar seus dados em repouso. Você pode importar seu próprio material de chave para uma chave do KMS de criptografia simétrica e criar chaves do KMS de criptografia simétrica em armazenamentos personalizados de chaves. Para acessar uma tabela comparando as operações que podem ser executadas em chaves do KMS simétricas e assimétricas, consulte Comparar chaves do KMS simétricas e assimétricas.

Para obter detalhes técnicos sobre o AWS KMS e chaves de criptografia simétrica, consulte Detalhes criptográficos do AWS Key Management Service.

Chaves de HMAC no AWS KMS

As chaves do KMS de código de autenticação de mensagem por hash (HMAC) são chaves simétricas que você usa para gerar e verificar HMACs no AWS KMS. O material exclusivo de chave associado a cada chave do KMS de HMAC fornece a chave secreta exigida pelos algoritmos de HMAC. Você pode usar uma chave do KMS de HMAC com as operações `GenerateMac` e `VerifyMac` para verificar a integridade e a autenticidade dos dados no AWS KMS.

Os algoritmos de HMAC combinam uma função de hash criptográfica e uma chave secreta compartilhada. Eles pegam uma mensagem e uma chave secreta, como o material da chave em uma chave do KMS de HMAC, e retornam um código ou etiqueta exclusiva e de tamanho fixo. Se até mesmo um caractere da mensagem mudar, ou se a chave secreta não for idêntica, a etiqueta resultante será totalmente diferente. Ao exigir uma chave secreta, o HMAC também fornece autenticidade; é impossível gerar uma etiqueta idêntica de HMAC sem a chave secreta. Algumas vezes, os HMACs são chamados de assinaturas simétricas, pois eles funcionam como assinaturas digitais, mas usam somente uma chave para assinatura e verificação.

As chaves do KMS de HMAC e os algoritmos de HMAC que o AWS KMS usa estão em conformidade com os padrões do setor definidos no RFC 2104. A AWS KMS GenerateMacoperação gera tags HMAC padrão. As chaves do KMS de HMAC são geradas em módulos de segurança de hardware do AWS KMS certificados sob o Programa de validação de módulos criptográficos FIPS 140-2 (exceto nas regiões China [Pequim] e China [Ningxia]) e nunca saem descriptografadas do AWS KMS. Para usar uma chave do KMS de HMAC, é necessário chamar o AWS KMS.

Você pode usar chaves do KMS de HMAC para determinar a autenticidade de uma mensagem, como um JSON Web Token (JWT), informações tokenizadas de cartão de crédito ou uma senha enviada. Eles também podem ser usados como Key Derivation Functions (KDFs – Funções de derivação de chave) seguras, especialmente em aplicações que exigem chaves determinísticas.

As chaves do KMS de HMAC fornecem uma vantagem sobre os HMACs de software de aplicação, pois o material da chave é inteiramente gerado e usado no AWS KMS, estando sujeito aos controles de acesso que você definiu na chave.

> **Tip**
>
> As práticas recomendadas sugerem que você limite o tempo durante o qual qualquer mecanismo de assinatura, inclusive um HMAC, permanece vigente. Isso dissuade um ataque no qual o protagonista usa uma mensagem assinada para estabelecer a validade repetidamente ou muito depois que a mensagem é substituída. As etiquetas de HMAC não incluem um carimbo de data/hora, mas você pode incluir um carimbo de data/hora no token ou na mensagem para ajudar você a detectar quando está na hora de atualizar o HMAC.

Os usuários autorizados podem criar, gerenciar e usar as chaves do KMS de HMAC em sua conta da AWS. Isso inclui ativação e desativação de chaves, configuração e alteração de aliases e etiquetas, além da programação de exclusão de chaves do KMS de HMAC. Você também pode controlar o acesso a chaves do KMS de HMAC usando políticas de chave, políticas do IAM e concessões. Você pode auditar todas as operações que usam ou gerenciam chaves do KMS de HMAC na AWS em logs do AWS CloudTrail. É possível criar chaves do HMAC KMS com material de chave importado. Você também pode criar chaves do KMS de várias regiões para HMAC que se comportam como cópias da mesma chave do KMS de HMAC em várias Regiões da AWS.

As chaves do KMS de HMAC só são compatíveis com as operações criptográficas `GenerateMac` e `VerifyMac`. Você não pode usar chaves do KMS de HMAC para criptografar dados ou assinar mensagens, nem usar nenhum outro tipo de chave do KMS em operações de HMAC. Ao usar a

operação `GenerateMac`, você fornece uma mensagem de até 4.096 bytes, uma chave do KMS de HMAC e o algoritmo de Message authentication code (MAC – Código de autenticação de mensagem) compatível com a especificação de chave de HMAC, e `GenerateMac` calcula a etiqueta de HMAC. Para verificar uma etiqueta de HMAC, você deve fornecer a etiqueta de HMAC e a mesma mensagem, a chave do KMS de HMAC e o algoritmo de MAC que `GenerateMac` usou para calcular a etiqueta original de HMAC. A operação `VerifyMac` calcula a etiqueta de HMAC e verifica se ela é idêntica à etiqueta de HMAC fornecida. Se as etiquetas de HMAC recebidas e calculadas não forem idênticas, a verificação falhará.

As chaves do KMS de HMAC não são compatíveis com alternância automática de chaves e não é possível criar uma chave do KMS de HMAC em um armazenamento personalizado de chaves.

Se você estiver criando uma chave do KMS para criptografar dados em um serviço da AWS, use uma chave de criptografia simétrica. Não é possível usar uma chave do KMS de HMAC.

Regiões

AS chaves do KMS de HMAC têm suporte em todas as Regiões da AWS compatíveis com o AWS KMS.

Saiba mais

- Para obter ajuda na escolha de um tipo de chave do KMS, consulte Escolha de um tipo de chave do KMS.
- Para acessar uma tabela que compara as operações de API do AWS KMS compatíveis com cada tipo de chave do KMS, consulte Referência de tipos de chaves.
- Para obter informações sobre como criar chaves do KMS de HMAC de várias regiões, consulte Chaves multirregionais em AWS KMS.
- Para examinar a diferença na política de chaves padrão que o console do AWS KMS define para chaves do KMS de HMAC, consulte the section called “Permite que os usuários de chaves usem a chave do KMS com serviços da AWS”.
- Para obter mais informações sobre os preços das chaves do KMS de HMAC, consulte Preços do AWS Key Management Service.
- Para obter informações sobre as cotas aplicáveis a chaves do KMS de HMAC, consulte Cotas de recurso e Cotas de solicitações.
- Para obter informações sobre como excluir chaves do KMS de HMAC, consulte Excluir AWS KMS keys.

- Para saber mais sobre o uso de HMACs para criar tokens de Web JSON, consulte How to protect HMACs inside AWS KMS no blog de Segurança da AWS.
- Ouça um podcast: Introducing HMACs for AWS Key Management Service no Podcast oficial da AWS.

Tópicos

- Especificações de chave para chaves do KMS de HMAC
- Criar chaves do KMS de HMAC
- Controlar o acesso a chaves do KMS de HMAC
- Visualizar chaves do KMS de HMAC

Especificações de chave para chaves do KMS de HMAC

O AWS KMS é compatível com chaves de HMAC simétricas de comprimentos variados. A especificação de chave que você escolhe depende de seus requisitos regulatórios, de segurança ou de negócios. O comprimento da chave determina o algoritmo MAC usado nas GenerateMacVerifyMacoperações. Em geral, chaves mais longas são mais seguras. Use a chave mais longa que seja viável para o seu caso de uso.

Especificação de chave de HMAC	Algoritmo de MAC
HMAC_224	HMAC_SHA_224
HMAC_256	HMAC_SHA_256
HMAC_384	HMAC_SHA_384
HMAC_512	HMAC_SHA_512

Criar chaves do KMS de HMAC

Você pode criar chaves do KMS de Hash-based message authentication code (HMAC – Código de autenticação de mensagem por hash) no console do AWS KMS, usando a API CreateKey ou usando um modelo do AWS CloudFormation.

O AWS KMS é compatível com várias especificações de chave para chaves do KMS de HMAC. A especificação de chave que você escolhe pode ser determinada por requisitos regulatórios, de segurança ou de negócios. Em geral, chaves maiores são mais resistentes a ataques de força bruta.

> **Important**
>
> Não inclua informações confidenciais ou sigilosas no alias, na descrição ou nas tags. Esses campos podem aparecer em texto simples em CloudTrail registros e outras saídas.

Se estiver criando uma chave do KMS para criptografar dados em um serviço da AWS, use uma chave do KMS de criptografia simétrica. Os serviços da AWS que têm integração com o AWS KMS não são compatíveis com chaves do KMS assimétricas ou chaves do KMS de HMAC. Para obter ajuda na criação de uma chave do KMS de criptografia simétrica, consulte Criar chaves.

Saiba mais

- Para determinar qual tipo de chave do KMS criar, consulte Escolha de um tipo de chave do KMS.
- É possível seguir os procedimentos descritos neste tópico para criar uma chave primária do KMS de HMAC de várias regiões. Para replicar uma chave de HMAC de várias regiões, consulte the section called “Criar chaves de réplica”.
- Para obter informações sobre as permissões necessárias para criar chaves do KMS, consulte Permissões para criar chaves do KMS.
- Para obter informações sobre como usar um AWS CloudFormation modelo para criar uma chave HMAC KMS, consulte o AWS::KMS::KeyGuia do AWS CloudFormationusuário.

Tópicos

- Criar chaves do KMS de HMAC (console)
- Criar chaves do KMS de HMAC (API do AWS KMS)

Criar chaves do KMS de HMAC (console)

Você pode usar o AWS Management Console para criar chaves do KMS de HMAC. As chaves do KMS de HMAC são chaves simétricas com um uso de chave para gerar e verificar Message authentication code (MAC – Código de autenticação de mensagem). Você também pode criar chaves de HMAC de várias regiões.

1. Faça login no AWS Management Console e abra o console do AWS Key Management Service (AWS KMS) em https://console.aws.amazon.com/kms.
2. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.
3. No painel de navegação, escolha Customer managed keys (Chaves gerenciadas pelo cliente).
4. Escolha Create key (Criar chave).
5. Para Key type (Tipo de chave), escolha Symmetric (Simétrica).

   As chaves do KMS de HMAC são simétricas. Você usa a mesma chave para gerar e verificar etiquetas de HMAC.
6. Em Key usage (Uso de chave), escolha Generate and verify MAC (Gerar e verificar MAC).

   Gerar e verificar MAC é o único uso de chave válido para chaves do KMS de HMAC.

   > **Note**
   >
   > Key usage (Uso de chave) é exibido para chaves simétricas somente quando as chaves do KMS de HMAC são compatíveis com a região selecionada.
7. Escolha uma especificação (Key spec [Especificação de chave]) para sua chave do KMS de HMAC.

   A especificação de chave que você escolhe pode ser determinada por requisitos regulatórios, de segurança ou de negócios. Em geral, chaves mais longas são mais seguras.
8. Para criar uma chave de HMAC primária de várias regiões, em Advanced options (Opções avançadas), escolha Multi-Region key (Chave de várias regiões). As propriedades compartilhadas que você define para essa chave do KMS, como o tipo de chave e o uso de chave, serão compartilhados com suas réplicas de chave. Para obter detalhes, consulte Criar chaves de várias regiões.

   Não é possível aplicar esse procedimento para criar uma réplica de chave. Para criar uma réplica de chave de HMAC de várias regiões, siga as instruções para criar uma réplica de chave.
9. Escolha Próximo.
10. Insira um alias para a chave do KMS. O nome do alias não pode começar com **`aws/`**. O prefixo **`aws/`** é reservado pela Amazon Web Services para representar as Chaves gerenciadas pela AWS na sua conta.

Recomendamos que você use um alias que identifique a chave do KMS como uma chave de HMAC, p. ex., `HMAC/test-key`. Isso facilitará a identificação de suas chaves de HMAC no console do AWS KMS, onde você pode classificar e filtrar chaves por etiquetas e aliases, mas não por especificação de chave ou uso de chave.

Aliases são necessários ao criar uma chave do KMS no AWS Management Console. Você não pode especificar um alias ao usar a CreateKeyoperação, mas pode usar o console ou a CreateAliasoperação para criar um alias para uma chave KMS existente. Para obter detalhes, consulte Usar aliases.

11. (Opcional) Insira uma descrição para a chave do KMS.

    Insira uma descrição que explique o tipo de dados que você planeja proteger ou a aplicação que planeja usar com a chave do KMS.

    Você pode adicionar uma descrição agora ou atualizá-la a qualquer momento, a não ser que o estado da chave seja `Pending Deletion` ou `Pending Replica Deletion`. Para adicionar, alterar ou excluir a descrição de uma chave gerenciada pelo cliente existente, edite a descrição na operação AWS Management Console ou use a UpdateKeyDescriptionoperação.

12. (Opcional) Insira uma chave de etiqueta e um valor opcional de etiqueta. Para adicionar mais de uma etiqueta à chave do KMS, selecione Add tag (Adicionar etiqueta).

    Considere a possibilidade de adicionar uma etiqueta que identifique a chave como uma chave de HMAC, p. ex., `Type=HMAC`. Isso facilitará a identificação de suas chaves de HMAC no console do AWS KMS, onde você pode classificar e filtrar chaves por etiquetas e aliases, mas não por especificação de chave ou uso de chave.

    Ao adicionar tags aos recursos da AWS, a AWS gera um relatório de alocação de custos com utilização e custos agrupados por tags. Etiquetas também podem ser utilizadas para controlar o acesso a uma chave do KMS. Para informações sobre marcação de chaves do KMS, consulte Marcar chaves com tags e ABAC para AWS KMS.

13. Escolha Próximo.

14. Selecione os usuários e as funções do IAM que podem administrar a chave do KMS.

> **Note**
>
> Esta política de chave concede controle total dessa chave do KMS à Conta da AWS. Ela permite que os administradores de conta usem políticas do IAM para conceder a outras

entidades principais a permissão para gerenciar a chave do KMS. Para obter detalhes, consulte the section called “Política de chaves padrão”.
As práticas recomendadas do IAM não encorajam o uso de usuários do IAM com credenciais de longo prazo. Sempre que possível, use os perfis do IAM, por fornecerem credenciais temporárias. Para obter detalhes, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

15. (Opcional) Para evitar que os usuários e funções do IAM selecionados excluam essa chave do KMS, na seção Key deletion (Exclusão de chaves) na parte inferior da página, desmarque a caixa de seleção Allow key administrators to delete this key (Permitir que os administradores de chaves excluam essa chave).
16. Escolha Próximo.
17. Selecione os usuários e as funções do IAM que podem usar a chave do KMS para operações de criptografia.

> **Note**
>
> Esta política de chave concede controle total dessa chave do KMS à Conta da AWS. Ela permite que os administradores de conta usem políticas do IAM para conceder a outras entidades principais a permissão para usar a chave do KMS em operações de criptografia. Para obter detalhes, consulte the section called “Política de chaves padrão”.
> As práticas recomendadas do IAM não encorajam o uso de usuários do IAM com credenciais de longo prazo. Sempre que possível, use os perfis do IAM, por fornecerem credenciais temporárias. Para obter detalhes, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

18. (Opcional) Você pode permitir que outras Contas da AWS usem essa chave do KMS para operações de criptografia. Para fazer isso, na parte inferior da página na seção Other Contas da AWS (Outras), escolha Add another Conta da AWS (Adicionar outra) e insira o número de identificação da Conta da AWS de uma conta externa. Para adicionar várias contas externas, repita essa etapa.

> **Note**
>
> Para permitir que as entidades principais de contas externas usem a chave do KMS, os administradores da conta externa devem criar políticas do IAM que forneçam essas

permissões. Para ter mais informações, consulte Permitir que usuários de outras contas usem uma chave do KMS.

19. Escolha Próximo.
20. Revise as configurações que você escolheu. Ainda é possível voltar e alterar todas as configurações.
21. Escolha Finish (Concluir) para criar a chave do KMS de HMAC.

Criar chaves do KMS de HMAC (API do AWS KMS)

Você pode usar a CreateKeyoperação para criar uma chave HMAC KMS. Estes exemplos usam a AWS Command Line Interface (AWS CLI), mas você pode usar qualquer linguagem de programação compatível.

Ao criar uma chave do KMS de HMAC, você deve especificar o parâmetro `KeySpec`, que determina o tipo de chave do KMS. Além disso, você deve especificar um valor de GENERATE_VERIFY_MAC para `KeyUsage`, mesmo que seja o único valor válido de uso de chave para chaves de HMAC. Para criar uma chave do KMS de HMAC de várias regiões, adicione o parâmetro `MultiRegion` com um valor de `true`. Não é possível alterar essas propriedades depois que a chave do KMS é criada.

A `CreateKey` operação não permite que você especifique um alias, mas você pode usar a CreateAliasoperação para criar um alias para sua nova chave KMS. Recomendamos que você use um alias que identifique a chave do KMS como uma chave de HMAC, p. ex., `HMAC/test-key`. Isso facilitará a identificação de suas chaves de HMAC no console do AWS KMS, onde você pode classificar e filtrar chaves por alias, mas não por especificação de chave ou uso de chave.

Se você tentar criar uma chave do KMS de HMAC em uma Região da AWS incompatível com as chaves de HMAC, a operação `CreateKey` retorna `UnsupportedOperationException`

O exemplo a seguir usa a operação `CreateKey` para criar uma chave do KMS de HMAC de 512 bits.

```
$ 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
    }
}
```

Controlar o acesso a chaves do KMS de HMAC

Para controlar o acesso a uma chave do KMS de Hash-based message authentication code (HMAC – Código de autenticação de mensagem por hash), você usa uma política de chaves, que é necessária para cada chave do KMS. Você também pode usar políticas do IAM e concessões.

A política padrão de chaves para chaves de HMAC criadas no console do AWS KMS permite que os usuários de chave chamem as operações `GenerateMac` e `VerifyMac`. No entanto, isso não inclui a instrução de política de chaves desenvolvida para usar concessões com serviços da AWS. Se criar chaves de HMAC usando a operação `CreateKey`, você deverá especificar essas permissões na política de chaves ou em uma política do IAM.

Você pode usar as chaves de condição global da AWS e as chaves de condição do AWS KMS a fim de refinar e limitar permissões para chaves de HMAC. Por exemplo, você pode usar a chave de condição `kms:ResourceAliases` para controlar o acesso a operações do AWS KMS baseadas nos aliases associados a uma chave de HMAC. Os seguintes exemplos de condições de política do AWS KMS são úteis para políticas em chaves de HMAC.

- Use uma chave de condição `kms:MacAlgorithm` para limitar os algoritmos que as entidades principais podem solicitar quando chamarem as operações `GenerateMac` e `VerifyMac`. Por exemplo, você pode permitir que as entidades principais chamem as operações `GenerateMac`, mas somente quando o algoritmo de Message authentication code (MAC – Código de autenticação de mensagem) na solicitação for `HMAC_SHA_384`.

- Use uma chave de condição `kms:KeySpec` para permitir ou impedir que entidades principais criem certos tipos de chaves de HMAC. Por exemplo, para permitir que os diretores criem somente chaves HMAC, você pode permitir a CreateKeyoperação, mas usar a `kms:KeySpec` condição para permitir somente chaves com uma especificação de `HMAC_384` chave.

  Também é possível usar a chave de condição `kms:KeySpec` para controlar o acesso a outras operações em uma chave do KMS com base na especificação de chave da chave. Por exemplo, você pode permitir que as entidades principais programem e cancelem a exclusão de chaves somente em chaves do KMS com uma especificação de chave `HMAC_256`.
- Use a chave de condição `kms:KeyUsage` para permitir ou impedir que entidades principais criem qualquer chave de HMAC. Por exemplo, para permitir que os diretores criem somente chaves HMAC, você pode permitir a CreateKeyoperação, mas usar a `kms:KeyUsage` condição para permitir somente chaves com o uso de uma `GENERATE_VERIFY_MAC` chave.

  Também é possível usar a chave de condição `kms:KeyUsage` para controlar o acesso a outras operações em uma chave do KMS com base no uso de chave da chave. Por exemplo, você pode permitir que as entidades principais habilitem e desabilitem somente em chaves do KMS com um uso de chave `GENERATE_VERIFY_MAC`.

Você também pode criar concessões para as operações `GenerateMac` e `VerifyMac`, que são operações de concessão. No entanto, não é possível usar um contexto de criptografia de restrição de concessão em uma concessão para uma chave de HMAC. O formato de etiqueta de HMAC não é compatível com valores de contexto de criptografia.

Visualizar chaves do KMS de HMAC

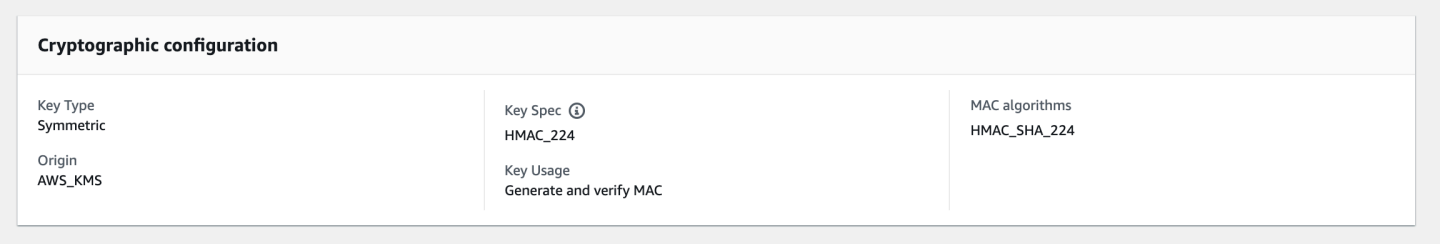
É possível visualizar chaves do KMS de Hash-based message authentication code (HMAC – Código de autenticação de mensagem por hash) no console do AWS KMS ou usando a API DescribeKey. Você pode monitorar o uso de suas chaves HMAC KMS em AWS CloudTrailregistros e na Amazon. CloudWatch Para obter instruções básicas sobre como visualizar chaves do KMS, consulte Visualizar chaves.

Você pode distinguir chaves do KMS de HMAC de outros tipos de chaves do KMS por sua especificação de chave, que começa com `HMAC`, ou pelo uso de chave, que sempre é Generate and verify MAC (Gerar e verificar MAC) (`GENERATE_VERIFY_MAC`).

As chaves do KMS de HMAC estão incluídas na tabela na página Customer managed keys (Chaves gerenciadas pelo cliente) do console do AWS KMS. No entanto, não é possível classificar ou filtrar

as chaves do KMS por especificação de chave ou uso de chave. Para facilitar a localização de suas chaves de HMAC, atribua um alias ou etiqueta distinta a elas. Em seguida, você pode classificar ou filtrar com base no alias ou etiqueta.

Na página de detalhes da chave para uma chave do KMS de HMAC, você pode encontrar os detalhes de configuração na guia Cryptographic configuration (Configuração criptográfica).



Chaves multirregionais em AWS KMS

AWS KMS suporta chaves multirregionais, que são AWS KMS keys diferentes Regiões da AWS e podem ser usadas de forma intercambiável, como se você tivesse a mesma chave em várias regiões. Cada conjunto de chaves multirregionais relacionadas tem o mesmo material de chave e ID de chave, então você pode criptografar dados em um Região da AWS e descriptografá-los em outro Região da AWS sem precisar recriptografar ou fazer uma chamada entre regiões. AWS KMS

Como todas as chaves KMS, as chaves multirregionais nunca saem AWS KMS sem criptografia. Você pode criar chaves multirregionais simétricas ou assimétricas para criptografia ou assinatura, criar chaves multirregionais HMAC para gerar e verificar tags HMAC e criar chaves multirregionais com material de chave importado ou material de chave gerado. AWS KMS Você deve gerenciar cada chave de várias regiões de maneira independente, incluindo a criação de aliases e tags, a definição de suas principais políticas e concessões e sua habilitação e sua desabilitação seletivas. Você pode usar chaves de várias regiões em todas as operações de criptografia que podem ser feitas com chaves de região única.

As chaves de várias regiões são uma solução flexível e eficiente para vários cenários comuns de segurança de dados.

Recuperação de desastres

> Em uma arquitetura de backup e recuperação, as chaves multirregionais permitem que você processe dados criptografados sem interrupção, mesmo no caso de uma Região da AWS interrupção. Os dados mantidos na região de backup podem ser descriptografados nessa região,

enquanto os dados recém-criptografados na região de backup podem ser descriptografados na região principal quando esta for restaurada.

Gerenciamento de dados globais

As empresas que operam globalmente precisam de dados distribuídos globalmente que estejam disponíveis de forma consistente entre Regiões da AWS. Você pode criar chaves de várias regiões em todas as regiões nas quais seus dados residem e, em seguida, usar essas chaves como se fossem uma chave de região única, sem a latência de uma chamada entre regiões ou o custo de recriptografar os dados com uma chave diferente em cada região.

Aplicações de assinatura distribuídas

As aplicações que exigem recursos de assinatura entre regiões podem usar chaves de assinatura assimétrica de várias regiões para gerar assinaturas digitais idênticas de maneira consistente e repetida em diferentes Regiões da AWS.

Se você usar o encadeamento de certificados com um único armazenamento de confiança global (para uma única autoridade de certificação [CA] raiz e CAs intermediárias regionais assinadas pela CA raiz, você não precisará de chaves multirregionais. No entanto, se o sistema não for compatível com CAs intermediárias, como assinatura de aplicações, você poderá usar chaves de várias regiões para trazer consistência às certificações regionais.

Aplicações ativas-ativas que abrangem várias regiões

Algumas workloads e aplicações podem abranger várias regiões em arquiteturas ativas-ativas. Para essas aplicações, chaves de várias regiões podem reduzir a complexidade, fornecendo o mesmo material de chave para operações simultâneas de criptografia e descriptografia em dados que podem estar se movendo pelos limites da região.

Você pode usar chaves de várias regiões com bibliotecas de criptografia do lado do cliente, como AWS Encryption SDK, o DynamoDB Encryption Client e a criptografia do Amazon S3 no lado do cliente. Para ver um exemplo do uso de chaves multirregionais com as tabelas globais do Amazon DynamoDB e o DynamoDB Encryption Client, consulte Criptografar dados globais do lado do cliente com chaves multirregionais no blog de segurança. AWS KMS AWS

AWS os serviços que se integram AWS KMS para criptografia em repouso ou assinaturas digitais atualmente tratam as chaves multirregionais como se fossem chaves de uma única região. Elas podem reempacotar ou criptografar novamente os dados movidos entre Regiões. Por exemplo, a replicação entre regiões do Amazon S3 descriptografa e recriptografa os dados em uma chave do KMS na Região de destino, mesmo ao replicar objetos protegidos por uma chave de várias Regiões.

Chaves de várias Regiões não são globais. Você cria uma chave primária de várias Regiões e, em seguida, a replica em Regiões selecionadas em uma partição da AWS. Em seguida, você gerencia a chave de várias Regiões em cada Região independentemente. AWS Nem AWS KMS nunca cria ou replica automaticamente chaves multirregionais em qualquer região em seu nome. Chaves gerenciadas pela AWS, as chaves KMS que AWS os serviços criam em sua conta para você, são sempre chaves de região única.

Não é possível converter uma chave de Região única existente em uma chave de várias Regiões. Esse design garante que todos os dados protegidos com chaves de Região única existentes mantenham as mesmas propriedades de residência e soberania dos dados.

Para a maioria das necessidades de segurança de dados, o isolamento regional e a tolerância a falhas dos recursos regionais tornam as chaves padrão AWS KMS de região única a solução mais adequada. No entanto, quando você precisa criptografar ou assinar dados em aplicações no lado do cliente em várias Regiões, as chaves de várias Regiões podem ser a melhor solução.

Regiões

As chaves multirregionais são suportadas em todos os Regiões da AWS que oferecem AWS KMS suporte, exceto na China (Pequim) e na China (Ningxia).

Preços e cotas

Cada chave em um conjunto de chaves de várias Regiões relacionado conta como uma única chave do KMS para preços e cotas. As cotas do AWS KMS são calculadas separadamente para cada Região de uma conta. O uso e o gerenciamento das chaves de várias Regiões em cada Região contam para as cotas para essa Região.

Tipos de chave do KMS com suporte

É possível criar os seguintes tipos de chaves KMS multirregionais:

- Chaves do KMS de criptografia simétrica
- Chaves do KMS assimétricas
- Chaves do KMS de HMAC
- Chaves do KMS com material de chave importado

Não é possível criar chaves de várias Regiões em um armazenamento de chaves personalizado.

Tópicos

- Controlar o acesso a chaves de várias regiões
- Criar chaves de várias regiões
- Visualizar chaves de várias regiões
- Gerenciar chaves de várias regiões
- Importar material de chave para chaves de várias regiões
- Excluir chaves de várias regiões

Considerações de segurança de chaves de várias Regiões

Use uma chave AWS KMS multirregional somente quando precisar de uma. Chaves de várias Regiões fornecem uma solução flexível e escalável para workloads que movem dados criptografados entre Regiões da AWS ou que precisam de acesso entre Regiões. Considere usar uma chave de várias Regiões se precisar compartilhar, mover ou fazer backup de dados protegidos entre Regiões ou se precisar criar assinaturas digitais idênticas de aplicações que operam em Regiões diferentes.

No entanto, o processo de criar uma chave de várias Regiões move seu material de chave entre limites de Região da AWS dentro do AWS KMS. O texto criptografado gerado por uma chave de várias Regiões pode ser descriptografado por várias chaves relacionadas em diversas localizações geográficas. Existem também benefícios significativos para serviços e recursos regionalmente isolados. Cada Região da AWS é independente e isolada das outras Regiões. As regiões fornecem tolerância a falhas, estabilidade e resiliência e também podem reduzir a latência. Elas permitem criar recursos redundantes que permanecem disponíveis e não são afetados por uma interrupção em outra Região. Em AWS KMS, eles também garantem que cada texto cifrado possa ser decifrado por apenas uma chave.

As chaves de várias Regiões também levantam novas considerações de segurança:

- É mais complexo controlar o acesso e impor a política de segurança de dados com chaves de várias Regiões. Você precisa garantir que a política seja auditada de maneira consistente na chave entre várias regiões isoladas. Também precisa usar políticas para impor limites, em vez de depender de chaves separadas.

  Por exemplo, você precisa definir condições de políticas nos dados para evitar que equipes de folha de pagamento em uma região possam ler dados de folha de pagamento de uma Região diferente. Além disso, você deve usar o controle de acesso para evitar um cenário em que uma

chave de várias Regiões em uma Região protege os dados de um locatário e uma chave de várias Regiões relacionada em outra Região protege os dados de um locatário diferente.

- A auditoria de chaves entre Regiões também é mais complexa. Com chaves de várias Regiões, você precisa examinar e reconciliar atividades de auditoria em várias Regiões para obter uma compreensão completa das principais atividades em dados protegidos.
- A conformidade com exigências de residência de dados pode ser mais complexa. Com Regiões isoladas, você garante a conformidade da residência de dados e a soberania dos dados. As chaves do KMS em uma determinada Região podem descriptografar dados sigilosos somente nessa Região. Os dados criptografados em uma Região permanecem protegidos e inacessíveis em qualquer outra Região.

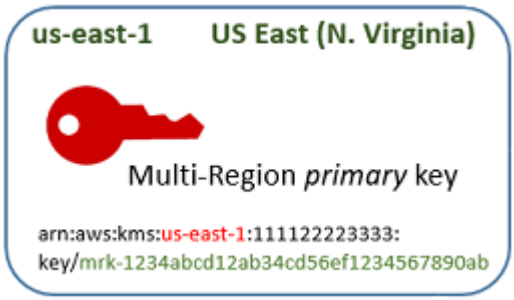
  Para verificar a residência e a soberania dos dados com chaves multirregionais, você precisa implementar políticas de acesso e compilar AWS CloudTrail eventos em várias regiões.

Para facilitar o gerenciamento do controle de acesso em chaves multirregionais, a permissão para replicar uma chave multirregional (kms: ReplicateKey) é separada da permissão padrão para criar chaves (kms:). CreateKey Além disso, AWS KMS oferece suporte a várias condições de política para chaves multirregionais`kms:MultiRegion`, inclusive, que permite ou nega permissão para criar, usar ou gerenciar chaves multirregionais e `kms:ReplicaRegion` que restringe as regiões nas quais uma chave multirregional pode ser replicada. Para obter detalhes, consulte Controlar o acesso a chaves de várias Regiões.

Como funcionam chaves de várias Regiões

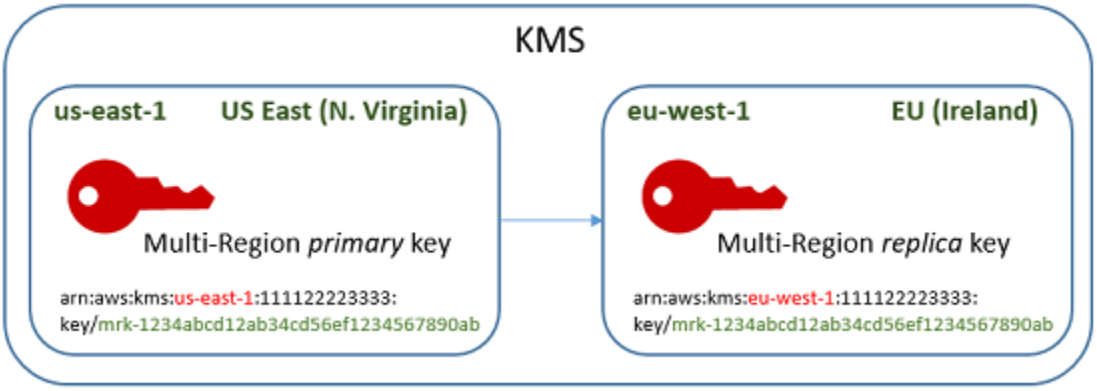
Você começa criando uma chave primária multirregional simétrica ou assimétrica em uma Região da AWS que AWS KMS ofereça suporte, como Leste dos EUA (Norte da Virgínia). Você decide se uma chave é de Região única ou de várias Regiões apenas ao criá-la. Não será possível alterar essa propriedade mais tarde. Como em qualquer chave do KMS, você define uma política de chave para a chave de várias Região, além de poder criar concessões e adicionar aliases e tags para categorização e autorização. (Estas são propriedades independentes que não são compartilhadas ou sincronizadas com outras chaves.) Você pode usar sua chave primária de várias Regiões em operações de criptografia para criptografia ou assinatura.

Você pode criar uma chave primária multirregional no AWS KMS console ou usando a CreateKeyAPI com o `MultiRegion` parâmetro definido como. `true` Observe que chaves de várias Regiões têm um ID de chave distintivo que começa com `mrk-`. É possível usar o prefixo `mrk-` para identificar MRKs de maneira programática.



Se você escolher, poderá replicar a chave primária multirregional em uma ou mais diferentes Regiões da AWS na mesma AWS partição, como Europa (Irlanda). Ao fazer isso, AWS KMS cria uma chave de réplica na região especificada com o mesmo ID de chave e outras propriedades compartilhadas da chave primária. Em seguida, ele transporta com segurança o material de chave pelo limite da Região e o associa à nova chave do KMS na Região de destino, tudo dentro do AWS KMS. O resultado são duas chaves de várias Regiões relacionados, uma chave primária e uma chave de réplica, que podem ser usadas de maneira intercambiável.

Você pode criar uma chave de réplica multirregional no AWS KMS console ou usando a ReplicateKeyAPI.



A chave de réplica de várias Regiões resultante é uma chave do KMS totalmente funcional com as mesmas propriedades compartilhadas que a chave primária. Em todos os outros aspectos, ela é uma chave do KMS independente com sua própria descrição, política de chave, concessões, aliases e etiquetas. Habilitar ou desabilitar uma chave de várias Regiões não tem efeito sobre chaves de várias Regiões relacionadas. Você pode usar as chaves primárias e de réplica independentemente em operações de criptografia ou coordenar seu uso. Por exemplo, você pode criptografar dados com a chave primária na região Leste dos EUA (Norte da Virgínia), mover os dados até a região Europa (Irlanda) e usar a chave de réplica para descriptografar esses dados.

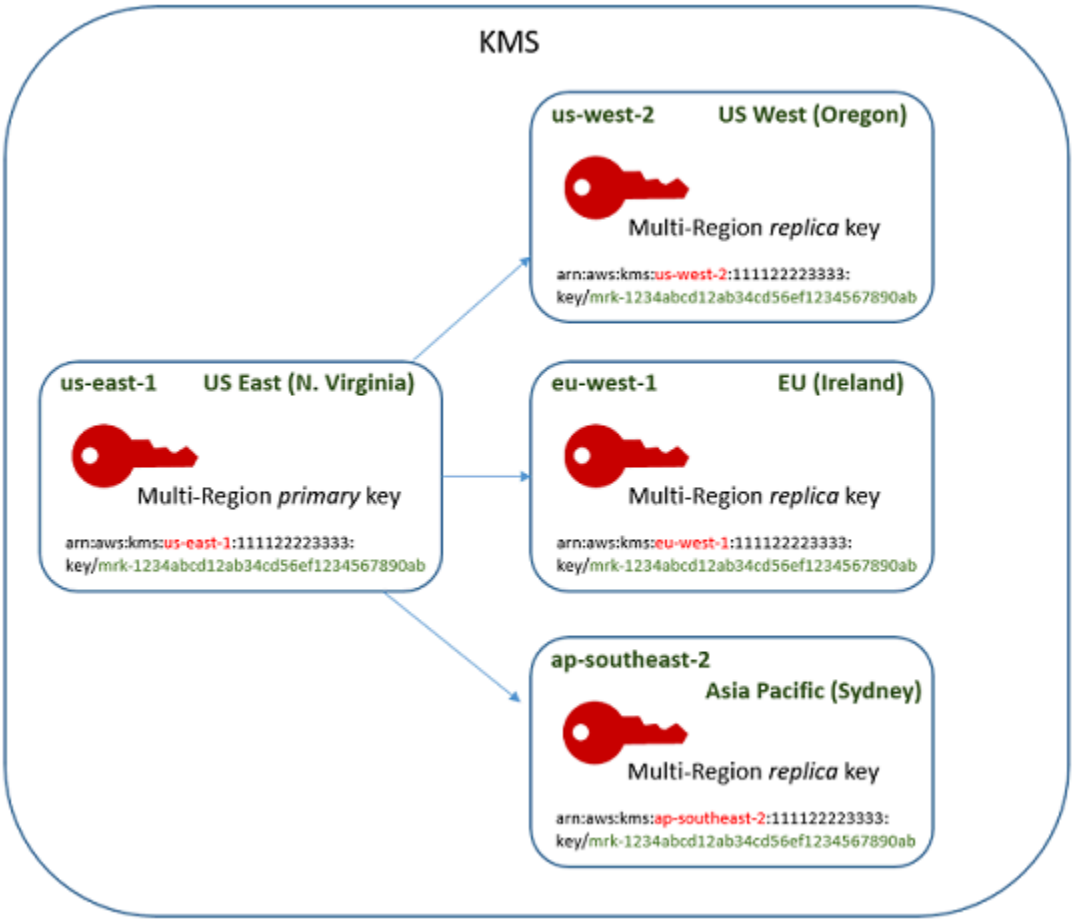
Chaves de várias Regiões relacionadas têm o mesmo ID de chave. Seus ARNs (Nomes de recursos Amazon) de chave diferem apenas no campo Região. Por exemplo, a chave primária e as chaves

de réplica de várias Regiões podem ter os seguintes ARNs de chave de exemplo. O ID da chave, o último elemento no ARN da chave, é idêntico. Ambas as chaves têm o ID de chave distinto de chaves de várias regiões, que começa com 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
```

Ter o mesmo ID de chave é um requisito para interoperabilidade. Ao criptografar, AWS KMS vincula a ID da chave KMS ao texto cifrado para que o texto cifrado possa ser descriptografado somente com essa chave KMS ou com uma chave KMS com a mesma ID de chave. Esse recurso também torna as chaves de várias Regiões relacionadas fáceis de reconhecer e facilita sua utilização intercambiável. Por exemplo, ao usá-las em uma aplicação, você pode fazer referência a chaves de várias Regiões relacionadas com base no ID de chave compartilhada. Em seguida, se necessário, especifique a Região ou o ARN para diferenciá-las.

Conforme suas necessidades de dados mudam, você pode replicar a chave primária para outra Regiões da AWS na mesma partição, como Oeste dos EUA (Oregon) e Ásia-Pacífico (Sydney). O resultado são quatro chaves de várias Regiões relacionados com o mesmo material de chave e IDs de chave, como mostra o seguinte diagrama. Você gerencia as chaves de maneira independente. Elas podem ser usadas de maneira independente ou coordenada. Por exemplo, é possível criptografar dados com a chave de réplica na região Ásia-Pacífico (Sydney), mover os dados para a região Oeste dos EUA (Oregon) e descriptografá-los com a chave de réplica na região Oeste dos EUA (Oregon).



Outras considerações para chaves de várias Regiões incluem as seguintes.

Sincronização de propriedades compartilhadas — Se uma propriedade compartilhada das chaves multirregionais for alterada, AWS KMS sincronizará automaticamente a alteração da chave primária para todas as suas chaves de réplica. Você não pode solicitar ou forçar uma sincronização de propriedades compartilhadas. AWS KMS detecta e sincroniza todas as alterações para você. No entanto, você pode auditar a sincronização usando o SynchronizeMultiRegionKeyevento nos CloudTrail registros.

Por exemplo, se você ativar a rotação automática de chaves em uma chave primária multirregional simétrica, AWS KMS copiará essa configuração para todas as chaves de réplica. Quando o material de chave é alternado, a alternância é sincronizada entre todas as chaves de várias Regiões relacionadas, para que elas continuem a ter o mesmo material de chave atual e também acesso a todas as versões mais antigas do material de chave. Se você criar uma nova chave de réplica, ela terá o mesmo material de chave atual de todas as chaves de várias Regiões relacionadas e terá acesso a todas as versões anteriores do material de chave. Para obter detalhes, consulte Alternância de chaves de várias regiões.

Alterar a chave primária: todo conjunto de chaves de várias Regiões deve ter exatamente uma chave primária. A chave primária é a única que pode ser replicada. Ela é também a fonte das propriedades compartilhadas das suas chaves de réplica. Porém, você pode transformar a chave primária em uma réplica e promover uma das chaves de réplica para chave primária. Você pode fazer isso para excluir uma chave primária de várias Regiões de uma determinada Região ou localizar a chave primária em uma Região mais próxima dos administradores do projeto. Para obter detalhes, consulte Atualizar a região primária.

Excluindo chaves multirregionais — Como todas as chaves KMS, você deve programar a exclusão das chaves multirregionais antes de excluí-las. AWS KMS Enquanto a exclusão da chave estiver pendente, não será possível usá-la em operações de criptografia. No entanto, não AWS KMS excluirá uma chave primária multirregional até que todas as chaves de réplica sejam excluídas. Para obter detalhes, consulte Excluir chaves de várias regiões.

Conceitos

Os seguintes termos e conceitos são usados com chaves de várias Regiões.

Chave de várias Regiões

A chave de várias Regiões é uma chave de um conjunto de chaves do KMS com o mesmo ID de chave e material de chave (e outras propriedades compartilhadas) em diferentes Regiões da AWS. Cada chave de várias Regiões é uma chave do KMS totalmente funcional que pode ser usada de maneira independente de suas chaves de várias Regiões relacionadas. Como todas as chaves multirregionais relacionadas têm o mesmo ID e material de chave, elas são interoperáveis, ou seja, qualquer chave multirregional relacionada em qualquer uma Região da AWS pode descriptografar texto cifrado criptografado por qualquer outra chave multirregional relacionada.

Você define a propriedade de várias Regiões de uma chave do KMS ao criá-la. Não é possível alterar a propriedade de várias regiões em uma chave existente. Não é possível converter uma chave de região única em chave de várias regiões nem converter uma chave de várias regiões em uma chave de região única. Para mover workloads existentes para cenários de várias regiões, é necessário recriptografar seus dados ou criar novas assinaturas com novas chaves de várias regiões.

Uma chave multirregional pode ser simétrica ou assimétrica e pode usar material chave ou material AWS KMS chave importado. Não é possível criar chaves de várias Regiões em um armazenamento de chaves personalizado.

Em um conjunto de chaves de várias Regiões relacionadas, há exatamente uma chave primária em um determinado momento. Você pode criar chaves de réplica dessa chave primária em outras Regiões da AWS. Também pode atualizar a região primária, o que transforma a chave primária em uma chave de réplica e transforma uma chave de réplica especificada na chave primária. No entanto, você pode manter somente uma chave primária ou chave de réplica em cada uma Região da AWS. Todas as Regiões devem estar na mesma partição da AWS.

Você pode ter diversos conjuntos de chaves de várias regiões relacionadas nas mesmas Regiões da AWS ou em regiões diferentes. Embora chaves de várias Regiões relacionadas sejam interoperáveis, chaves de várias Regiões não relacionadas não são interoperáveis.

Chave primária

Uma chave primária multirregional é uma chave KMS que pode ser replicada em outra Regiões da AWS na mesma partição. Cada conjunto de chaves de várias Regiões tem somente uma chave primária.

Uma chave primária é diferente de uma chave de réplica nos seguintes aspectos:

- Somente uma chave primária pode ser replicada.
- A chave primária é a fonte de propriedades compartilhadas de suas chaves de réplica, incluindo o material da chave e o ID da chave.
- Você pode habilitar e desabilitar a alternância automática de chaves somente em uma chave primária.
- Você pode programar a exclusão de uma chave primária a qualquer momento. Mas não AWS KMS excluirá uma chave primária até que todas as chaves de réplica sejam excluídas.

Entretanto, as chaves primárias e de réplica não diferem em nenhuma propriedade criptográfica. É possível usar uma chave primária e suas chaves de réplica alternadamente.

Não é necessário replicar uma chave primária. Você pode usá-la como faria com qualquer chave do KMS e replicá-la se e quando ela for útil. No entanto, como chaves de várias Regiões têm propriedades de segurança diferentes das chaves de uma única Região, recomendamos criar uma chave de várias Regiões apenas quando você planeja replicá-la.

Chave de réplica

Uma chave de réplica de várias Regiões é uma chave do KMS que tem o mesmo ID de chave e material de chave de sua chave primária e chaves de réplica relacionadas, mas existe em uma Região da AWS diferente,

Uma chave de réplica é uma chave do KMS totalmente funcional com sua própria política de chave, concessões, alias, etiquetas e outras propriedades. Ela não é uma cópia ou ponteiro da chave primária ou de qualquer outra chave. Você pode usar uma chave de réplica mesmo quando sua chave primária e todas as chaves de réplica relacionadas estão desabilitadas. Também pode converter uma chave de réplica em uma chave primária, e vice-versa. Depois de criada, uma chave de réplica depende de sua chave primária somente para alternância de chaves e atualização da Região primária.

Chaves primárias e de réplica não diferem em nenhuma propriedade criptográfica. É possível usar uma chave primária e suas chaves de réplica alternadamente. Os dados criptografados por uma chave primária ou uma chave de réplica podem ser descriptografados pela mesma chave ou por qualquer chave primária ou chave de réplica relacionada.

Replicar

Você pode replicar uma chave primária multirregional em outra Região da AWS na mesma partição. Ao fazer isso, AWS KMS cria uma chave de réplica multirregional na região especificada com o mesmo ID de chave e outras propriedades compartilhadas da chave primária. Em seguida, ele transporta com segurança o material de chave pelo limite da Região e o associa à nova chave de réplica, tudo dentro do AWS KMS.

Propriedades compartilhadas

Propriedades compartilhadas são propriedades de uma chave primária multirregional que são compartilhadas com suas chaves de réplica. AWS KMS cria as chaves de réplica com os mesmos valores de propriedade compartilhada da chave primária. Em seguida, ele sincroniza periodicamente os valores das propriedades compartilhadas da chave primária com suas chaves de réplica. Não é possível definir essas propriedades em uma chave de réplica.

Veja a seguir as propriedades compartilhadas de chaves de várias Regiões.

- ID da chave: (O elemento `Region` do elemento do é diferente do ARN da chave.)
- Material de chave

- Origem do material de chave
- Especificação da chave e algoritmos de criptografia
- Uso da chave
- Alternância da chave automática:: você pode habilitar e desabilitar a alternância automática de chaves somente em uma chave primária. Novas chaves de réplica são criadas com todas as versões do material de chave compartilhado. Para obter detalhes, consulte Alternância de chaves de várias regiões.
- Rotação sob demanda — Você pode realizar a rotação sob demanda somente na chave primária. Novas chaves de réplica são criadas com todas as versões do material de chave compartilhado. Para obter detalhes, consulte Alternância de chaves de várias regiões.

Você também pode pensar nemas designações primárias e de réplicas de chaves de várias Regiões relacionadas como propriedades compartilhadas. Quando você cria novas chaves de réplica ou atualiza a chave primária, AWS KMS sincroniza a alteração com todas as chaves multirregionais relacionadas. Quando essas alterações estiverem concluídas, todas as chaves de várias Regiões relacionadas listarão suas chaves primárias e chaves de réplica com precisão.

Todas as outras propriedades das chaves de várias regiões são propriedades independentes, incluindo descrição, política de chaves, concessões, estados de chave habilitadas e desabilitadas, aliases e etiquetas. Você pode definir os mesmos valores para essas propriedades em todas as chaves de várias regiões relacionadas. Porém, se você alterar o valor de uma propriedade independente, o AWS KMS não a sincronizará.

Você pode rastrear a sincronização das propriedades compartilhadas das suas chaves de várias regiões. Em seu AWS CloudTrail registro, procure o SynchronizeMultiRegionKeyevento.

Controlar o acesso a chaves de várias Regiões

Você pode usar chaves de várias regiões em cenários de conformidade, recuperação de desastres e backup que seriam mais complexos com chaves de uma única região. No entanto, como as propriedades de segurança das chaves de várias regiões são significativamente diferentes das de chaves de uma única região, convém ter cuidado ao autorizar a criação, o gerenciamento e o uso de chaves de várias regiões.

> **Note**
>
> Instruções de políticas do IAM existentes com caracteres curinga no campo `Resource` agora aplicam-se a chaves de região única e de várias regiões. Para restringi-las a chaves KMS de região única ou chaves de várias regiões, use a chave de condição kms:. MultiRegion

Use suas ferramentas de autorização para impedir a criação e o uso de chaves de várias regiões em qualquer cenário em que uma única região seja suficiente. Permita que as entidades principais repliquem uma chave de várias regiões apenas nas Regiões da AWS que precisam dessa chave. Dê permissão para chaves de várias regiões apenas às entidades principais que precisam delas e apenas para tarefas necessárias.

Você pode usar políticas de chaves, políticas do IAM e concessões para permitir que as entidades principais do IAM gerenciem e usem chaves de várias regiões na sua Conta da AWS. Cada chave de várias regiões é um recurso independente com um ARN de chave exclusivo e uma política de chaves. Você precisa estabelecer e manter uma política de chaves para cada chave e certificar-se de que as políticas do IAM novas e existentes implementem sua estratégia de autorização.

Tópicos

- Noções básicas de autorização para chaves de várias regiões
- Autorizar administradores e usuários de chave de várias regiões
- Autorizar o AWS KMS a sincronizar chaves de várias regiões

Noções básicas de autorização para chaves de várias regiões

Ao projetar políticas de chaves e políticas do IAM para chaves de várias regiões, considere os seguintes princípios.

- Política de chaves — Cada chave de várias regiões é um recurso de chave do KMS independente com sua própria política de chaves. Você pode aplicar a mesma política de chaves ou uma política de chaves diferente a cada chave no conjunto de chaves de várias regiões relacionadas. Políticas de chaves não são propriedades compartilhadas de chaves de várias regiões. O AWS KMS não copia nem sincroniza instruções de chaves entre chaves de várias regiões relacionadas.

  Quando você cria uma chave de réplica no console do AWS KMS, este exibe a política de chaves atual da chave primária por questão de conveniência. É possível usar essa política de chaves,

editá-la ou excluí-la e substituí-la. Porém, mesmo que você aceite a política de chaves primária sem alterações, o AWS KMS não sincroniza as políticas. Por exemplo, se você alterar a política de chaves da chave primária, a política de chaves da chave de réplica permanecerá igual.

- Política de chaves padrão — Quando você cria chaves multirregionais usando as `ReplicateKey` operações CreateKeye, a política de chaves padrão é aplicada, a menos que você especifique uma política de chaves na solicitação. Essa é a mesma política de chave padrão aplicada a chaves de região única.
- Políticas do IAM — Assim como acontece com todas as chaves do KMS, você pode usar políticas do IAM para controlar o acesso a chaves de várias regiões somente quando a política de chaves permite. Políticas do IAM aplicam-se a todas as Regiões da AWS por padrão. No entanto, você pode usar chaves de condição, como aws: RequestedRegion, para limitar as permissões a uma região específica.

  Para criar chaves primárias e de réplica, as entidades principais devem ter a permissão `kms:CreateKey` em uma política do IAM aplicável à região na qual a chave é criada.
- Concessões — As concessões do AWS KMS são regionais. Cada concessão dá permissões para uma chave do KMS. É possível usar concessões para dar permissões para uma chave primária ou chave de réplica de várias regiões. Porém, você não pode usar uma única concessão para dar permissões para várias chaves do KMS, mesmo que elas sejam chaves de várias regiões relacionadas.
- ARN de chave — Cada chave de várias regiões tem um ARN de chave. Os ARNs de chaves de várias regiões relacionadas têm a mesma partição, conta e ID de chave, mas regiões diferentes.

  Para aplicar uma instrução de política do IAM a uma chave de várias regiões específica, use seu ARN de chave ou um padrão de ARN de chave que inclua a região. Para aplicar uma instrução de política do IAM a todas as chaves de várias regiões relacionadas, use um caractere curinga (*) no elemento Region do ARN, como mostra o exemplo abaixo.

```
{
  "Effect": "Allow",
  "Action": [
    "kms:Describe*",
    "kms:List*"
  ],
  "Resource": {
      "arn:aws:kms:*::111122223333:key/mrk-1234abcd12ab34cd56ef1234567890ab"
  }
}
```

Para aplicar uma declaração de política a todas as chaves multirregionais em suaConta da AWS, você pode usar a condição kms: MultiRegion policy ou um padrão de ID de chave que inclua o prefixo distinto`mrk-`.

- Função vinculada ao serviço — Os diretores que criam chaves primárias multirregionais devem ter a permissão iam:. CreateServiceLinkedRole

  Para sincronizar as propriedades compartilhadas de chaves de várias regiões relacionadas, o AWS KMS pressupõe uma função vinculada ao serviço do IAM. O AWS KMS cria a função vinculada ao serviço na Conta da AWS sempre que você cria uma chave primária de várias regiões. (Se a função existir, o AWS KMS a recriará, o que não causa nenhum problema.) A função é válida em todas as regiões. AWS KMSPara permitir a criação (ou recriação) da função vinculada ao serviço, os diretores que criam chaves primárias multirregionais devem ter a permissão iam:. CreateServiceLinkedRole

Autorizar administradores e usuários de chave de várias regiões

As entidades principais que criam e gerenciam chaves de várias regiões precisam das seguintes permissões nas regiões primária e de réplica:

- `kms:CreateKey`
- `kms:ReplicateKey`
- `kms:UpdatePrimaryRegion`
- `iam:CreateServiceLinkedRole`

Criar uma chave primária

Para criar uma chave primária multirregional, o principal precisa das CreateServiceLinkedRole permissões kms: CreateKey e iam: em uma política do IAM que seja efetiva na região da chave primária. As entidades principais que têm essas permissões podem criar chaves de região única e de várias regiões, a menos que você restrinja suas permissões.

A `iam:CreateServiceLinkedRole` permissão permite criar AWS KMS a AWSServiceRoleForKeyManagementServiceMultiRegionKeysfunção para sincronizar as propriedades compartilhadas das chaves multirregionais relacionadas.

Por exemplo, essa política do IAM permite que uma entidade principal crie qualquer tipo de chave do KMS.

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

Para permitir ou negar a permissão para criar chaves primárias multirregionais, use a chave de MultiRegion condição kms:. Os valores válidos são `true` (chave de várias regiões) ou `false` (chave de região única). Por exemplo, a instrução de política do IAM a seguir usa uma ação `Deny` com a chave de condição `kms:MultiRegion` para impedir que as entidades principais criem chaves de várias regiões.

```
{
  "Version": "2012-10-17",
  "Statement":{
      "Action":"kms:CreateKey",
      "Effect":"Deny",
      "Resource":"*",
      "Condition": {
          "Bool": "kms:MultiRegion": true
      }
  }
}
```

Replicação de chaves

Para criar uma chave de réplica de várias regiões, a entidade principal precisará das seguintes permissões:

- kms: ReplicateKey permissão na política de chaves da chave primária.
- kms: CreateKey permissão em uma política do IAM que é efetiva na região da chave de réplica.

Tenha cuidado ao conceder essas permissões. Elas permitem que as entidades principais criem chaves do KMS e as políticas de chaves que autorizam seu uso. A permissão `kms:ReplicateKey` também autoriza a transferência de material chave através dos limites da região no AWS KMS.

Para restringir o modo Regiões da AWS em que uma chave multirregional pode ser replicada, use a chave de condição kms: ReplicaRegion. Ela limita apenas a permissão `kms:ReplicateKey`. De outra forma, ela não terá efeito. Por exemplo, a política de chaves a seguir permite que a entidade principal replique essa chave primária, mas somente nas regiões especificadas.

```
{
  "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"
      ]
    }
  }
}
```

Atualizar a região primária

As entidades principais autorizadas podem converter uma chave de réplica em uma chave primária, o que transforma a chave primária anterior em uma réplica. Essa ação é conhecida como atualização da região primária. Para atualizar a região principal, o principal precisa de kms: UpdatePrimaryRegion permissão em ambas as regiões. Você pode fornecer essas permissões em uma política de chaves ou política do IAM.

- `kms:UpdatePrimaryRegion` na chave primária. Essa permissão deve ser efetiva na região da chave primária.
- `kms:UpdatePrimaryRegion` na chave de réplica. Essa permissão deve ser efetiva na região da chave de réplica.

Por exemplo, a política de chaves a seguir dá aos usuários que podem assumir a função Administrador permissão para atualizar a região primária da chave do KMS. Essa chave do KMS pode ser a chave primária ou uma chave de réplica nessa operação.

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

Para restringir o Regiões da AWS que pode hospedar uma chave primária, use a chave de PrimaryRegion condição kms:. Por exemplo, a seguinte instrução de política do IAM permite que as entidades principais atualizem a região primária das chaves de várias regiões na Conta da AWS, mas somente quando a nova região primária é uma das regiões especificadas.

```
{
  "Effect": "Allow",
  "Action": "kms:UpdatePrimaryRegion",
  "Resource": {
      "arn:aws:kms:*:111122223333:key/*"
  },
  "Condition": {
    "StringEquals": {
      "kms:PrimaryRegion": [
         "us-west-2",
         "sa-east-1",
         "ap-southeast-1"
      ]
    }
  }
}
```

Usar e gerenciar chaves de várias regiões

Por padrão, as entidades principais que têm permissão para usar e gerenciar chaves do KMS em uma Conta da AWS e região também têm permissão para usar e gerenciar chaves de várias regiões. No entanto, você pode usar a chave de MultiRegion condição kms: para permitir somente chaves de região única ou somente chaves de várias regiões. Ou use a chave de MultiRegionKeyType

condição kms: para permitir somente chaves primárias multirregionais ou somente chaves de réplica. Ambas as chaves de condição controlam o acesso à CreateKeyoperação e a qualquer operação que use uma chave KMS existente, como Criptografar ou. EnableKey

A instrução de política do IAM a seguir usa a chave de condição `kms:MultiRegion` para impedir que as entidades principais usem ou gerenciem qualquer chave de várias regiões.

```
{
  "Effect": "Deny",
  "Action": "kms:*",
  "Resource": "*",
  "Condition": {
    "Bool": "kms:MultiRegion": true
  }
}
```

Esse exemplo de instrução de política do IAM usa a condição `kms:MultiRegionKeyType` para permitir que as entidades principais programem e cancelem a exclusão de chaves, mas somente em chaves de réplica de várias regiões.

```
{
  "Effect": "Allow",
  "Action": [
    "kms:ScheduleKeyDeletion",
    "kms:CancelKeyDeletion"
  ],
  "Resource": {
      "arn:aws:kms:us-west-2:111122223333:key/*"
  },
  "Condition": {
    "StringEquals": "kms:MultiRegionKeyType": "REPLICA"
  }
}
```

Autorizar o AWS KMS a sincronizar chaves de várias regiões

Para oferecer suporte a chaves de várias regiões, o AWS KMS usa uma função vinculada ao serviço do IAM. Essa função dá ao AWS KMS as permissões necessárias para sincronizar propriedades compartilhadas. Você pode ver o SynchronizeMultiRegionKey CloudTrail evento que registra a AWS KMS sincronização de propriedades compartilhadas em seus AWS CloudTrail registros.

Sobre a função vinculada ao serviço para chaves de várias regiões

Uma função vinculada ao serviço é uma função do IAM que oferece permissão a um serviço da AWS para chamar outros serviços da AWS em seu nome. Ela foi projetada para facilitar o uso dos recursos de vários serviços integrados da AWS sem a necessidade de criar e manter políticas complexas do IAM.

Para chaves multirregionais, AWS KMS cria a função AWSServiceRoleForKeyManagementServiceMultiRegionKeysvinculada ao serviço com a política. AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy Essa política concede à função a permissão `kms:SynchronizeMultiRegionKey`, que permite sincronizar as propriedades compartilhadas de chaves de várias regiões.

Como a função AWSServiceRoleForKeyManagementServiceMultiRegionKeysvinculada ao serviço é confiável somente`mrk.kms.amazonaws.com`, somente AWS KMS pode assumir essa função vinculada ao serviço. Essa função é limitada às operações necessárias para o AWS KMS sincronizar as propriedades compartilhadas de várias regiões. Ele não concede permissões adicionais ao AWS KMS. Por exemplo, o AWS KMS não tem permissão para criar, replicar ou excluir chaves do KMS.

Para obter mais informações sobre como os serviços da AWS usam funções vinculadas a serviços, consulte Usar funções vinculadas a serviços, no Manual do usuário do IAM.

Criar a função vinculada ao serviço

AWS KMScria automaticamente a função AWSServiceRoleForKeyManagementServiceMultiRegionKeysvinculada ao serviço em sua Conta da AWS quando você cria uma chave multirregional, se a função ainda não existir. Não é possível criar ou criar outra vez essa função vinculada a serviço diretamente.

Editar a descrição de uma função vinculada ao serviço

Você não pode editar o nome da função ou as declarações de política na função AWSServiceRoleForKeyManagementServiceMultiRegionKeysvinculada ao serviço, mas você pode editar a descrição da função. Para obter mais informações, consulte Editar uma função vinculada ao serviço, no Manual do usuário do IAM.

Excluir a função vinculada ao serviço

AWS KMSnão exclui a função AWSServiceRoleForKeyManagementServiceMultiRegionKeysvinculada ao serviço da

sua Conta da AWS e você não pode excluí-la. No entanto, AWS KMS não assume a AWSServiceRoleForKeyManagementServiceMultiRegionKeysfunção nem usa nenhuma de suas permissões, a menos que você tenha chaves multirregionais em sua Conta da AWS região.

Criar chaves de várias regiões

Você pode criar chaves de várias regiões no console ou usando a API do AWS KMS.

A propriedade de várias regiões definida neste procedimento é imutável. Não é possível converter uma chave de região única em chave de várias regiões nem converter uma chave de várias regiões em uma chave de região única.

Tópicos

- Criar chaves primárias de várias regiões
- Criar chaves de réplica de várias regiões

Criar chaves primárias de várias regiões

Você pode criar uma chave primária de várias regiões no console do AWS KMS ou com o uso da API do AWS KMS. Você pode criar a chave primária em qualquer Região da AWS em que o AWS KMS oferece suporte para chaves de várias regiões.

Para criar uma chave primária multirregional, o principal precisa das mesmas permissões necessárias para criar qualquer chave KMS, incluindo a CreateKey permissão kms: em uma política do IAM. O diretor também precisa do objetivo: CreateServiceLinkedRole permissão. Você pode usar a chave de MultiRegionKeyType condição kms: para permitir ou negar permissão para criar chaves primárias multirregionais.

Essas instruções criam uma chave primária de várias regiões com o material de chave gerado pelo AWS KMS. Para criar uma chave primária de várias regiões com material de chave importado, consulte Criar uma chave primária com material de chave importado.

Tópicos

- Criar uma chave primária de várias regiões (console)
- Criar uma chave primária de várias regiões (API do AWS KMS)

Criar uma chave primária de várias regiões (console)

Para criar uma chave primária de várias regiões no console do AWS KMS, use o mesmo processo que você usaria para criar qualquer chave do KMS. Selecione uma chave de várias regiões em Advanced options (Opções avançadas). Para obter instruções completas, consulte Criar chaves.

> **Important**
>
> Não inclua informações confidenciais ou sigilosas no alias, na descrição ou nas tags. Esses campos podem aparecer em texto simples em CloudTrail registros e outras saídas.

1. Faça login no AWS Management Console e abra o console do AWS Key Management Service (AWS KMS) em https://console.aws.amazon.com/kms.
2. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.
3. No painel de navegação, escolha Customer managed keys (Chaves gerenciadas pelo cliente).
4. Escolha Create key (Criar chave).
5. Selecione um tipo de chave simétrica ou assimétrica. As chaves simétricas são o padrão.

   Você pode criar chaves simétricas e assimétricas de várias regiões, inclusive chaves do KMS de HMAC de várias regiões, que são simétricas.
6. Selecione o uso da chave. Encrypt and decrypt (Criptografar e descriptografar) é o padrão.

   Para obter ajuda, consulte the section called “Criar chaves”, the section called “Criar chaves do KMS assimétricas” ou the section called “Criar chaves de HMAC”.
7. Expanda Advanced options (Opções avançadas).
8. Em Key material origin (Origem do material de chave), para que o AWS KMS gere o material chave que as suas chaves primárias e de réplica compartilharão, escolha KMS. Se você estiver importando material de chave para chaves primárias e de réplica, escolha External (Import key material) (Externo [Importar material de chave]).
9. Em Multi-Region replication (Replicação em várias regiões), escolha Allow this key to be replicated into other Regions (Permitir que esta chave seja replicada em outras regiões).

   Não será possível alterar essa configuração após a criação da chave do KMS.
10. Digite um alias para a chave primária.

Aliases não são uma propriedade compartilhada de chaves de várias regiões. Você pode dar à chave primária de várias regiões e suas réplicas o mesmo alias ou alias diferentes. AWS KMS não sincroniza os aliases de chaves de várias regiões.

> **Note**
>
> Adicionar, excluir ou atualizar um alias pode conceder ou negar uma permissão à chave do KMS. Para obter mais detalhes, consulte ABAC para AWS KMS e Usar aliases para controlar o acesso a chaves do KMS.

11. (Opcional) Digite uma descrição da chave primária.

    Descrições não são uma propriedade compartilhada de chaves de várias regiões. Você pode fornecer à chave primária de várias regiões e suas réplicas a mesma descrição ou descrições diferentes. O AWS KMS não sincroniza as descrições de chaves de várias regiões.

12. (Opcional) Digite uma chave de tag e um valor de tag opcional. Para atribuir mais de uma etiqueta à chave primária, selecione Add tag (Adicionar etiqueta).

    Etiquetas não são uma propriedade compartilhada de chaves de várias regiões. Você pode dar à chave primária de várias regiões e suas réplicas as mesmas etiquetas ou etiquetas diferentes. AWS KMS não sincroniza as etiquetas de chaves de várias regiões. É possível alterar as etiquetas em chaves do KMS a qualquer momento.

> **Note**
>
> Marcar ou desmarcar uma chave do KMS pode conceder ou negar uma permissão a essa chave do KMS. Para obter mais detalhes, consulte ABAC para AWS KMS e Usar etiquetas para controlar o acesso a chaves do KMS.

13. Selecione os usuários e as funções do IAM que podem administrar a chave primária.

> **Note**
>
> As políticas do IAM podem conceder permissão para gerenciar a chave do KMS a outros usuários e funções do IAM.
> As práticas recomendadas do IAM não encorajam o uso de usuários do IAM com credenciais de longo prazo. Sempre que possível, use os perfis do IAM, por fornecerem

credenciais temporárias. Para obter detalhes, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

Essa etapa inicia o processo de criação de uma política de chaves para a chave primária. Políticas de chaves não são uma propriedade compartilhada de chaves de várias regiões. Você pode fornecer à chave primária de várias regiões e suas réplicas a mesma política de chaves ou políticas de chave diferentes. O AWS KMS não sincroniza as políticas de chaves de várias regiões. Você pode alterar a política de chaves de uma chave do KMS a qualquer momento.

14. Conclua as etapas para criar a política de chaves, incluindo a seleção de usuários de chaves. Após revisar a política de chaves, escolhaFinish (Concluir) para criar a chave do KMS.

Criar uma chave primária de várias regiões (API do AWS KMS)

Para criar uma chave primária multirregional, use a CreateKeyoperação. Use também o parâmetro `MultiRegion` com um valor de `True`.

Por exemplo, o comando a seguir cria uma chave primária de várias regiões na Região da AWS (us-east-1) do autor da chamada. Ele aceita valores padrão para todas as outras propriedades, incluindo a política de chaves. Os valores padrão para chaves primárias de várias regiões são os mesmos que os valores padrão para todas as outras chaves do KMS, incluindo a política de chaves padrão. Este procedimento cria uma chave de criptografia simétrica, a chave padrão do KMS.

A resposta inclui o elemento `MultiRegion` e o elemento `MultiRegionConfiguration` com subelementos típicos e valores para uma chave primária de várias regiões sem chaves de réplica. O ID de chave de uma chave de várias regiões sempre começa com `mrk-`.

> **Important**
>
> Não inclua informações confidenciais ou sigilosas nos campos `Description` ou `Tags`. Esses campos podem aparecer em texto simples em CloudTrail registros e outras saídas.

```
$ 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": [ ]
      }
    }
}
```

Criar chaves de réplica de várias regiões

Você pode criar uma chave de réplica multirregional no AWS KMS console, usando a ReplicateKeyoperação ou usando um AWS CloudFormation modelo. Você não pode usar a CreateKeyoperação para criar uma chave de réplica.

Você pode usar esses procedimentos para replicar qualquer chave primária de várias regiões, inclusive uma chave do KMS de criptografia simétrica, uma chave do KMS de criptografia assimétrica ou uma chave do KMS de Hash-based message authentication code (HMAC – Código de autenticação de mensagem por hash).

Quando essa operação for concluída, a nova chave de réplica terá um estado de chave transitório de `Creating`. Esse estado da chave muda para `Enabled` (ou PendingImport) após alguns segundos, quando o processo de criação da nova chave de réplica é concluído. Enquanto o estado da chave for `Creating`, você poderá gerenciar a chave, mas ainda não poderá usá-la em operações

de criptografia. Se você estiver criando e usando a chave de réplica programaticamente, tente novamente `KMSInvalidStateException` ou ligue DescribeKeypara verificar seu `KeyState` valor antes de usá-la.

Se você excluir uma chave de réplica por engano, poderá usar esse procedimento para recriá-la. Se você replicar a mesma chave primária na mesma região, a nova chave de réplica criada terá as mesmas propriedades compartilhadas que a chave de réplica original.

> **Important**
>
> Não inclua informações confidenciais ou sigilosas no alias, na descrição ou nas tags. Esses campos podem aparecer em texto simples em CloudTrail registros e outras saídas.

Saiba mais

- Para criar uma chave de réplica de várias regiões com material de chave importado, consulte Criar uma chave de réplica com material de chave importado.
- Para usar um AWS CloudFormation modelo para criar uma chave de réplica, consulte AWS::KMS::ReplicaKeyo Guia do AWS CloudFormation usuário.

Tópicos

- Regiões de réplica
- Criar chaves de réplica (console)
- Criar uma chave de réplica (API do AWS KMS)

Regiões de réplica

Você normalmente opta por replicar uma chave de várias regiões em uma Região da AWS com base no seu modelo de negócios e requisitos normativos. Por exemplo, você pode replicar uma chave em regiões nas quais você mantém seus recursos. Ou, para atender a um requisito de recuperação de desastres, você pode replicar uma chave em regiões geograficamente distantes.

Veja a seguir os requisitos do AWS KMS para regiões de réplica. Se a região escolhida não atender a esses requisitos, as tentativas de replicar uma chave falharão.

- Uma chave de várias regiões relacionada por região — Não é possível criar uma chave de réplica na mesma região que a chave primária ou na mesma região que outra réplica da chave primária.

Se você tentar replicar uma chave primária em uma região que já tenha uma réplica dessa chave primária, a tentativa falhará. Se a chave de réplica atual na região estiver no estado de chave `PendingDeletion`, você poderá cancelar a exclusão da chave de réplica ou aguardar até que a chave de réplica seja excluída.

- Várias chaves de várias regiões não relacionadas na mesma região — É possível ter várias chaves de várias regiões não relacionadas na mesma região. Por exemplo, você pode ter duas chaves primárias de várias regiões na região `us-east-1`. Cada uma das chaves primárias pode ter uma chave de réplica na região `us-west-2`.
- Regiões na mesma partição — A região da chave de réplica deve estar na mesma partição da AWS que a região da chave primária.
- A região deve estar habilitada — Se uma região estiver desabilitada por padrão, você não poderá criar nenhum recurso nessa região até que ela esteja habilitada para a sua Conta da AWS.

Criar chaves de réplica (console)

No console do AWS KMS, você pode criar uma ou várias réplicas de uma chave primária de várias regiões na mesma operação.

Esse procedimento é semelhante à criação de uma chave do KMS de região única padrão no console. No entanto, como uma chave de réplica é baseada na chave primária, você não seleciona valores para propriedades compartilhadas, como a especificação da chave (simétrica ou assimétrica), o uso da chave ou a origem da chave.

Você especifica propriedades que não são compartilhadas, incluindo alias, etiquetas, descrição e política de chaves. Por conveniência, o console mostra os valores de propriedade atuais da chave primária, mas é possível alterá-los. Mesmo que você mantenha os valores das chaves primárias, o AWS KMS não mantém esses valores sincronizados.

> **Important**
>
> Não inclua informações confidenciais ou sigilosas no alias, na descrição ou nas tags. Esses campos podem aparecer em texto simples em CloudTrail registros e outras saídas.

1. Faça login no AWS Management Console e abra o console do AWS Key Management Service (AWS KMS) em https://console.aws.amazon.com/kms.
2. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.

3. No painel de navegação, escolha Customer managed keys (Chaves gerenciadas pelo cliente).
4. Selecione o ID de chave ou alias de uma chave primária de várias regiões. Isso abre a página de detalhes da chave do KMS.

   Para identificar uma chave primária de várias regiões, use o ícone de ferramenta no canto superior direito para adicionar a coluna Regionality (Regionalidade) à tabela.
5. Escolha a guia Regionality (Regionalidade).
6. Na seção Related multi-Region keys (Chaves de várias regiões relacionadas), selecione Create new replica keys (Criar novas chaves de réplica).

   A seção Related multi-Region keys (Chaves de várias regiões relacionadas) mostra a região da chave primária e suas chaves de réplica. Você pode usar essa tela para ajudar a escolher a região da sua nova chave de réplica.
7. Escolha uma ou mais Regiões da AWS. Esse procedimento cria uma chave de réplica em cada uma das regiões selecionadas.

   O menu inclui apenas regiões na mesma partição da AWS que a chave primária. As regiões que já têm uma chave de várias regiões relacionada são exibidas, mas podem ser selecionadas. Talvez você não tenha permissão para replicar uma chave em todas as regiões no menu.

   Quando terminar de escolher regiões, feche o menu. As regiões escolhidas são exibidas. Para cancelar a replicação em uma região, escolha a opção X ao lado do nome da região.
8. Digite um alias para a chave de réplica.

   O console exibe um dos aliases atuais da chave primária, mas você pode alterá-lo. Você pode dar à chave primária de várias regiões e suas réplicas o mesmo alias ou alias diferentes. Aliases não são uma propriedade compartilhada de chaves de várias regiões. O AWS KMS não sincroniza os aliases de chaves de várias regiões.

   Adicionar, excluir ou atualizar um alias pode conceder ou negar uma permissão à chave do KMS. Para obter mais detalhes, consulte ABAC para AWS KMS e Usar aliases para controlar o acesso a chaves do KMS.
9. (Opcional) Digite uma descrição da chave de réplica.

   O console exibe a descrição atual da chave primária, mas é possível alterá-la. Descrições não são uma propriedade compartilhada de chaves de várias regiões. Você pode fornecer à chave primária de várias regiões e suas réplicas a mesma descrição ou descrições diferentes. O AWS KMS não sincroniza as descrições de chaves de várias regiões.

10. (Opcional) Digite uma chave de etiqueta e um valor de etiqueta opcional. Para atribuir mais de uma etiqueta à chave de réplica, escolha Add tag (Adicionar etiqueta).

    O console mostra as etiquetas atualmente anexadas à chave primária, mas é possível alterá-las. Etiquetas não são uma propriedade compartilhada de chaves de várias regiões. Você pode dar à chave primária de várias regiões e suas réplicas as mesmas etiquetas ou etiquetas diferentes. AWS KMS não sincroniza as etiquetas de chaves de várias regiões.

    Marcar ou desmarcar uma chave do KMS pode conceder ou negar uma permissão a essa chave do KMS. Para obter mais detalhes, consulte ABAC para AWS KMS e Usar etiquetas para controlar o acesso a chaves do KMS.

11. Selecione os usuários e as funções do IAM que podem administrar a chave de réplica.

    > **Note**
    >
    > As políticas do IAM podem conceder permissão para gerenciar as chaves de réplica a outros usuários e funções do IAM.
    > As práticas recomendadas do IAM não encorajam o uso de usuários do IAM com credenciais de longo prazo. Sempre que possível, use os perfis do IAM, por fornecerem credenciais temporárias. Para obter detalhes, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

    Essa etapa inicia o processo de criação de uma política de chaves para a chave de réplica. O console exibe a política de chaves atual da chave primária, mas é possível alterá-la. Políticas de chaves não são uma propriedade compartilhada de chaves de várias regiões. Você pode fornecer à chave primária de várias regiões e suas réplicas a mesma política de chaves ou políticas de chave diferentes. O AWS KMS não sincroniza políticas de chaves. Você pode alterar a política de chaves de qualquer chave do KMS a qualquer momento.

12. Conclua as etapas para criar a política de chaves, incluindo a seleção de usuários de chaves. Após revisar a política de chaves, escolha Finish (Concluir) para criar a chave de réplica.

Criar uma chave de réplica (API do AWS KMS)

Para criar uma chave de réplica multirregional, use a ReplicateKeyoperação. Você não pode usar a CreateKeyoperação para criar uma chave de réplica. Essa operação cria uma chave de réplica por

vez. A região que você especificar deve estar em conformidade com os Requisitos de região para chaves de réplica.

Ao usar a operação `ReplicateKey`, não especifique valores para propriedades compartilhadas de chaves de várias regiões. Valores de propriedades compartilhadas são copiados da chave primária e mantidos sincronizados. No entanto, é possível especificar valores para propriedades não compartilhadas. De outra forma, o AWS KMS aplicara os valores padrão para chaves do KMS, e não os valores da chave primária.

> **Note**
>
> Se você não especificar valores para os parâmetros `Description`, `KeyPolicy` ou `Tags`, o AWS KMS criará a chave de réplica e uma descrição de string vazia, a política de chave padrão e sem etiquetas.
> Não inclua informações confidenciais ou sigilosas nos campos `Description` ou `Tags`. Esses campos podem aparecer em texto simples em CloudTrail registros e outras saídas.

Por exemplo, o comando a seguir cria uma chave de várias regiões na região Ásia-Pacífico (Sydney) (ap-southeast-2). Essa chave de réplica é modelada na chave primária na região Leste dos EUA (Norte da Virgínia) (us-east-1), identificada pelo valor do parâmetro `KeyId`. Esse exemplo aceita valores padrão para todas as outras propriedades, incluindo a política de chaves.

A resposta descreve a nova chave de réplica. Ela inclui campos para propriedades compartilhadas, como `KeyId`, `KeySpec`, `KeyUsage` e a origem do material de chave (`Origin`). Ela também inclui propriedades que são independentes da chave primária, como `Description`, política de chaves (`ReplicaKeyPolicy`) e etiquetas (`ReplicaTags`).

A resposta também inclui o ARN de chave e a região da chave primária e todas as suas chaves de réplica, incluindo aquela que acabou de ser criada na região ap-southeast-2. Neste exemplo, o elemento `ReplicaKey` mostra que essa chave primária já foi replicada na região 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": []
}
```

Visualizar chaves de várias regiões

Você pode visualizar chaves de região única e chaves de várias regiões no console do AWS KMS e usando operações de API do AWS KMS.

Tópicos

- Visualizar chaves de várias regiões no console
- Visualizar chaves de várias regiões na API

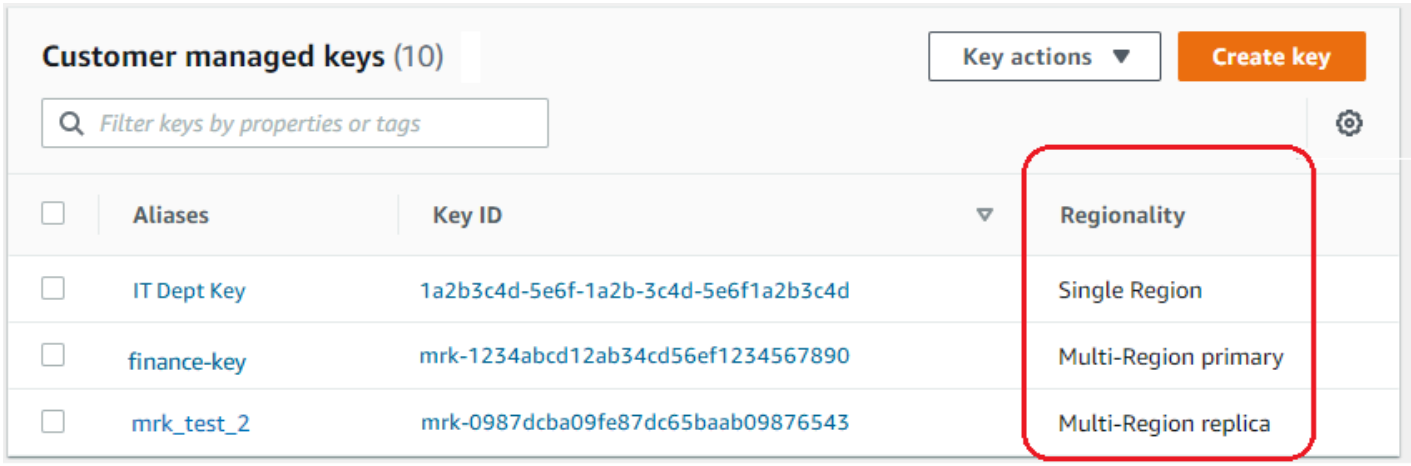
Visualizar chaves de várias regiões no console

No console do AWS KMS, é possível visualizar chaves do KMS na região selecionada. Porém, se você tiver uma chave de várias regiões, poderá ver suas chaves de várias regiões relacionadas em outras Regiões da AWS.

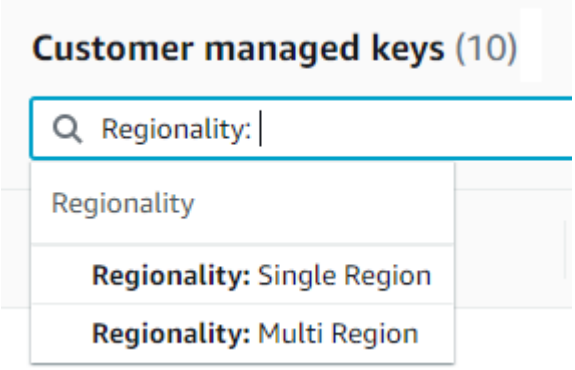
A tabela Customer managed keys (Chaves gerenciadas pelo cliente) no console do AWS KMS mostra apenas as chaves do KMS na região selecionada. É possível visualizar chaves primárias e de réplica de várias regiões na região selecionada. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.

A tabela Chaves gerenciadas pela AWS não tem os recursos de regionalidade porque Chaves gerenciadas pela AWS são sempre chaves de uma única região.

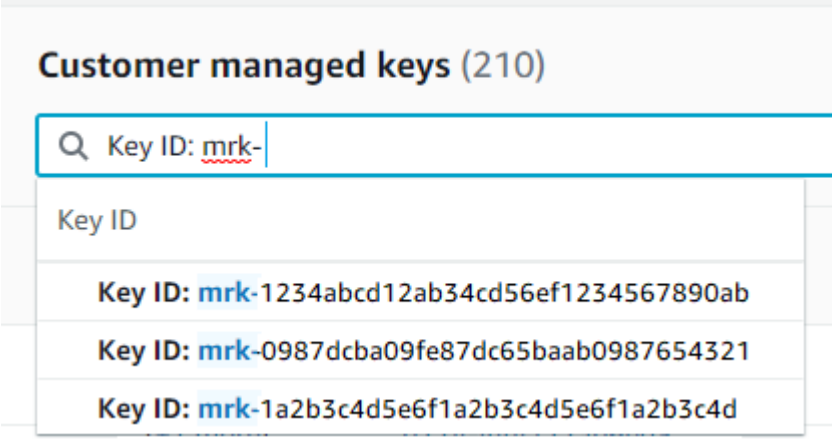
- Para facilitar a identificação das suas chaves de várias regiões, adicione a coluna Regionality (Regionalidade) à sua tabela de chaves. Para obter ajuda, consulte Personalizar suas tabelas de chaves do KMS.



- Para mostrar somente chaves de uma única região ou somente chaves de várias regiões na tabela de chaves, filtre suas chaves pela propriedade Regionality (Regionalidade) de cada chave. Para obter ajuda, consulte Classificar e filtrar as chaves do KMS .



- Também é possível classificar e filtrar a tabela Customer managed keys (Chaves gerenciadas pelo cliente) para o prefixo de ID de chave mrk- distintivo.

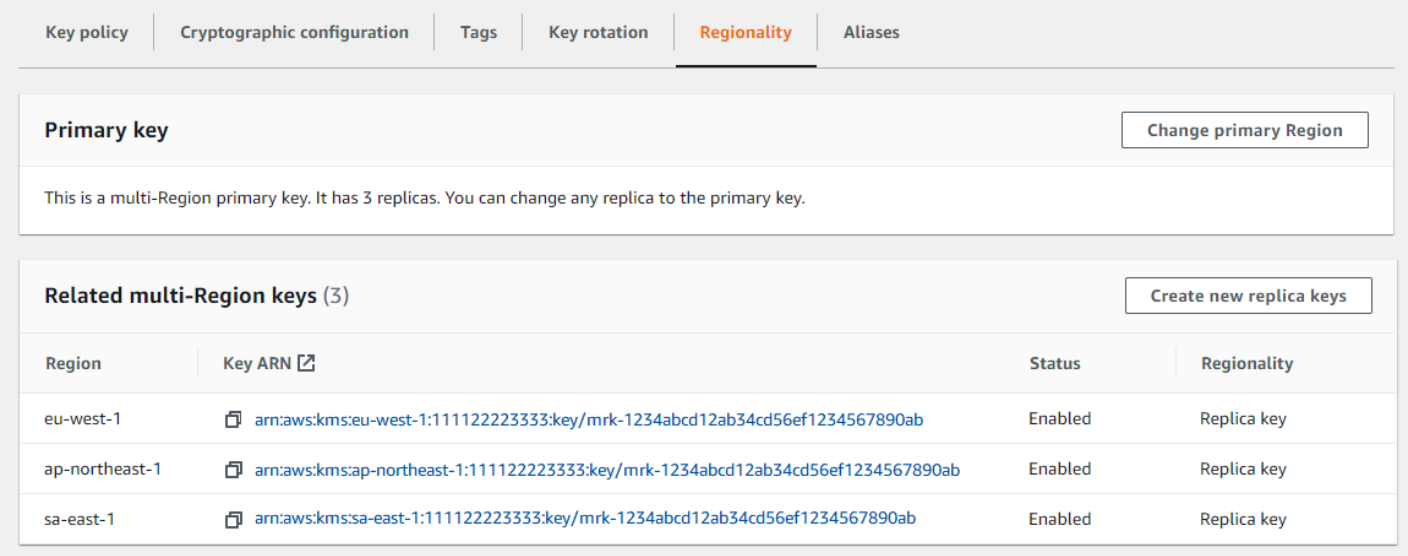


- Para obter detalhes sobre uma chave primária ou uma chave de réplica de várias regiões, acesse a página de detalhes da chave e escolha a guia Regionality (Regionalidade).

  A guia Regionality (Regionalidade) de uma chave primária inclui os botões Change primary Region (Alterar região primária) e Create new replica keys (Criar novas chaves de réplica). (A guia Regionality (Regionalidade) de uma chave de réplica não tem botão.) A seção Related multi-Region keys (Chaves de várias regiões relacionadas) lista todas as chaves de várias regiões relacionadas à atual. Se a chave atual for uma chave de réplica, essa lista incluirá a chave primária.

  Se você escolher uma chave de várias regiões relacionada na lista Related multi-Region keys (Chaves de várias regiões relacionadas), o console do AWS KMS muda para a região da chave selecionada e abrirá a página de detalhes da chave. Por exemplo, se você escolher a chave de

réplica na região `sa-east-1` da seção de exemplo Related multi-Region keys (Chaves de várias regiões relacionadas) abaixo, o console AWS KMS alterará para a região `sa-east-1` a fim de exibir a página de detalhes dessa chave de réplica. Você pode fazer isso para exibir o alias ou a política de chave da chave de réplica. Para alterar novamente a região, use o seletor de região no canto superior direito da página.



Visualizar chaves de várias regiões na API

Para visualizar as chaves multirregionais na AWS KMS API, use a DescribeKeyoperação. Ele exibe a chave especificada e todas as suas chaves de várias regiões relacionadas.

Como o console do AWS KMS, as operações de API do AWS KMS são regionais. Por exemplo, quando você chama as ListAliasesoperações ListKeysou, elas retornam somente os recursos na região atual ou especificada. Porém, quando você chama a operação `DescribeKey` em uma chave de várias regiões, a resposta inclui todas as chaves de várias regiões relacionadas em outras Regiões da AWS.

Por exemplo, a seguinte solicitação `DescribeKey` obtém detalhes sobre uma chave de réplica de várias regiões na região Ásia-Pacífico (Tóquio) (`ap-northeast-1`).

```
$ aws kms describe-key \
        --key-id arn:aws:kms:ap-northeast-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab \
        --region ap-northeast-1
```

A maioria das `KeyMetadata` na resposta descreve a chave de réplica na região Ásia-Pacífico (Tóquio) que é o requerente da solicitação. No entanto, o elemento `MultiRegionConfiguration` descreve a chave primária na região Oeste dos EUA (Oregon) (us-west-2) e suas chaves de réplica em outras Regiões da AWS, incluindo a réplica na região Ásia-Pacífico (Tóquio). O `DescribeKey` retorna o mesmo valor `MultiRegionConfiguration` para todas as chaves de várias regiões relacionadas.


```
{
    "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"
                }
            ]
        }
    }
}
```

Como gerenciar chaves de várias regiões

Para a maioria das ações, você gerencia as chaves de várias regiões da mesma maneira que usa e gerencia as chaves de uma única região. Você pode habilitar e desabilitar as chaves, definir e atualizar aliases, políticas de chaves, concessões e etiquetas. No entanto, o gerenciamento de chaves de várias regiões difere das seguintes maneiras.

- Você pode atualizar a região primária. Isso transforma uma das chaves de réplica para uma chave primária e a chave primária atual em uma réplica.
- Você gerencia a alternância de chaves automática apenas na chave primária.
- Você pode obter a chave pública para uma chave de várias regiões assimétrica de qualquer uma das chaves primárias ou de réplica relacionadas.

A propriedade de várias regiões definida quando uma chave do KMS é criada é imutável. Não é possível converter uma chave de região única em chave de várias regiões nem converter uma chave de várias regiões em uma chave de região única.

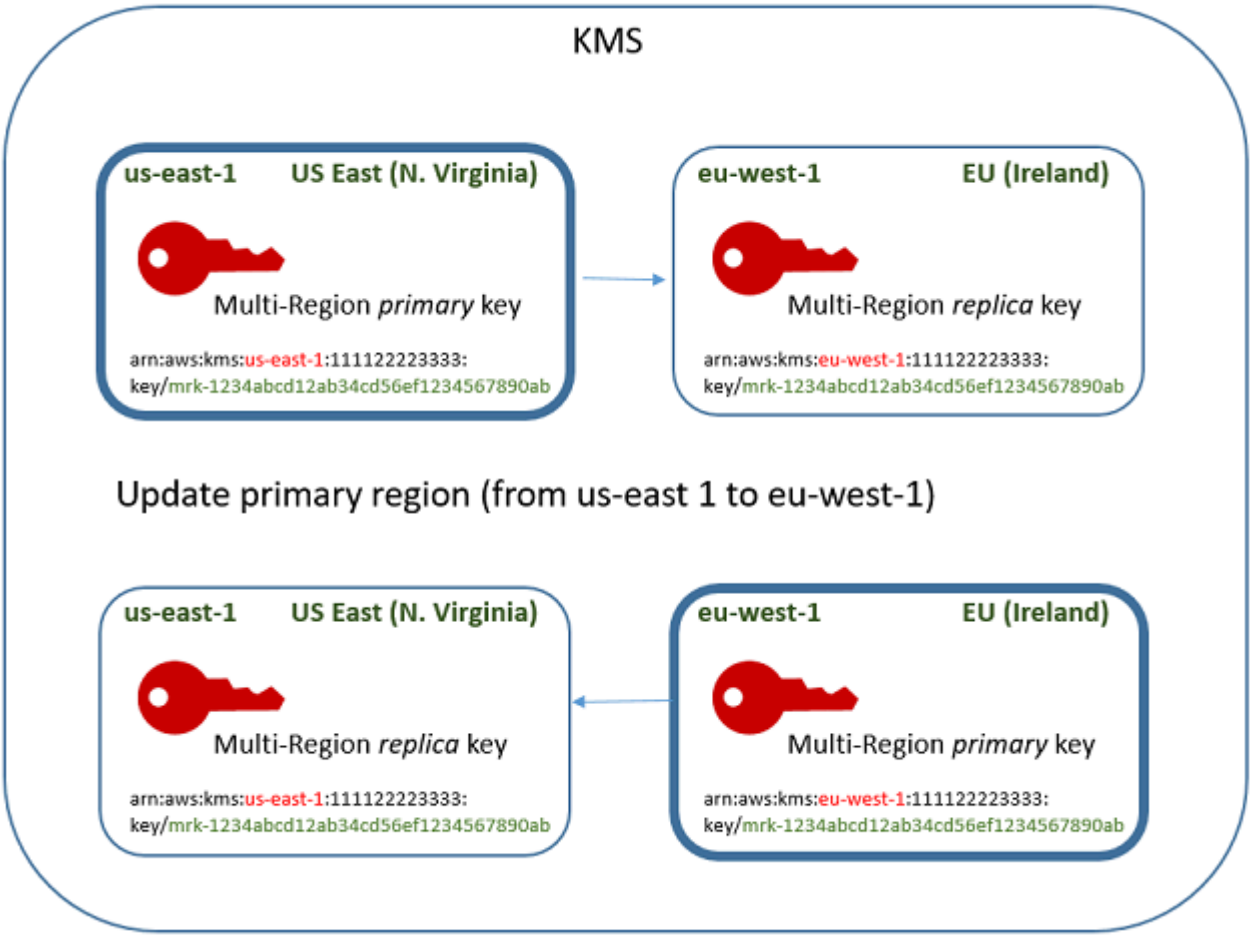
Atualizar a região primária

Todos os conjuntos de chaves de várias regiões relacionadas devem ter uma chave primária. Porém, você pode alterar a chave primária. Esta ação, conhecida como atualizar a região primária, converte a chave primária atual em uma chave de réplica e converte uma das chaves de réplica relacionadas na chave primária. Você pode fazer isso quando precisa excluir a chave primária atual enquanto mantém as chaves de réplica ou para localizar a chave primária na mesma região que seus administradores de chave.

Você pode selecionar qualquer chave de réplica relacionada para ser a nova chave primária. Tanto a chave primária quanto a chave de réplica devem estar no estado de chave `Enabled` quando a operação começar.

Mesmo após a conclusão dessa operação, o processo de atualização da região primária pode permanecer em andamento por mais alguns segundos. Durante esse tempo, as chaves primárias antigas e novas têm um estado de chave transitório Updating (Atualizando). Enquanto o estado de chave é `Updating`, você pode usar as chaves em operações de criptografia, mas não pode replicar a nova chave primária ou realizar certas operações de gerenciamento, como habilitar ou desabilitar essas chaves. Operações como a DescribeKeypodem exibir as chaves primárias antigas e novas como réplicas. O estado de chave `Enabled` será restaurado quando a atualização estiver concluída.

Suponha que você tenha uma chave primária no Leste dos EUA (Norte da Virgínia) (us-east-1) e uma chave de réplica na Europa (Irlanda) (eu-west-1). É possível usar o recurso de atualização para transformar a chave primária na região Leste dos EUA (Norte da Virgínia) (us-east-1) em uma chave de réplica e transformar a chave de réplica na Europa (Irlanda) (eu-west-1) na chave primária.



Quando o processo de atualização for concluído, a chave de várias regiões na região Europa (Irlanda) (eu-west-1) é uma chave primária de várias regiões, enquanto a chave na região Leste dos EUA (Norte da Virgínia) (us-east-1) é sua chave de réplica. Se houver outras chaves de réplica relacionadas, elas se tornarão réplicas da nova chave primária. Na próxima vez que AWS KMS

sincronizar as propriedades compartilhadas das chaves multirregionais, ele obterá as propriedades compartilhadas da nova chave primária e as copiará para suas chaves de réplica, incluindo a chave primária anterior.

A operação de atualização não surte efeito no ARN de chave de chaves de várias regiões. Ela também não surte efeito em propriedades compartilhadas, como material de chave, ou em propriedades independentes, como política de chaves. Porém, talvez você queira Aatualizar a política de chaves da nova chave primária. Por exemplo, talvez você queira adicionar kms:ReplicateKey permission for trust principals à nova chave primária e removê-la da nova chave de réplica.

O estado de chave **`Updating`**

O processo de atualização de uma região primária demora um pouco mais do que o breve atraso de consistência que afeta a maioria das AWS KMS operações. O processo ainda pode estar em andamento após o retorno da operação `UpdatePrimaryRegion` ou depois de você concluir o procedimento de atualização no console. Operações como a DescribeKeypodem exibir as chaves primárias antigas e novas como réplicas até que o processo seja concluído.

Durante o processo de atualização da região primária, a chave primária antiga e a nova chave primária estão no estado de chave `Updating`. Quando o processo de atualização for concluído com êxito, ambas as chaves retornam para o estado de chave `Enabled`. Durante o estado `Updating`, algumas operações de gerenciamento, como habilitar e desabilitar chaves, não estão disponíveis. No entanto, você pode continuar a usar as duas chaves em operações de criptografia sem interrupção. Para obter informações sobre o efeito do estado de chave `Updating`, consulte Principais estados das AWS KMS chaves.

Atualizar uma região primária (console)

Você pode atualizar a chave primária no AWS KMS console. Comece na página de detalhes de chaves da chave primária atual.

1. Faça login no console AWS Management Console e abra o AWS Key Management Service (AWS KMS) em https://console.aws.amazon.com/kms.
2. Para alterar o Região da AWS, use o seletor de região no canto superior direito da página.
3. No painel de navegação, escolha Customer managed keys (Chaves gerenciadas de cliente).
4. Selecione o ID de chave ou alias da chave primária de várias regiões. Isso abre a página de detalhes da chave primária.

Para identificar uma chave primária de várias regiões, use o ícone de ferramenta no canto superior direito para adicionar a coluna Regionality (Regionalidade) à tabela.

5. Escolha a guia Regionality (Regionalidade).
6. Na seção Primary key (Chave primária), escolha Change primary Region (Alterar região primária).
7. Escolha a região da nova chave primária. Você só pode escolher uma região no menu.

   O menu Change primary Regions (Alterar regiões primárias) inclui apenas regiões que têm uma chave de várias regiões relacionada. Você pode não ter permissão para atualizar a região primária em todas as regiões no menu.
8. Escolha Alterar região primária.

Atualização de uma região primária (AWS KMS API)

Para alterar a chave primária em um conjunto de chaves multirregionais relacionadas, use a UpdatePrimaryRegionoperação.

Usar o parâmetro `KeyId` para identificar a chave primária atual. Use o `PrimaryRegion` parâmetro para indicar a Região da AWS da nova chave primária. Se a chave primária ainda não tiver uma réplica na nova região primária, a operação falhará.

O exemplo a seguir altera a chave primária da chave de várias regiões na região `us-west-2` para sua réplica na região `eu-west-1`. O parâmetro `KeyId` identifica a chave primária atual na região `us-west-2`. O `PrimaryRegion` parâmetro especifica a Região da AWS da nova chave primária,`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
```

Quando bem-sucedida, essa operação não retorna saída; apenas o código de status HTTP. Para ver o efeito, chame a DescribeKeyoperação em qualquer uma das teclas multirregionais. Talvez você queira esperar até que o estado da chave volte a ser `Enabled`. Enquanto estado da chave é Updating (Atualizando), os valores da chave ainda podem estar em fluxo.

Por exemplo, a seguinte chamada `DescribeKey` obtém os detalhes sobre a chave de várias regiões na região `eu-west-1`. A saída mostra que a chave de várias regiões na região `eu-west-1` é agora

a chave primária. A chave de várias regiões relacionada (mesma ID de chave) na região `us-west-2` agora é uma chave de réplica.

```
$ 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"
              }
           ]
        }
    }
}
```

Alternância de chaves de várias regiões

Você pode ativar e desativar a rotação automática e realizar a rotação sob demanda do material da chave em chaves multirregionais. A rotação de chaves é uma propriedade compartilhada das chaves multirregionais.

Você habilita e desabilita a alternância automática de chaves somente na chave primária. Você inicia a rotação sob demanda somente na chave primária.

- Quando AWS KMS sincroniza as chaves multirregionais, ele copia a configuração da propriedade de rotação da chave primária para todas as chaves de réplica relacionadas.
- Quando AWS KMS gira o material da chave, ele cria um novo material de chave para a chave primária e, em seguida, copia o novo material de chave além dos limites da região para todas as chaves de réplica relacionadas. O material da chave nunca sai AWS KMS sem criptografia. Essa etapa é cuidadosamente controlada para garantir que o material de chave seja totalmente sincronizado antes que qualquer chave seja usada em uma operação criptográfica.
- AWS KMS não criptografa nenhum dado com o novo material de chave até que esse material esteja disponível na chave primária e em cada uma de suas chaves de réplica.
- Quando você replica uma chave primária que foi alternada, a nova chave de réplica tem o material de chave atual e todas as versões anteriores do material de chave para suas chaves de várias regiões relacionadas.

Esse padrão garante que as chaves de várias regiões relacionadas sejam totalmente interoperáveis. Qualquer chave de várias regiões pode descriptografar qualquer texto cifrado por uma chave de várias regiões relacionada, mesmo que esse texto cifrado tenha sido criptografado antes de a chave ser criada.

A alternância de chaves automática não tem suporte em chaves do KMS assimétricas ou em chaves do KMS com material de chave importado. Para obter informações sobre rotação automática e sob demanda de chaves, consulteGirando AWS KMS keys.

Fazer download de chaves públicas

Ao criar uma chave KMS assimétrica multirregional, AWS KMS cria um par de chaves RSA ou curva elíptica (ECC) para a chave primária. Em seguida, ele copia esse par de chaves para cada réplica da chave primária. Como resultado, é possível baixar a chave pública da chave primária ou de qualquer uma de suas chaves de réplica. Você sempre terá o mesmo material de chave.

Para obter informações sobre como baixar e usar chaves públicas fora do AWS KMS, consulteConsiderações especiais sobre o download de chaves públicas. Para obter instruções, consulte Fazer download de chaves públicas.

Importar material de chave para chaves de várias regiões

É possível importar seu próprio material de chave para chaves KMS de várias regiões. As chaves de várias regiões que você cria com seu próprio material de chave são interoperáveis. Você pode criptografar dados em uma região e descriptografá-los em qualquer outra região com uma chave de várias regiões relacionada.

No entanto, você deve gerenciar o material de chave.

- O AWS KMS não copia nem sincroniza o material de chave de uma chave primária que contém material de chave importado com suas chaves de réplica. É necessário importar o mesmo material de chave para chaves primárias e de réplica relacionadas.
- Defina o modelo de validade e as datas de validade para cada chave independentemente ao importar o material de chave. É possível configurar o mesmo modelo de validade e datas de validade diferentes para chaves de várias regiões relacionadas. Se o material de chave se aproximar da data de validade, você deverá reimportá-lo para a chave de várias regiões afetada.

  Os estados chave das chaves de várias regiões relacionadas são independentes uns dos outros. Por exemplo, se o material de chave na chave primária expirar, suas chaves de réplica não serão afetadas.

Os mesmos Requisitos de região para chaves de réplica aplicam-se a chaves de várias regiões com material de chave importado. Se você importar o mesmo material de chave para chaves de região única ou chaves de várias regiões não relacionadas, essas chaves do KMS não serão interoperáveis.

É possível criar chaves de várias regiões com material de chave importado simétrico, assimétrico ou HMAC. O AWS KMS não é compatível com material de chave importado em repositórios de chaves personalizados. Além disso, não é possível habilitar a alternância automática de chaves de qualquer chave do KMS com material de chave importado.

Com exceção de seus recursos de várias regiões, chaves de várias regiões com material de chave importado são as mesmas que outras chaves do KMS com material de chave importado. Para obter informações detalhadas sobre como criar e configurar chaves de uma única região com material de chave importado, consulte Sobre o material de chave importada.

Tópicos

- Por que nem todas as chaves do KMS com material de chave importado são interoperáveis?
- Criar uma chave primária com material de chave importado
- Criar uma chave de réplica com material de chave importado

Por que nem todas as chaves do KMS com material de chave importado são interoperáveis?

As chaves do KMS de região única com material de chave importado não são interoperáveis, mesmo quando possuem o mesmo material de chave. Quando o AWS KMS usa uma chave do KMS para criptografar dados, ele vincula criptograficamente alguns dos metadados de chave ao texto cifrado. Isso protege o texto cifrado, para que somente a chave do KMS que criptografou os dados possa descriptografá-los.

Chaves de várias regiões foram projetadas para serem interoperáveis. Além de terem o mesmo material de chave, elas têm o mesmo ID de chave e outros metadados. Assim, os textos cifrados que elas geram podem ser descriptografados por qualquer chave de várias regiões relacionada. Como resultado, as propriedades de confiança de chaves de várias regiões são diferentes das de chaves de uma única região. Porém, para alguns clientes, o benefício da descriptografia em várias regiões supera o valor de segurança de um texto cifrado dependente de uma única chave do KMS em uma única Região da AWS.

Criar uma chave primária com material de chave importado

Para criar uma chave primária com material de chave importado, comece criando uma chave do KMS sem material de chave. Ao criar a chave primária sem material de chave, você deve especificar a especificação da chave que reflete o tipo de material de chave que você planeja importar. Em seguida, importe o material de chave para a chave primária.

O procedimento para criar uma chave primária de várias regiões sem material de chave é quase o mesmo que o procedimento para criar uma chave de região única sem material de chave. A única diferença é que você especifica que a chave é uma chave de várias regiões.

As permissões para criar uma chave primária multirregional com material de chave importado são as mesmas necessárias para criar uma chave primária multirregional com material de AWS KMS chave, incluindo as CreateServiceLinkedRole permissões kms: CreateKey e iam: em uma política do IAM. Você pode usar as chaves de KeyOrigin condição kms: MultiRegionKeyType e kms: para permitir ou negar permissão para criar chaves primárias multirregionais com material de chave importado.

Ao criar uma chave primária com material de chave importado no console do AWS KMS, use as configurações na seção Advanced options (Opções avançadas). Não é possível alterar essas propriedades depois que a chave do KMS é criada.

- Defina Key material origin (Origem do material-chave) como External (Import key material) (Externa [Importar material-chave]).
- Defina Multi-Region replication (Replicação em várias regiões) como Allow this key to be replicated into other Regions (Permitir que esta chave seja replicada em outras regiões).

Ao usar a CreateKeyoperação para criar uma chave primária com material de chave importado, use os `MultiRegion` parâmetros `Origin` e e especifique o `KeySpec` e `KeyUsage` o. O exemplo a seguir cria uma chave `EXTERNAL` do KMS que pode importar material de chaves `ECC_NIST_P384`.

```
$ aws kms create-key --origin EXTERNAL --key-spec ECC_NIST_P384 --key-usage SIGN_VERIFY
 --multi-region
```

O resultado é uma chave primária de várias regiões sem material de chave e um estado de chave `PendingImport`.

Para habilitar essa chave do KMS, baixe uma chave pública e um token de importação, use a chave pública para criptografar seu material de chaves e, em seguida, importe seu material de chaves. Para obter instruções, consulte Importação de material chave para AWS KMS chaves.

Criar uma chave de réplica com material de chave importado

Você pode criar uma chave de réplica de várias regiões no console do AWS KMS ou usando as operações de API do AWS KMS. Para replicar uma chave primária de várias regiões com material de chave importado, use o mesmo procedimento usado para criar uma chave de réplica com material de chave do AWS KMS. Porém, o resultado é diferente. Em vez de retornar uma chave de réplica com o mesmo material de chave que a chave primária, o processo de replicação retorna uma chave de réplica sem material de chave e um estado de chave de `PendingImport`. Para habilitar a chave de réplica, você deve importar o mesmo material de chave para a chave de réplica importada para sua chave primária.

Embora ele não replique o material de chave, o AWS KMS cria a chave de réplica com o mesmo ID de chave, especificação de chave, uso de chave e origem de material de chave que a chave primária. Ele também garante que o material de chave importado para a chave de réplica seja idêntico ao material de chave importado para a chave primária.

Para criar uma chave de réplica com material de chave importado:

1. Crie uma chave primária de várias regiões com material de chave importado.
2. Faça uma das coisas a seguir.

   No console do AWS KMS, escolha uma chave primária de várias regiões com material de chave importado. Em seguida, na guia Regionality (Regionalidade), selecione Create new replica keys (Criar novas chaves de réplica). Para obter instruções, consulte Criar chaves de réplica (console).

   Ou use a ReplicateKeyoperação. Para o parâmetro `KeyId`, insira o ID da chave ou o ARN da chave de uma chave primária de várias regiões com material de chave importado. Para obter instruções, consulte Criar uma chave de réplica (API do AWS KMS).
3. Para cada nova chave de réplica, siga as etapas para baixar uma chave pública e um token de importação. Use a chave pública para criptografar o material da chave primária e, em seguida, importe esse material para a chave de réplica. É necessário ter uma chave pública e um token de importação diferentes para cada chave de réplica.

   Se o material de chave que você tentar importar para a chave de réplica não for o mesmo material de chave da sua chave primária, a operação falhará. O AWS KMS não exige que o modelo de validade e as datas de validade sejam coordenados, mas você pode estabelecer regras de negócios para suas chaves de várias regiões. Para obter instruções, consulte Importação de material chave para AWS KMS chaves.

Permissões para replicar chaves com materiais de chave importado

Para criar uma chave de réplica com material de chaves importado, você deve ter as permissões a seguir.

Na região da chave primária:

- kms: ReplicateKey na chave primária (na região da chave primária). Inclua essa permissão na política de chave primária ou em uma política do IAM.

Na região da chave de réplica:

- kms: CreateKey em uma política do IAM.
- kms: GetParametersForImport. Essa permissão pode ser incluída na política de chaves da chave de réplica ou em uma política do IAM.

- kms: ImportKeyMaterial. Essa permissão pode ser incluída na política de chaves da chave de réplica ou em uma política do IAM.
- kms: TagResource é necessário para atribuir tags durante a replicação. Inclua essa permissão em uma política do IAM na região da réplica.
- kms: CreateAlias é necessário para replicar uma chave no AWS KMS console. Para obter mais detalhes, consulte Controlar o acesso a aliases.

Excluir chaves de várias regiões

Quando não estiver mais usando uma chave primária de várias regiões ou uma chave de réplica, você pode programar sua exclusão.

Embora a exclusão de chaves do KMS sempre deva ser feita com cautela, excluir uma réplica de uma chave de várias regiões é uma operação menos arriscada, desde que a chave primária ainda exista no AWS KMS. Se você excluir uma chave de réplica da sua região, mas descobrir texto cifrado que foi criptografado com a chave excluída, poderá descriptografar esse texto cifrado com qualquer chave de várias regiões relacionada. Também é possível recriar a chave de réplica, replicando a chave primária novamente na região da chave de réplica.

No entanto, excluir uma chave primária e todas as suas chaves de réplica é uma operação muito perigosa, equivalente a excluir uma chave de região única.

> **Warning**
>
> Excluir uma chave do KMS é um processo destrutivo e potencialmente perigoso. Prossiga somente quando você tiver certeza de que não vai precisar mais usar a chave do KMS futuramente. Caso não tenha certeza, desabilite a chave do KMS em vez de excluí-la.

Para excluir uma chave primária, exclua primeiro todas as chaves de réplica. Se você precisar excluir uma chave primária de uma determinada região sem excluir suas chaves de réplica, transforme a chave primária em uma chave de réplica atualizando a região primária.

Antes de agendar a exclusão de qualquer chave KMS, revise os cuidados no Excluir AWS KMS keys tópico e os tópicos que explicam como determinar o uso anterior de uma chave KMS e como definir um CloudWatch alarme que alerta você sobre o uso da chave KMS durante o período de espera. Antes de excluir a chave primária de uma chave assimétrica de várias regiões, reveja o tópico Excluir chaves assimétricas.

Tópicos

- Permissões para excluir chaves de várias regiões
- Como excluir uma chave de réplica
- Como excluir uma chave primária

Permissões para excluir chaves de várias regiões

Para programar a exclusão de uma chave de várias regiões, você precisa apenas da seguinte permissão.

- kms: ScheduleKeyDeletion — para agendar a exclusão da chave multirregional e definir seu período de espera.

Também é altamente recomendável que você tenha as seguintes permissões relacionadas.

- kms: CancelKeyDeletion — para cancelar a exclusão programada da chave multirregional.
- kms: DescribeKey — para visualizar o estado da chave multirregional e a lista de chaves multirregionais relacionadas.
- kms: DisableKey — para oferecer a opção de desativar uma chave multirregional em vez de excluí-la.
- kms: EnableKey — para restaurar a funcionalidade de uma chave multirregional após cancelar sua exclusão.

Você também pode incluir permissão para replicar a chave primária e alterar a chave primária.

- kms: ReplicateKey
- kms: UpdateReplicaRegion

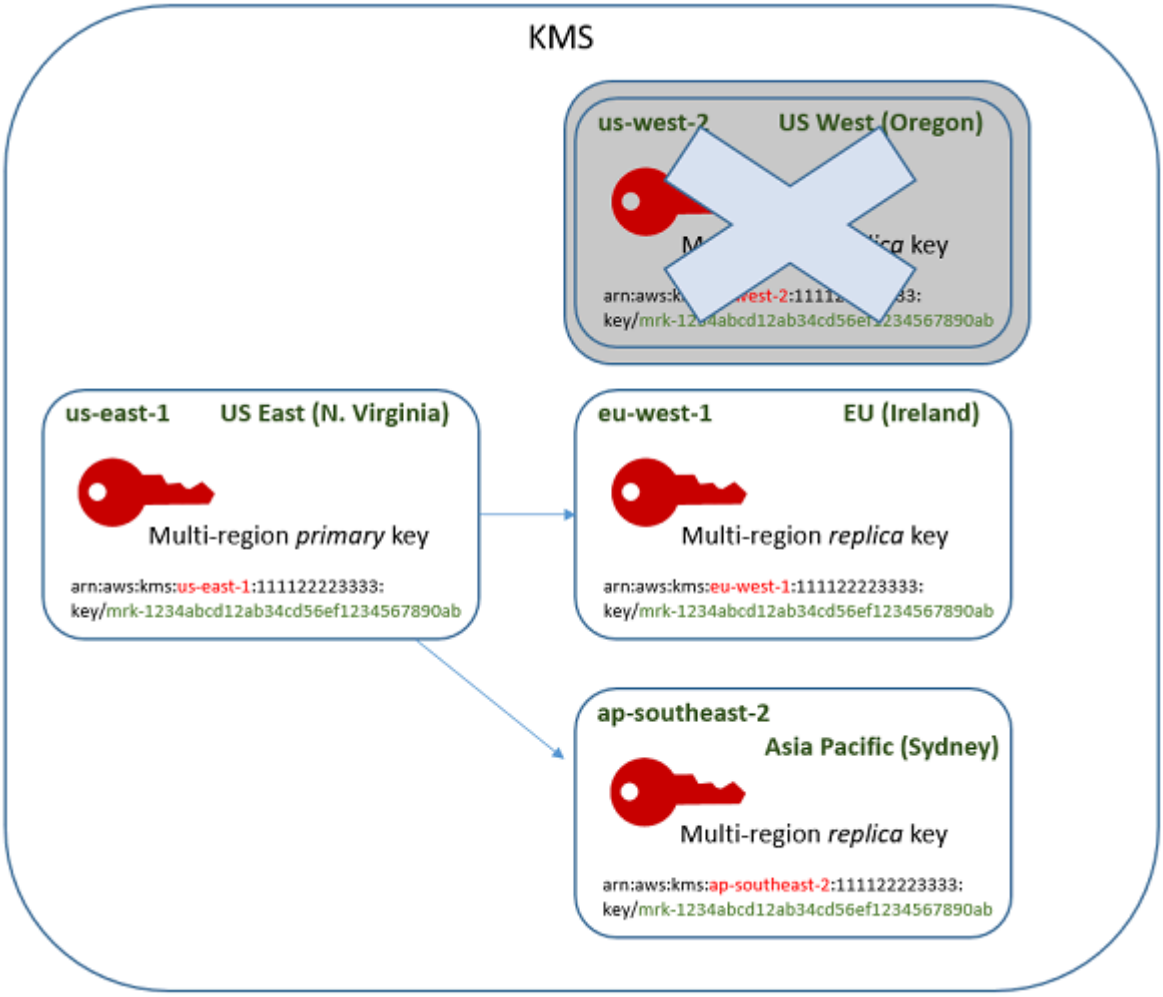
É possível incluir essas permissões em uma política do IAM, mas a prática recomendada é colocá-las em uma política de chaves na qual elas se apliquem somente à chave do KMS que você precisa gerenciar.

Como excluir uma chave de réplica

Use o console do AWS KMS ou a API do AWS KMS para excluir um chave de réplica. É possível excluir uma chave de réplica a qualquer momento. Ele não depende do estado da chave de qualquer outra chave do KMS.

Se você excluir uma chave de réplica por engano, poderá recriá-la replicando a mesma chave primária na mesma região. A nova chave de réplica que você criar terá as mesmas propriedades compartilhadas do que a chave de réplica original.

O procedimento para excluir uma chave de réplica de várias regiões é o mesmo que o para excluir uma chave de região única.



1. Programe a exclusão da chave de réplica. Selecione um período de espera de 7 a 30 dias. O período de espera padrão é de 30 dias.

2. Durante o período de espera, o estado de chave da chave de réplica muda para `Pending deletion` (`PendingDeletion`), e você não pode usá-la em operações de criptografia.
3. Você pode cancelar a exclusão programada da chave de réplica a qualquer momento durante o período de espera. O estado da chave é alterado para `Disabled`, mas você podereabilitar a chave do KMS.
4. Quando o período de espera expirar, o AWS KMS exclui a chave de réplica.

Você pode exibir um registro das suas ações no log do AWS CloudTrail. O AWS KMS registra as operações que programam a exclusão da chave do KMS e a ação que exclui a chave do KMS.

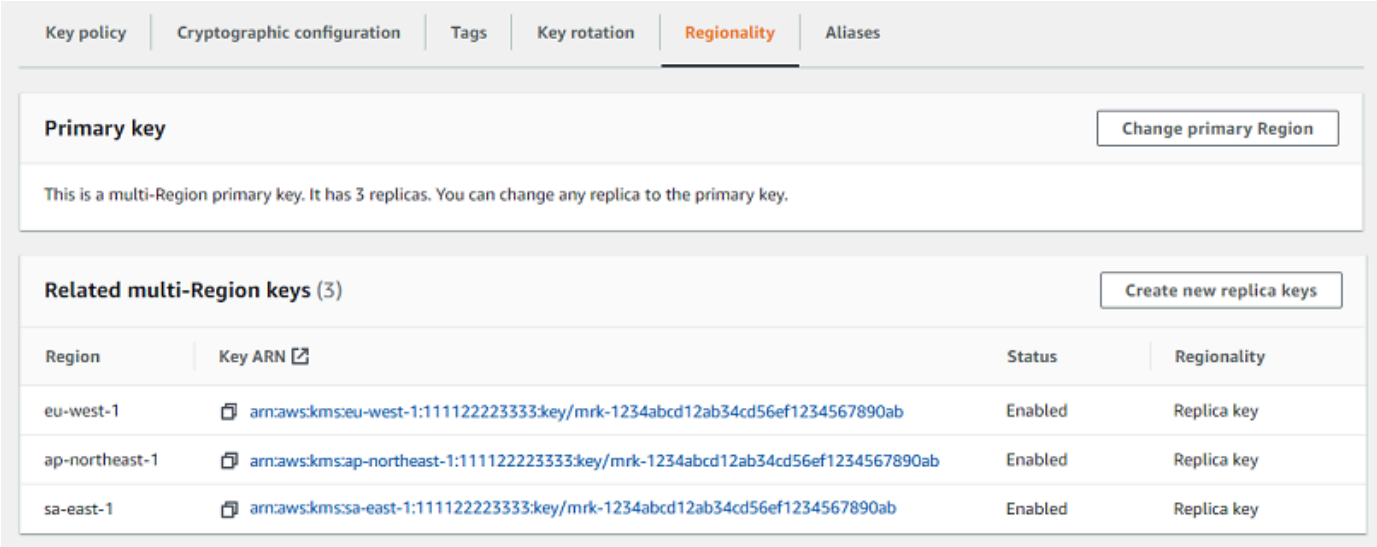
Excluindo uma chave de réplica (console)

Para programar a exclusão de uma chave de réplica de várias regiões, use o mesmo procedimento que você usa para programar a exclusão de uma chave de região única.

Como as chaves de réplica relacionadas estão em diferentes Regiões da AWS, você não pode programar a exclusão de mais de uma chave de réplica por vez. Para excluir todas as chaves de réplica relacionadas, use um padrão como o seguinte.

Para programar a exclusão de todas as chaves de réplica relacionadas

1. Faça login no AWS Management Console e abra o console do AWS Key Management Service (AWS KMS) em https://console.aws.amazon.com/kms.
2. No painel de navegação, escolha Customer managed keys (Chaves gerenciadas de cliente).
3. Use o seletor de região no canto superior direito para escolher a região da chave primária de várias regiões.
4. Escolha seu alias ou ID de chave primária.
5. Escolha a guia Regionality (Regionalidade).



6. Na seção Related multi-Region keys (Chaves de várias regiões relacionadas), escolha o ARN de chave de uma chave de réplica.

   Essa ação abre a página de detalhes da chave da réplica em uma nova guia do navegador. O console está definido para a região da chave de réplica.

7. No menu Key actions (Ações de chave), escolha Schedule key deletion (Programar exclusão de chaves).

   Essa ação inicia o processo de programação de exclusão da chave. Conclua o processo de programação de exclusão da chave. Para obter mais detalhes, consulte Programar e cancelar a exclusão de chaves (console).

8. Retorne para a guia do navegador que exibe a guia Regionality (Regionalidade) da chave primária. (Talvez seja necessário atualizar a página para ver o status atualizado das chaves de réplica.) Escolha o ARN de chave de outra chave de réplica e repita o processo de programação da exclusão da chave de réplica.

Excluir uma chave de réplica (API do AWS KMS)

Para agendar a exclusão de uma chave de réplica multirregional, use a operação. ScheduleKeyDeletion Para especificar a chave do KMS, use seu ID de chave ou ARN de chave. Ao trabalhar com chaves de várias regiões, você pode reduzir a incidência de erros usando o ARN da chave com seu valor de região explícito.

Por exemplo, esse comando exclui uma chave de réplica da região us-west-2 (Oeste dos EUA (Oregon)). Como o comando não especifica um período de espera, este é definido como o padrão de 30 dias.

```
$ aws kms schedule-key-deletion \
    --region us-west-2 \
    --key-id arn:aws:kms:us-west-2:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab
```

Quando o comando é bem-sucedido, ele retorna o ARN de chave (`KeyId`), o período de espera (`PendingWindowInDays`), a data de exclusão (`DeletionDate`) e o estado de chave atual (`KeyState`), que espera-se ser `PendingDeletion`.

Ao excluir uma chave de réplica de várias regiões, verifique se os valores de ID de chave e região no ARN de chave são os esperados.

```
{
    "KeyId": "arn:aws:kms:us-west-2:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
    "DeletionDate": 1599523200.0,
    "KeyState": "PendingDeletion",
    "PendingWindowInDays": 30
}
```

Para excluir todas as réplicas de uma chave primária de várias regiões programaticamente, crie uma lista das regiões que contêm chaves de réplica. Em seguida, para cada região na lista, chame a operação `ScheduleKeyDeletion`, como mostrado acima.

Ao contrário de uma chave de região única que é permanentemente excluída, você pode restaurar uma chave de réplica ao replicar a chave primária na região em que a chave de réplica excluída estava localizada.

Para verificar o status da chave de réplica e visualizar a chave primária e as chaves de réplica de uma chave multirregional, use a operação. DescribeKey

Como excluir uma chave primária

Você pode programar a exclusão de uma chave primária de várias regiões a qualquer momento. No entanto, o AWS KMS não excluirá uma chave primária de várias regiões com chaves de réplica, mesmo que estejam programadas para exclusão.

Para excluir uma chave primária, você deve programar a exclusão de todas as chaves de réplica e, em seguida, aguardar até que as chaves de réplica sejam excluídas. O período de espera necessário para excluir uma chave primária começa quando a última de suas chaves de réplica é excluída. Se você precisar excluir uma chave primária de uma determinada região sem excluir suas chaves de réplica, transforme a chave primária em uma chave de réplica atualizando a região primária.

Se uma chave primária não tiver chaves de réplica, o processo será idêntico à exclusão de uma chave de réplica ou à exclusão de qualquer chave do KMS regional.

Enquanto uma chave primária estiver programada para exclusão, não será possível usá-la em operações de criptografia e não será possível replicá-la. No entanto, a menos que também estejam programadas para exclusão, suas chaves de réplica não serão afetadas.

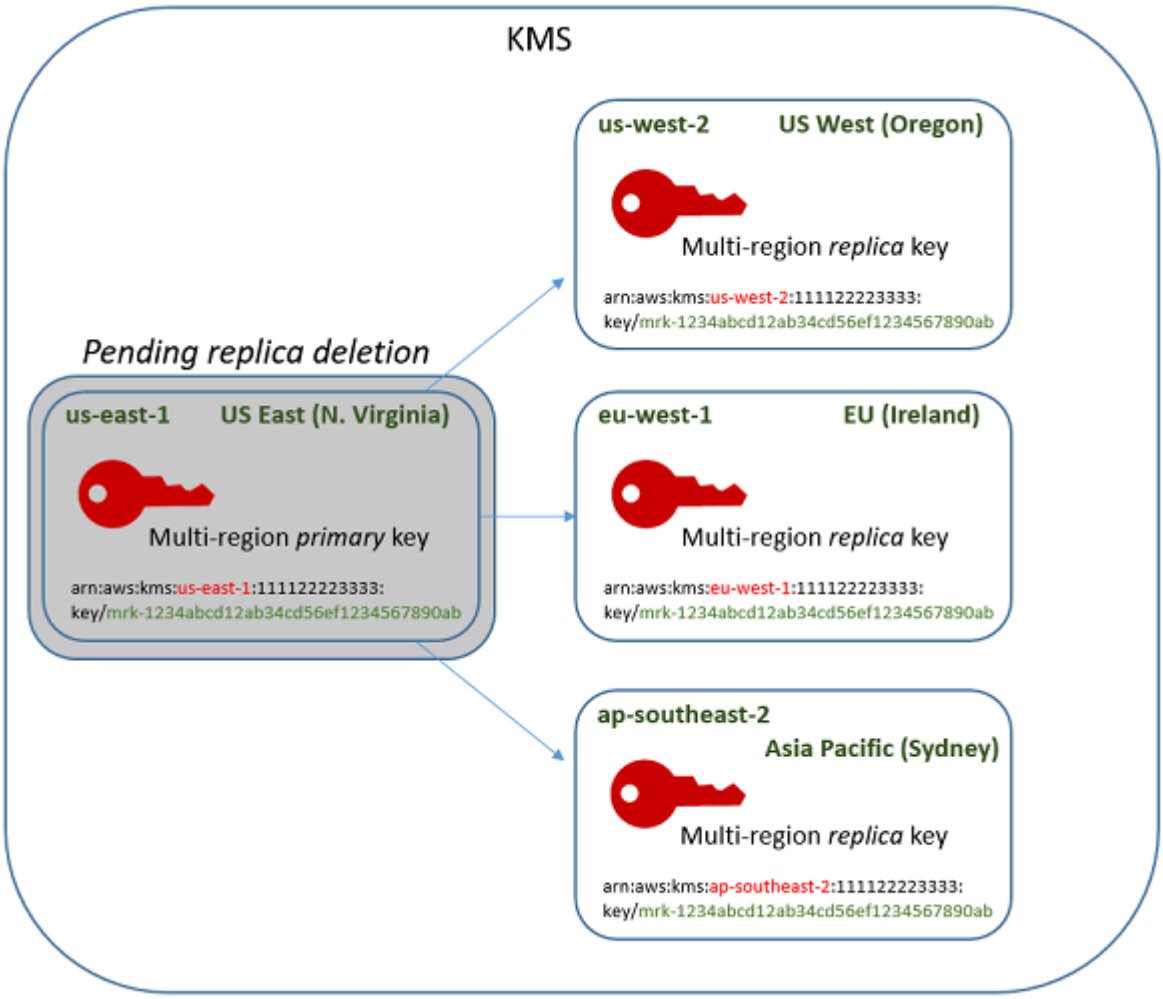
Você pode usar o console do AWS KMS ou a API do AWS KMS para programar a exclusão de chaves primárias e de réplica. Você pode programar a exclusão da chave primária antes, depois ou ao mesmo tempo que programar a exclusão das chaves de réplica. O processo pode ser parecido com o seguinte.

1. Programe a exclusão da chave primária. Selecione um período de espera de 7 a 30 dias. O período de espera padrão é de 30 dias. No entanto, o período de espera para a chave primária não começará até que todas as chaves de réplica sejam excluídas.

   Se ainda existirem chaves de réplica, o estado de chave da chave primária mudará para `Pending replica deletion` (`PendingReplicaDeletion`). Caso contrário, ele será alterado para `Pending deletion`(`PendingDeletion`). Em ambos os casos, você não pode usar a chave primária em operações de criptografia e não pode replicá-la.

   Programar a exclusão de uma chave primária não afeta as chaves de réplica. Seu estado de chave permanece habilitado, e você pode usá-las em operações de criptografia. Se as chaves de réplica não forem excluídas, o `Pending replica deletion` estado da chave primária poderá persistir indefinidamente.

```
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. Programar a exclusão de cada chave de réplica. Selecione um período de espera de 7 a 30 dias. O período de espera padrão é de 30 dias. Você pode excluir várias chaves de réplica ao mesmo tempo. Seus períodos de espera são executados simultaneamente. Durante o período de espera, o estado da chave das chaves de réplica muda para `Pending deletion` (`PendingDeletion`), e você não pode usar essas chaves do KMS em operações de criptografia.

   Por exemplo, se você tiver três chaves de réplica, poderá programar a exclusão de todas as três ao mesmo tempo. Elas podem ter períodos de espera iguais ou diferentes. Observe que o período de espera na chave primária ainda não começou. Seu estado chave é `PendingReplicaDeletion` porque tem chaves de réplica existentes.

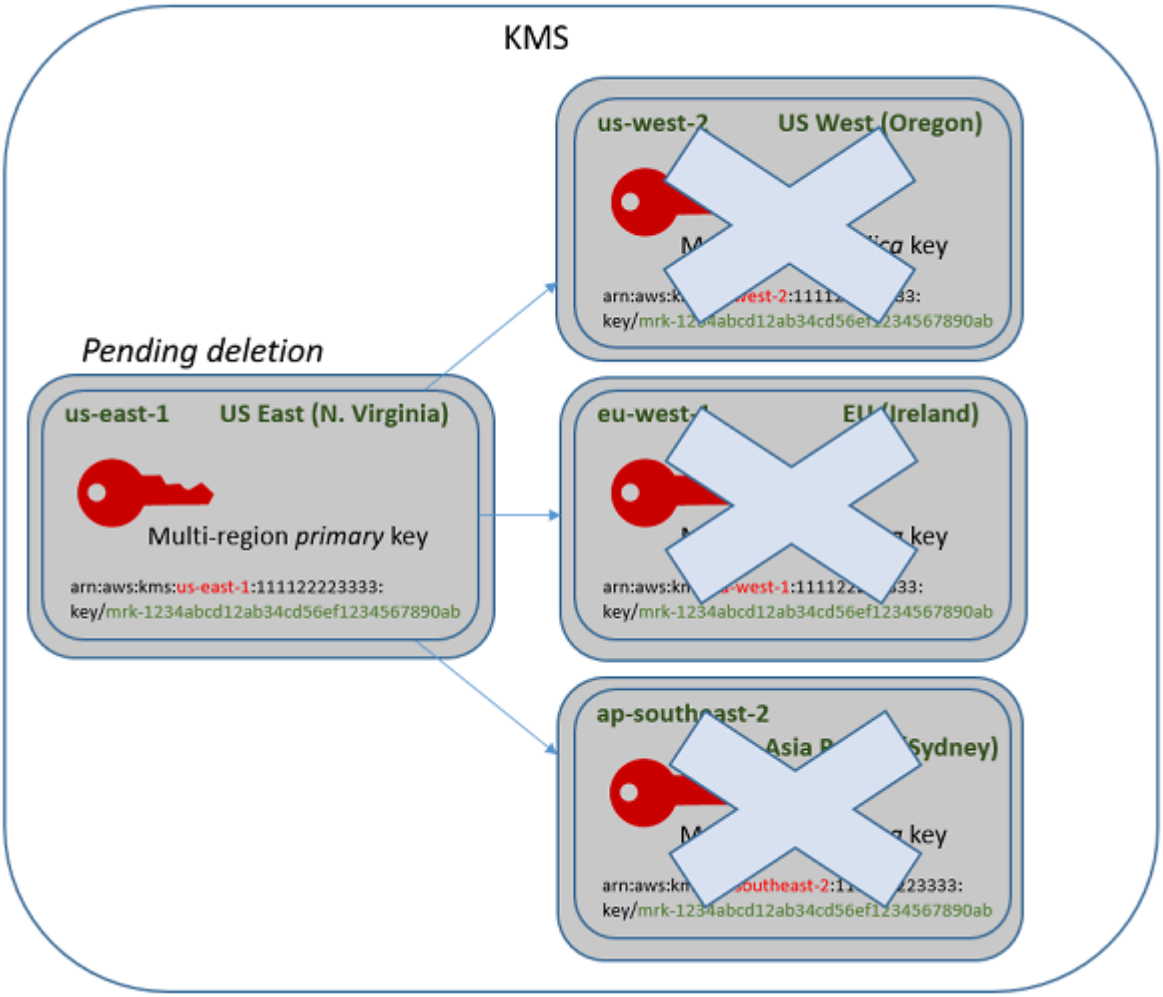
```
KMS key:                    Key state:
Primary key (us-east-1)       Pending replica deletion (waiting period 30 days -- not
 started)
Replica (us-west-2)           Pending deletion (7 days)
```

```
Replica (eu-west-1)           Pending deletion (7 days)
Replica (ap-southeast-2)      Pending deletion (30 days)
```

3. Você pode cancelar a exclusão programada da chave primária ou de qualquer chave de réplica até que ela seja excluída. O estado da chave é alterado para `Disabled`, mas você pode reabilitar a chave do KMS.

4. Quando o período de espera da última chave de réplica expirar, o AWS KMS excluirá a última chave de réplica. O estado da chave primária muda de `Pending replica deletion` (`PendingReplicaDeletion`) para `Pending deletion` (`PendingDeletion`), e o período de espera de 7 a 30 dias para a chave primária começa.

```
KMS key:                    Key state:
Primary key (us-east-1)       Pending deletion (waiting period 30 days)
```



5. Quando o período de espera expirar, o AWS KMS excluirá a chave primária.

O tempo mínimo para excluir uma chave primária com réplicas é de 14 dias.

Se você programar a exclusão da chave primária e de todas as chaves de réplica com um período de espera de 7 dias, as chaves de réplica serão excluídas após 7 dias. A chave primária é excluída no dia 14.

- Dia 1: Programe a exclusão das chaves primárias e de réplica com o período de espera mínimo de 7 dias. Os períodos de espera de exclusão de 7 dias para as chaves de réplica são iniciados. O período de espera de exclusão para a chave primária ainda não é iniciado.
- Dia 7: Os períodos de espera de exclusão para as chaves de réplica terminam. O AWS KMS exclui todas as chaves de réplica. Quando a última chave de réplica é excluída, o período de espera de exclusão de 7 dias para a chave primária é iniciado.
- Dia 14: O período de espera de exclusão para a chave primária termina. O AWS KMS exclui a chave primária.

Você pode exibir um registro das suas ações no log do AWS CloudTrail. O AWS KMS registra as operações que programam a exclusão de cada chave do KMS e a ação que exclui a chave do KMS.

Excluir uma chave primária (console)

Para excluir uma chave primária de várias regiões, use o procedimento a seguir.

Para programar a exclusão de chaves

1. Faça login no AWS Management Console e abra o console do AWS Key Management Service (AWS KMS) em https://console.aws.amazon.com/kms.
2. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.
3. No painel de navegação, escolha Customer managed keys (Chaves gerenciadas pelo cliente).
4. Marque a caixa de seleção ao lado da chave que você deseja excluir. Você também pode selecionar uma ou mais chaves do KMS, incluindo as réplicas dessa chave primária.
5. Escolha Key actions (Ações de chave), Schedule key deletion (Programar exclusão da chave).
6. Leia e considere o aviso e as informações sobre o cancelamento e a exclusão durante o período de espera. Se você decidir cancelar a exclusão, escolha Cancel (Cancelar).
7. Para Waiting period (in days) (Período de espera (em dias)), digite um número de dias entre 7 e 30. Se você selecionou várias chaves do KMS, o período de espera escolhido será aplicado a todas as chaves do KMS selecionadas. O período de espera para chaves de réplica é executado

simultaneamente, mas o período de espera para a chave primária não começará até o AWS KMS excluir a última das chaves de réplica.

8. Marque a caixa de seleção ao lado de Confirm that you want to delete this key in ***<number of days>*** days (Confirme que você deseja excluir esta chave em <número de dias> dias).
9. Escolha Schedule deletion.

Para conferir expio status de exclusão das suas chaves do KMS, na página de detalhes da chave primária, consulte a seção General configuration (Configuração geral). O estado da chave será exibido no campo Status. Quando o estado da chave primária mudar para `Pending deletion`, a Scheduled deletion date (Data de exclusão programada) será exibida.

Você também pode conferir o estado da chave (Status) de todas as chaves primárias e de réplica na guia Regionality (Regionalidade) da página de detalhes para qualquer chave de várias regiões. Para obter mais detalhes, consulte Visualizar chaves de várias regiões.

Excluir uma chave primária (API do AWS KMS)

Para excluir uma chave de réplica multirregional, use a ScheduleKeyDeletionoperação. Para especificar a chave do KMS, use seu ID de chave ou ARN de chave. Ao trabalhar com chaves de várias regiões, você pode reduzir a incidência de erros usando o ARN da chave com seu valor de região explícito.

Por exemplo, esse comando exclui uma chave primária da região us-east-1 (Leste dos EUA (Norte da Virgínia)). Como o comando não especifica um período de espera, este é definido como o padrão de 30 dias.

```
$ aws kms schedule-key-deletion \
    --key-id arn:aws:kms:us-east-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab
```

Quando o comando é bem-sucedido, ele retorna o ARN da chave, o estado de chave resultante e o período de espera (`PendingWindowInDays`).

Se a chave primária não tiver réplicas, o estado da chave primária será `PendingDeletion`, e a saída inclui o campo `DeletionDate`. Se as chaves de réplica permanecerem, o estado da chave primária será `PendingReplicaDeletion` e `DeletionDate` será omitido porque é incerto. Mesmo que as chaves de réplica também estejam programadas para exclusão, você poderá cancelar a exclusão programada.

Ao excluir uma chave primária de várias regiões, verifique se os valores de ID de chave e região no ARN de chave são os esperados.

```
{
    "KeyId": "arn:aws:kms:us-east-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
    "KeyState": "PendingReplicaDeletion",
    "PendingWindowInDays": 30
}
```

Para verificar o status de exclusão de suas chaves KMS, use a DescribeKeyoperação na chave primária ou em qualquer chave de réplica restante. O relógio do período de espera para a chave primária não é iniciado até que a última réplica seja excluída e o estado da chave mude para `PendingDeletion`.

Para calcular a data de exclusão esperada da chave primária, percorra os ARNs da chave de réplica na resposta, execute `DescribeKey` em cada uma, obtenha o valor mais recente de `DeletionDate` e, em seguida, adicione o valor de `PendingDeletionWindowInDays` para a chave primária. Os períodos de espera para as chaves de réplica correm simultaneamente.

No exemplo a seguir, a chave do KMS é uma chave primária de várias regiões com chaves de réplica existentes. Como o estado da chave é `PendingReplicaDeletion`, a resposta inclui o período de espera (`PendingWindowInDays`), mas não a `DeletionDate`. A data de exclusão real da chave primária depende de quando as chaves de réplica são excluídas.

```
$ 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 todas as réplicas são excluídas, a saída `DescribeKey` mostra a chave primária restante com um estado de chave `PendingDeletion`. Enquanto o estado da chave é `PendingDeletion`, o campo `DeletionDate` aparece no lugar do campo `PendingWindowInDays`.

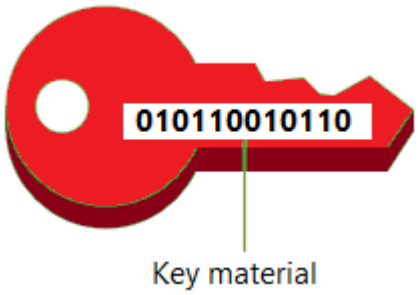
```
$ aws kms describe-key \
    --key-id arn:aws:kms:us-east-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab
```

```
{
    "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": []
        }
    }
}
```

Importação de material chave para AWS KMS chaves

É possível criar uma AWS KMS keys (chave do KMS) com material de chave que você fornece.

Uma chave do KMS é uma representação lógica de uma chave de criptografia. Os metadados de uma chave do KMS incluem o ID do material de chave usado para criptografar e descriptografar dados. Quando você cria uma chave do KMS, por padrão, o AWS KMS gera o material de chave para essa chave do KMS. No entanto, você pode criar uma chave do KMS sem material de chave e importar o seu próprio material de chaves para essa chave do KMS, um recurso normalmente conhecido como "traga sua própria chave" (BYOK).



> **Note**
>
> AWS KMS não suporta a descriptografia de nenhum texto AWS KMS cifrado fora do AWS KMS, mesmo que o texto cifrado tenha sido criptografado em uma chave KMS com material de chave importado. AWS KMS não publica o formato de texto cifrado exigido por essa tarefa e o formato pode ser alterado sem aviso prévio.

O material de chaves importadas é compatível com todos os tipos de chaves do KMS, exceto as chaves do KMS em repositórios de chaves personalizados.

Ao usar material de chave importado, você permanece responsável pelo material de chaves, AWS KMS permitindo o uso de uma cópia dele. Você pode optar por fazer isso por um ou mais dos seguintes motivos:

- Para comprovar que o material de chaves foi gerado usando uma origem de entropia que atende aos seus requisitos.
- Para usar o material chave de sua própria infraestrutura com AWS serviços e AWS KMS para gerenciar o ciclo de vida desse material chave em seu interior. AWS
- Para usar chaves existentes e bem estabelecidas AWS KMS, como chaves para assinatura de código, assinatura de certificado PKI e aplicativos fixados em certificados
- Para definir um prazo de validade para o material de chave AWS e excluí-lo manualmente, mas também para disponibilizá-lo novamente no futuro. Por outro lado, programar a exclusão de chaves exige um período de espera de 7 a 30 dias, após os quais você não pode recuperar a chave do KMS excluída.
- Possuir a cópia original do material principal e mantê-la do lado de fora AWS para maior durabilidade e recuperação de desastres durante todo o ciclo de vida do material principal.
- Para chaves assimétricas e chaves HMAC, a importação cria chaves compatíveis e interoperáveis que operam dentro e fora dela. AWS

Você pode auditar e monitorar o uso e o gerenciamento de uma chave KMS com material de chave importado. AWS KMS registra um evento em seu AWS CloudTrail registro quando você cria a chave KMS, baixa a chave pública de empacotamento e o token de importação e importa o material da chave. AWS KMS também registra um evento quando você exclui manualmente o material-chave importado ou quando AWS KMS exclui o material-chave expirado.

Para obter informações sobre diferenças importantes entre chaves KMS com material de chave importado e aquelas com material de chave gerado por AWS KMS, consulteSobre o material de chave importada.

Chaves do KMS compatíveis

AWS KMS suporta material de chave importado para os seguintes tipos de chaves KMS. Não é possível importar material de chave para chaves do KMS em repositórios de chaves personalizados.

- Chaves do KMS de criptografia simétrica
- Chaves do KMS RSA assimétricas (para criptografia ou assinatura, mas não ambas)
- Chaves do KMS de curva elíptica assimétrica (ECC) (somente assinatura)
- Chaves KMS SM2 assimétricas — somente regiões da China (para criptografia ou assinatura, mas não para ambas)
- Chaves do KMS de HMAC
- Chaves multirregionais de todos os tipos compatíveis.

Regiões

O material chave importado é suportado em todos Regiões da AWS os AWS KMS suportes.

Nas regiões da China, os principais requisitos de material para chaves KMS de criptografia simétrica diferem de outras regiões. Para obter detalhes, consulte Importar o material de chave — etapa 3: Criptografar o material de chave.

Tópicos

- Planejar para importar o material de chave
- Gerenciar o material de chave importada
- Etapa 1 da importação de material de chave: criar uma AWS KMS key sem material de chave
- Importar o material de chave - etapa 2: Fazer download da chave pública de empacotamento e do token de importação

- Importar o material de chave — etapa 3: Criptografar o material de chave
- Importar o material de chave — etapa 4: Importar o material de chave

Planejar para importar o material de chave

O material de chaves importadas permite que você proteja seus AWS recursos com as chaves criptográficas que você gera. O material da chave que você importa está associado a uma chave do KMS específica. Você pode reimportar o mesmo material de chave para a mesma chave KMS, mas não pode importar material de chave diferente para a chave KMS e não pode converter uma chave KMS projetada para material de chave importado em uma chave KMS com material de chave. AWS KMS

Saiba mais:

- the section called “Selecionar uma especificação de chave pública de empacotamento”
- the section called “Selecionar um algoritmo de empacotamento”

Tópicos

- Sobre o material de chave importada
- Proteger o material de chave importada
- Permissões para importar material de chave
- Requisitos para material de chave importada

Sobre o material de chave importada

Antes de decidir importar material de chave para AWS KMS, você deve compreender as seguintes características do material de chave importado.

Você gera o material de chave

> Você é responsável por gerar o material de chaves usando uma origem de aleatoriedade que atende aos seus requisitos de segurança.

Você pode excluir o material de chave.

> Você pode excluir material de chave importado de uma chave do KMS, tornando imediatamente a chave do KMS inutilizável. Além disso, ao importar o material de chave para uma chave do

KMS, é possível determinar se a chave expira e definir seu prazo de validade. Quando o prazo de validade chegar, AWS KMS exclui o material da chave. Sem o material de chave, a chave do KMS não pode ser usada em nenhuma operação criptográfica. Para restaurar a chave, é necessário reimportar o mesmo material de chave para a chave.

Não é possível alterar o material de chave

Quando você importa o material de chave para uma chave do KMS, esta é associada permanentemente a esse material de chave. Você pode reimportar o mesmo material de chaves, mas não pode importar outro material de chaves para essa chave do KMS. Além disso, não é possível habilitar a alternância automática de chaves de uma chave do KMS com material de chaves importado. No entanto, você pode alternar manualmente uma chave do KMS com material de chave importado.

Não é possível alterar a origem do material de chave

As chaves do KMS projetadas para material de chave importado têm um valor de origem de `EXTERNAL` que não pode ser alterado. Você não pode converter uma chave KMS de material de chave importado para usar material de chave de qualquer outra fonte, inclusive AWS KMS. Da mesma forma, você não pode converter uma chave KMS com material de AWS KMS chave em uma projetada para material de chave importado.

Não é possível exportar material de chave

Você não pode exportar nenhum material de chave que tenha importado. AWS KMS não é possível devolver o material da chave importada para você de nenhuma forma. Você deve manter uma cópia do material de chaves importado fora dele AWS, de preferência em um gerenciador de chaves, como um módulo de segurança de hardware (HSM), para poder reimportar o material de chaves se você excluí-lo ou se ele expirar.

É possível criar chaves de várias regiões com material de chave importado.

A chave de várias regiões com material de chave importado tem recursos das chaves do KMS com material de chave importado e pode interoperar entre as Regiões da AWS. Para criar uma chave de várias regiões com material de chave importado, você deve importar o mesmo material de chave para a chave do KMS primária e para cada chave de réplica. Para obter detalhes, consulte Importar material de chave para chaves de várias regiões.

As chaves assimétricas e as chaves de HMAC são portáteis e interoperáveis

Você pode usar seu material de chave assimétrica e material de chave HMAC externamente AWS para interoperar com AWS KMS chaves com o mesmo material de chave importado.

Ao contrário do texto cifrado AWS KMS simétrico, que está inextricavelmente vinculado à chave KMS usada no algoritmo, AWS KMS usa formatos HMAC e assimétricos padrão para criptografia, assinatura e geração de MAC. Como resultado, as chaves são portáteis e compatíveis com cenários tradicionais de garantia de chaves.

Quando sua chave KMS tiver importado material de chave, você poderá usar o material de chave importado de fora AWS para realizar as seguintes operações.

- Chaves de HMAC — É possível verificar uma etiqueta de HMAC que foi gerada pela chave do KMS de HMAC com material de chave importado. Você também pode usar a chave HMAC KMS com o material de chave importado para verificar uma tag HMAC que foi gerada pelo material de chave externo. AWS
- Chaves de criptografia assimétricas — Você pode usar sua chave privada de criptografia assimétrica externa para AWS descriptografar um texto cifrado criptografado pela chave KMS com a chave pública correspondente. Você também pode usar sua chave KMS assimétrica para descriptografar um texto cifrado assimétrico que foi gerado fora do. AWS
- Chaves de assinatura assimétrica — Você pode usar sua chave KMS de assinatura assimétrica com material de chave importado para verificar as assinaturas digitais geradas por sua chave de assinatura privada fora da. AWS Você também pode usar sua chave de assinatura pública assimétrica no exterior AWS para verificar as assinaturas geradas pela sua chave KMS assimétrica.

Se você importar o mesmo material de chave para chaves do KMS diferentes da mesma Região da AWS, essas chaves também serão interoperáveis. Para criar chaves KMS interoperáveis em diferentes Regiões da AWS, crie uma chave multirregional com material de chave importado.

As chaves de criptografia simétricas não são portáteis nem interoperáveis

Os textos cifrados simétricos que AWS KMS produz não são portáteis nem interoperáveis. AWS KMS não publica o formato de texto cifrado simétrico exigido pela portabilidade, e o formato pode mudar sem aviso prévio.

- AWS KMS não é possível descriptografar textos cifrados simétricos que você criptografa fora AWS, mesmo se você usar material de chave que tenha importado.
- AWS KMS não suporta a descriptografia de nenhum texto cifrado AWS KMS simétrico fora do AWS KMS, mesmo que o texto cifrado tenha sido criptografado em uma chave KMS com material de chave importado.
- As chaves do KMS com o mesmo material de chave importado não são interoperáveis. O texto cifrado simétrico que AWS KMS gera um texto cifrado específico para cada chave KMS. Esse

formato de texto cifrado garante que somente a chave do KMS que criptografou os dados poderá descriptografá-los.

Além disso, você não pode usar nenhuma AWS ferramenta, como a criptografia do lado do cliente AWS Encryption SDKou do Amazon S3, para descriptografar textos cifrados simétricos. AWS KMS

Como resultado, você não pode usar chaves com material de chave importado para apoiar acordos de custódia de chaves em que um terceiro autorizado com acesso condicional ao material de chaves possa decifrar determinados textos cifrados fora do. AWS KMS Para oferecer suporte à garantia de chave, use o AWS Encryption SDK para criptografar sua mensagem em uma chave que seja independente do AWS KMS.

Você é responsável pela disponibilidade e durabilidade

AWS KMS foi projetado para manter o material chave importado altamente disponível. Mas AWS KMS não mantém a durabilidade do material chave importado no mesmo nível do material chave AWS KMS gerado. Para obter detalhes, consulte Proteger o material de chave importada.

Proteger o material de chave importada

O material de chave importada é protegido em trânsito e em repouso. Antes de importar o material da chave, você criptografa (ou “empacota”) o material da chave com a chave pública de um par de chaves RSA gerado em módulos de segurança de AWS KMS hardware (HSMs) validados pelo Programa de Validação do Módulo Criptográfico FIPS 140-2. É possível criptografar o material da chave diretamente com a chave pública de empacotamento ou criptografar o material da chave com uma chave simétrica AES e, em seguida, criptografar a chave simétrica AES com a chave pública RSA.

Após o recebimento, AWS KMS descriptografa o material da chave com a chave privada correspondente em um AWS KMS HSM e o recriptografa sob uma chave simétrica AES que existe somente na memória volátil do HSM. O material de chave nunca sai do HSM em texto sem formatação. Ele é descriptografado somente enquanto está em uso e somente dentro dos HSMs. AWS KMS

O uso da chave do KMS com material de chave importado é determinado exclusivamente pelas políticas de controle de acesso que você define na chave do KMS. Além disso, é possível usar aliases e tags para identificar e controlar o acesso à chave do KMS. É possível ativar e desativar a chave, visualizar e editar suas propriedades e monitorá-la usando serviços como o AWS CloudTrail.

No entanto, você mantém a única cópia à prova de falhas do seu material de chave. Em troca dessa medida extra de controle, você é responsável pela durabilidade e disponibilidade geral do material chave importado. AWS KMS foi projetado para manter o material chave importado altamente disponível. Mas AWS KMS não mantém a durabilidade do material chave importado no mesmo nível do material chave AWS KMS gerado.

Essa diferença em durabilidade é importante nos seguintes casos:

- Quando você define um prazo de validade para o material de chaves importado, AWS KMS exclui o material de chaves depois que ele expira. AWS KMS não exclui a chave KMS nem seus metadados. Você pode criar um CloudWatch alarme da Amazon que o notifique quando o material de chave importado estiver se aproximando da data de expiração.

  Você não pode excluir o material da chave AWS KMS gerado para uma chave KMS e não pode definir que o material da AWS KMS chave expire, embora você possa girá-lo.
- Quando você exclui manualmente o material da chave importada, AWS KMS exclui o material da chave, mas não exclui a chave KMS ou seus metadados. Por outro lado, programar a exclusão de chaves exige um período de espera de 7 a 30 dias, após o qual o AWS KMS exclui permanentemente a chave do KMS, seus metadados e o material de chave.
- No caso improvável de certas falhas em toda a região que afetem AWS KMS (como perda total de energia), AWS KMS não é possível restaurar automaticamente o material de chave importado. No entanto, AWS KMS pode restaurar a chave KMS e seus metadados.

Você deve reter uma cópia do material de chave importado fora AWS de um sistema que você controla. Recomendamos armazenar uma cópia exportável do material de chave importado em um sistema de gerenciamento de chaves, como um HSM. Se o material de chave importado for excluído ou expirar, a chave do KMS associada se tornará inutilizável até que você reimporte o mesmo material de chave. Se o material de chave importada for perdido permanentemente, todo texto cifrado criptografado sob a chave do KMS será irrecuperável.

Permissões para importar material de chave

Para criar e gerenciar chaves do KMS com material de chave importado, o usuário precisa de permissão para as operações nesse processo. Você pode fornecer as permissões `kms:GetParametersForImport`, `kms:ImportKeyMaterial` e `kms:DeleteImportedKeyMaterial` na política de chaves ao criar a chave do KMS. No AWS KMS console, essas permissões são adicionadas automaticamente para administradores de chaves quando você cria uma chave com uma origem de material de chave externa.

Para criar chaves do KMS com material de chave importado, a entidade principal precisa das permissões a seguir.

- kms: CreateKey (política do IAM)
  - Para limitar essa permissão às chaves KMS com material de chave importado, use a condição kms: KeyOrigin policy com um valor de. EXTERNAL

```
{
  "Sid": "CreateKMSKeysWithoutKeyMaterial",
  "Effect": "Allow",
  "Resource": "*",
  "Action": "kms:CreateKey",
  "Condition": {
    "StringEquals": {
      "kms:KeyOrigin": "EXTERNAL"
    }
  }
}
```

- kms: GetParametersForImport (Política de chave ou política do IAM)
  - Para limitar essa permissão a solicitações que usam um algoritmo de empacotamento específico e uma especificação de chave de encapsulamento, use as condições de política kms: WrappingAlgorithm e kms:. WrappingKeySpec
- kms: ImportKeyMaterial (Política de chave ou política do IAM)
  - Para permitir ou proibir o material chave que expira e controlar a data de expiração, use as condições da política kms: ExpirationModel e kms:. ValidTo

Para reimportar o material de chave importado, o diretor precisa das permissões kms: GetParametersForImport e kms:. ImportKeyMaterial

Para excluir o material de chave importado, o diretor precisa de kms: DeleteImportedKeyMaterial permission.

Por exemplo, para permitir que o exemplo `KMSAdminRole` gerencie todos os aspectos de uma chave do KMS com material de chave importado, inclua uma declaração de política de chaves como a seguinte na política de chaves da chave do 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"
  ]
}
```

Requisitos para material de chave importada

O material da chave que você importa deve ser compatível com a especificação de chave da chave do KMS correspondente. Para pares de chaves assimétricas, importe somente a chave privada do par. AWS KMS deriva a chave pública da chave privada.

AWS KMS suporta as seguintes especificações principais para chaves KMS com material de chave importado.

Especificação de chave da chave do KMS	Requisitos de material de chaves
Chaves de criptografia simétrica SYMMETRIC_DEFAULT	256 bits (32 bytes) de dados binários Nas regiões da China, elas devem ter 128 bits (16 bytes) de dados binários.
Chaves de HMAC HMAC_224 HMAC_256 HMAC_384 HMAC_512	O material da chave de HMAC deve estar em conformidade com a RFC 2104. O comprimento da chave deve corresponder ao comprimento especificado pela especificação da chave.
Chave privada assimétrica RSA RSA_2048	A chave privada assimétrica RSA que você importa deve fazer parte de um par de chaves que esteja em conformidade com a RFC 3447.

Especificação de chave da chave do KMS	Requisitos de material de chaves
RSA_3072 RSA_4096	Módulo: 2048 bits, 3072 bits ou 4096 bits Número de primes: 2 (chaves RSA com vários primes não são compatíveis) O material de chave assimétrica deve ser codificado em BER ou DER no formato Public Key Cryptography Standards (PKCS) #8 que esteja em conformidade com a RFC 5208.
Chave privada assimétrica de curva elíptica ECC_NIST_P256 (secp256r1) ECC_NIST_P384 (secp384r1) ECC_NIST_P521 (secp521r1) ECC_SECG_P256K1 (secp256k1)	A chave privada assimétrica ECC que você importa deve fazer parte de um par de chaves que esteja em conformidade com a RFC 5915. Curva: NIST P-256, NIST P-384, NIST P-521 ou Secp256k1 Parâmetros: somente curvas nomeadas (chaves ECC com parâmetros explícitos são rejeitadas) Coordenadas de pontos públicos: podem ser compactadas, não compactadas ou projetivas O material de chave assimétrica deve ser codificado em BER ou DER no formato Public Key Cryptography Standards (PKCS) #8 que esteja em conformidade com a RFC 5208.

Especificação de chave da chave do KMS	Requisitos de material de chaves
Chave privada assimétrica SM2 (somente regiões da China)	A chave privada assimétrica SM2 que você importa deve fazer parte de um par de chaves que esteja em conformidade com GM/T 0003. Curva: SM2 Parâmetros: somente curva nomeada (teclas SM2 com parâmetros explícitos são rejeitadas) Coordenadas de pontos públicos: podem ser compactadas, não compactadas ou projetivas O material de chave assimétrica deve ser codificado em BER ou DER no formato Public Key Cryptography Standards (PKCS) #8 que esteja em conformidade com a RFC 5208.

Gerenciar o material de chave importada

Esses tópicos explicam como importar e reimportar material de chave em uma chave do KMS e como criar material de chave importado que expira automaticamente.

Tópicos

- Visão geral da importação do material de chave
- Reimportar o material de chave
- Identificar chaves do KMS com material de chave importado
- Criação de um CloudWatch alarme para expiração do material chave importado
- Excluir o material de chave importada
- Excluir uma chave do KMS com material de chave importado

Visão geral da importação do material de chave

A visão geral a seguir explica o processo para importar seu material de chaves para o AWS KMS. Para obter mais detalhes sobre cada etapa no processo, consulte o tópico correspondente.

1. Crie uma chave do KMS sem material de chave - A origem deve ser `EXTERNAL`. A origem da chave `EXTERNAL` indica que a chave foi projetada para material de chave importado e AWS KMS impede a geração de material de chave para a chave KMS. Em uma etapa posterior, você importará seu próprio material de chave para essa chave do KMS.

   O material da chave que você importa deve ser compatível com a especificação da chave associada AWS KMS . Para obter mais informações sobre compatibilidade, consulte the section called “Requisitos para material de chave importada”.

2. Baixar a chave pública de empacotamento e o token de importação – depois de concluir a etapa 1, baixe uma chave publica de empacotamento e um token de importação. Esses itens protegem seu material principal enquanto ele é importado para AWS KMS o.

   Nesta etapa, você escolhe o tipo (“especificação de chave”) para a chave de empacotamento RSA e o algoritmo de empacotamento que você usará para criptografar os dados em trânsito para o AWS KMS. É possível escolher uma especificação de chave de empacotamento e um algoritmo de chave de empacotamento diferentes sempre que importar ou reimportar o mesmo material de chave.

3. Criptografar o material de chaves – use a chave pública de empacotamento baixada na etapa 2 para criptografar o material de chaves que você criou no seu próprio sistema.

4. Importar o material de chaves – carregue o material de chave criptografado que você criou na etapa 3 e o token de importação que você baixou na etapa 2.

   Nessa etapa, é possível definir um prazo de validade opcional. Quando o material da chave importada expira, ele é AWS KMS excluído e a chave KMS fica inutilizável. Para continuar usando a chave do KMS, você deve reimportar o mesmo material de chave.

   Quando a operação de importação é concluída com êxito, o estado da chave KMS muda de `PendingImport` para `Enabled`. Agora, você pode usar suas chaves do KMS em operações de criptografia.

AWS KMS registra uma entrada em seu AWS CloudTrail registro quando você cria a chave KMS, baixa a chave pública de empacotamento e o token de importação e importa o material da chave. AWS KMS também registra uma entrada quando você exclui material de chave importado ou quando AWS KMS exclui material de chave expirado.

Reimportar o material de chave

Se você gerencia uma chave do KMS com material de chaves importado, talvez seja necessário importar novamente o material de chave. Você também reimportar o material de chave para substituir material de chave prestes a expirar ou excluído ou para alterar o modelo de expiração ou a data de validade do material de chave.

Quando você importa o material de chave para uma chave do KMS, esta é associada permanentemente a esse material de chave. Você pode reimportar o mesmo material de chaves, mas não pode importar outro material de chaves para essa chave do KMS. Você não pode alternar o material de chave e o AWS KMS não pode criar esse material de chave para uma chave do KMS com material de chave importado.

Você pode reimportar material da chave a qualquer momento, em qualquer programação que atenda aos seus requisitos de segurança. Não é necessário esperar até que o material da chave esteja expirando ou prestes a expirar.

Para importar novamente um material de chaves, use o mesmo procedimento que você usou para importar o material de chaves na primeira vez, com as seguintes exceções.

- Utilize uma chave do KMS existente em vez de criar uma nova. Você pode ignorar a Etapa 1 do procedimento de importação.
- Ao reimportar o material de chave, você pode alterar o modelo de expiração e data de expiração.

Cada vez que você importa o material de chave para uma chave do KMS, é necessário baixar e usar uma nova chave de empacotamento e token de importação da chave do KMS. O procedimento de empacotamento não afeta o conteúdo do material de chave, portanto você pode usar diferentes chaves públicas de empacotamento e diferentes algoritmos de empacotamento para importar o mesmo material de chave.

Identificar chaves do KMS com material de chave importado

Quando você cria uma chave do KMS sem material de chave, o valor da propriedade `Origin` dessa chave do KMS é `EXTERNAL` e não pode ser alterado. Ao contrário do key state (estado da chave), o valor `Origin` não depende da presença ou ausência de material de chave.

Você pode usar o valor de origem `EXTERNAL` para identificar chaves do KMS projetadas para material de chave importado. Você pode encontrar a origem da chave no AWS KMS console ou

usando a DescribeKeyoperação. Também é possível exibir as propriedades do material de chave, como se e quando ela expira, usando o console ou as APIs.

Para identificar chaves do KMS com material de chave importado (console)

1. Abra o AWS KMS console em https://console.aws.amazon.com/kms.
2. Para alterar o Região da AWS, use o seletor de região no canto superior direito da página.
3. Use uma das seguintes técnicas para visualizar a propriedade `Origin` das suas chaves do KMS.

   - Para adicionar uma coluna Origin (Origem) à sua tabela de chaves do KMS, no canto superior direito, escolha o ícone Settings (Configurações). Selecione Origin (Origem) e clique em Confirm (Confirmar). A coluna Origin (Origem) facilita a identificação das chaves do KMS com um valor de propriedade de origem External (Import Key material) (Externa [Importar material-chave]).
   - Para encontrar o valor da propriedade `Origin` de uma chave do KMS específica, escolha o ID de chave ou a alias da chave do KMS. Em seguida, escolha a guia Configuration (Configuração). As guias estão abaixo da seção General configuration (Configuração geral).
4. Para exibir informações detalhadas sobre o material de chave, escolha a guia Key material (Material de chave). Essa guia é exibida na página de detalhes apenas para chaves do KMS com material de chave importado.

Para identificar chaves KMS com material de chave importado (AWS KMS API)

Use a DescribeKeyoperação. A resposta inclui a propriedade `Origin` da chave do KMS, o modelo de validade e a data de validade, como mostra o exemplo a seguir.

```
$  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"
        ]
    }
}
```

Criação de um CloudWatch alarme para expiração do material chave importado

Você pode criar um CloudWatch alarme que o notifique quando o material de chave importado em uma chave KMS estiver se aproximando do prazo de expiração. Por exemplo, o alarme pode notificá-lo quando faltarem menos de 30 dias para a expiração.

Ao importar o material de chave para uma chave do KMS, é possível especificar opcionalmente uma data e hora quando o material de chave expira. Quando o material da chave expira, ele é AWS KMS excluído e a chave KMS fica inutilizável. Para usar a chave do KMS novamente, você deve reimportar o material de chave. No entanto, se você reimportar o material de chave antes que ele expire, você poderá evitar interromper processos que usem essa chave do KMS.

Esse alarme usa a `SecondsUntilKeyMaterialExpires`métrica que AWS KMS publica CloudWatch para chaves KMS com material de chave importado que expira. Cada alarme usa essa métrica para monitorar o material de chave importado para uma chave específica do KMS. Você não pode criar um alarme único para todas as chaves do KMS com material de chave expirado ou um alarme para chaves do KMS que você possa vir a criar futuramente.

Requisitos

Os seguintes recursos são necessários para um CloudWatch alarme que monitora a expiração do material de chave importado.

- Uma chave do KMS com material de chave importado que expira. Para obter ajuda, consulte Identificar chaves do KMS com material de chave importado.
- Um tópico do Amazon SNS. Para obter detalhes, consulte o tópico Criação de um Amazon SNS no Guia CloudWatch do usuário da Amazon.

Criar o alarme

Siga as instruções em Criar um CloudWatch alarme com base em um limite estático usando os seguintes valores obrigatórios. Para outros campos, aceite os valores padrão e forneça os nomes conforme solicitado.

Campo	Valor
Selecionar métrica	Escolha KMS e, em seguida, selecione Per-Key Metrics (Métricas por chave). Selecione a linha com a chave do KMS e a métrica `SecondsUntilKeyMaterialExpires`. Depois, escolha Select metric (Selecionar métrica). A lista Metrics (Métricas) exibe a métrica `SecondsUntilKeyMaterialExpires` apenas para chaves do KMS com material de chave importado que expira. Se você não tiver chaves do KMS com essas propriedades na conta e na região, essa lista estará vazia.
Estatística	Mínimo
Período	1 minuto
Tipo de limite	Estático
Sempre que…	Sempre que o *`nome da métrica`* for maior que 1

Excluir o material de chave importada

Você pode excluir o material de chave importado de uma chave do KMS a qualquer momento. Além disso, quando o material de chave importado com uma data de validade expirar, AWS KMS exclui o material de chave. Nos dois casos, quando o material da chave é excluído, o estado de chave da chave do KMS muda para Importação pendente e a chave do KMS não pode ser usada em nenhuma operação criptográfica até que você reimporte o mesmo material de chave. (Não é possível importar material de chave para uma chave do KMS de HMAC.)

Além de desativar a chave do KMS e retirar as permissões, a exclusão do material da chave pode ser usada como uma estratégia para interromper o uso da chave do KMS de forma rápida, mas temporária. Por outro lado, programar a exclusão de uma chave do KMS com material de chave importado também interrompe rapidamente o uso da chave do KMS. No entanto, se a exclusão

não for cancelada durante o período de espera, a chave do KMS, o material da chave e todos os metadados da chave serão excluídos permanentemente. Para obter detalhes, consulte the section called “Excluir uma chave do KMS com material de chave importado”.

Para excluir o material chave, você pode usar o AWS KMS console ou a operação DeleteImportedKeyMaterialda API. AWS KMS registra uma entrada em seu AWS CloudTrail registro quando você exclui material de chave importado e quando AWS KMS exclui material de chave expirado.

Tópicos

- Como a exclusão do material essencial afeta os serviços AWS
- Excluir material de chave (console)
- Excluir material chave (AWS KMS API)

Como a exclusão do material essencial afeta os serviços AWS

Quando você exclui o material da chave, a chave do KMS sem material da chave torna-se inutilizável imediatamente (sujeita a consistência posterior). Porém, os recursos criptografados com chaves de dados protegidas pela chave do KMS não serão afetados até que a chave do KMS seja usada novamente, por exemplo, para descriptografar a chave de dados. Esse problema afeta Serviços da AWS muitos dos quais usam chaves de dados para proteger seus recursos. Para obter detalhes, consulte Como as chaves do KMS inutilizáveis afetam as chaves de dados.

Excluir material de chave (console)

Você pode usar o AWS Management Console para excluir o material chave.

1. Faça login AWS Management Console e abra o console AWS Key Management Service (AWS KMS) em https://console.aws.amazon.com/kms.
2. Para alterar o Região da AWS, use o seletor de região no canto superior direito da página.
3. No painel de navegação, escolha Chaves gerenciadas pelo cliente.
4. Execute um destes procedimentos:

   - Marque a caixa de seleção de uma chave do KMS com material de chave importado. Escolha Key actions (Ações de chave), Delete key material (Excluir material de chaves).
   - Escolha o alias ou ID de uma chave do KMS com material de chave importado. Escolha a guia Key material (Material de chaves) e, em seguida, Delete key material (Excluir material de chave).

5. Confirme que você deseja excluir o material de chaves e selecione Delete key material (Excluir material de chaves). O status da chave do KMS, que corresponde ao seu estado de chave, muda para Pending import (Importação pendente).

Excluir material chave (AWS KMS API)

Para usar a AWS KMS API para excluir material chave, envie uma DeleteImportedKeyMaterialsolicitação. O exemplo a seguir mostra como fazer isso com a AWS CLI.

Substitua *1234abcd-12ab-34cd-56ef-1234567890ab* pelo ID da chave do KMS cujo material de chave você quer excluir. É possível usar o ID de chave ou o ARN da chave do KMS, mas não é possível usar um alias para essa operação.

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

Excluir uma chave do KMS com material de chave importado

A exclusão do material de chave de uma chave do KMS com material de chave importado é temporária e reversível. Para restaurar a chave, reimporte o material da chave.

Entretanto, a exclusão de uma chave do KMS é irreversível. Se você agendar a exclusão da chave e o período de espera necessário expirar, excluirá AWS KMS permanente e irreversivelmente a chave KMS, seu material de chave e todos os metadados associados à chave KMS.

No entanto, o risco e a consequência da exclusão de uma chave do KMS com material de chave importado dependem do tipo (“especificação de chave”) da chave do KMS.

- Chaves de criptografia simétricas — Se você excluir uma chave do KMS de criptografia simétrica, todos os textos cifrados restantes criptografados por essa chave serão irrecuperáveis. Não é possível criar uma nova chave do KMS de criptografia simétrica que possa descriptografar os textos cifrados de uma chave de criptografia simétrica excluída com chave do KMs, mesmo que você tenha o mesmo material de chave. Os metadados exclusivos de cada chave do KMS são vinculados criptograficamente a cada texto cifrado simétrico. Esse recurso de segurança garante que somente a chave do KMS que criptografou o texto cifrado simétrico poderá descriptografá-lo, mas impede que você recrie uma chave do KMS equivalente.
- Chaves assimétricas e HMAC — Se você tiver o material da chave original, poderá criar uma nova chave KMS com as mesmas propriedades criptográficas de uma chave KMS assimétrica ou HMAC que foi excluída. AWS KMS gera cifrotextos e assinaturas RSA padrão, assinaturas ECC e tags

HMAC, que não incluem nenhum recurso de segurança exclusivo. Além disso, é possível usar uma chave do HMAC ou a chave privada de um par de chaves assimétricas fora da AWS.

Uma nova chave do KMS criada com o mesmo material de chave assimétrica ou HMAC terá um identificador de chave diferente. Você precisará criar uma nova política de chaves, recriar todos os aliases e atualizar as políticas e concessões existentes do IAM para se referir à nova chave.

Etapa 1 da importação de material de chave: criar uma AWS KMS key sem material de chave

Por padrão, o AWS KMS cria o material de chave para você quando você cria uma chave do KMS. Se preferir importar seu próprio material de chave, comece criando uma chave do KMS sem material de chave. Em seguida, importe o material de chave. Para criar uma chave KMS sem material de chave, use o AWS KMS console ou a CreateKeyoperação.

Para criar uma chave sem material de chave, especifique uma origem como `EXTERNAL`. A propriedade de origem de uma chave do KMS é imutável. Depois de criar, você não poderá converter uma chave do KMS projetada para material de chave importado em uma chave do KMS com material de chave do AWS KMS ou de qualquer outra fonte.

O key state (estado de chave) de uma chave do KMS com uma origem `EXTERNAL` e sem material chave é `PendingImport`. Uma chave do KMS pode permanecer no estado `PendingImport` indefinidamente. No entanto, não é possível usar uma chave do KMS no estado `PendingImport` em operações criptográficas. Quando o material da chaves é importado, o estado da chave do KMS muda para `Enabled`, e você pode usar a chave do KMS em operações de criptografia.

AWS KMSregistra um evento em seu AWS CloudTrail registro quando você cria a chave KMS, baixa a chave pública e o token de importação e importa o material da chave. AWS KMStambém registra um CloudTrail evento quando você exclui material de chave importado ou quando AWS KMS exclui material de chave expirado.

Para obter informações sobre como criar chaves de várias regiões com o material de chave importado, consulte Importar material de chave para chaves de várias regiões.

Tópicos

- Criar uma chave do KMS sem material de chave (console)
- Criar uma chave do KMS sem material de chave (API do AWS KMS)

Criar uma chave do KMS sem material de chave (console)

Você somente precisa criar uma chave do KMS para o material de chave importado uma vez. É possível importar reimportar o mesmo material de chaves para as chave s do KMS quantas vezes desejar, mas não é possível importar outro material de chaves para uma chave do KMS. Para obter detalhes, consulte Etapa 2: Fazer download da chave pública de empacotamento e do token de importação.

Para encontrar chaves do KMS existentes com material de chave importado em sua tabela Customer managed keys (Chaves gerenciadas pelo cliente), use o ícone de engrenagem no canto superior direito para mostrar a coluna Origin (Origem) na lista de chaves do KMS. As chaves importadas têm um valor Origin (Origem) External (Externo) (Importar material de chave).

Para criar uma chave do KMS com material de chave importado, comece seguindo as instruções básicas para criar uma chave do KMS do seu tipo de chave preferido, com a exceção a seguir.

Depois de escolher o uso de chave, faça o seguinte:

1. Expanda Advanced options (Opções avançadas).
2. Em Key material origin (Origem do material de chave), escolha External (Import key material) (Externo [material de chave importado]).
3. Marque a caixa de seleção ao lado de I understand the security, availability, and durability implications of using an imported key (Entendo as implicações de segurança, disponibilidade e durabilidade do uso de uma chave importada) para indicar que você compreende as implicações do uso de material de chaves importadas. Para ler sobre essas implicações, consulte Proteger o material de chave importada.
4. Retorne às instruções básicas. As etapas restantes do procedimento básico são as mesmas para todas as chaves do KMS desse tipo.

Ao escolher Concluir, você criou uma chave do KMS sem material de chave e um status (estado da chave) de importação pendente.

No entanto, em vez de retornar à tabela de chaves gerenciadas pelo cliente, o console exibirá uma página na qual é possível baixar a chave pública e o token de importação necessários para importar o material da chave. É possível continuar com a etapa de download agora ou escolher Cancelar para parar nesse momento. É possível retornar a essa etapa de download a qualquer momento.

Próximo: Etapa 2: Fazer download da chave pública de empacotamento e do token de importação.

Criar uma chave do KMS sem material de chave (API do AWS KMS)

Para usar a AWS KMSAPI para criar uma chave KMS de criptografia simétrica sem material de chave, envie uma CreateKeysolicitação com o `Origin` parâmetro definido como. `EXTERNAL` O exemplo a seguir mostra como fazer isso com a AWS Command Line Interface (AWS CLI).

```
$ aws kms create-key --origin EXTERNAL
```

Quando o comando é bem-sucedido, a saída é semelhante à seguinte. A chave do AWS KMS `Origin` é `EXTERNAL` e seu `KeyState` é `PendingImport`.

> **Tip**
>
> Se o comando não for bem-sucedido, você poderá ver uma `KMSInvalidStateException` ou `NotFoundException`. Você poderá repetir a solicitação.

```
{
    "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"
        ]
    }
}
```

Copie o valor `KeyId` da saída do seu comando para usar em etapas posteriores e prossiga para Etapa 2: Fazer download da chave pública de empacotamento e do token de importação.

> **Note**
>
> Esse comando cria uma chave do KMS de criptografia simétrica com uma `KeySpec` de `SYMMETRIC_DEFAULT` e `KeyUsage` de `ENCRYPT_DECRYPT`. É possível usar os parâmetros opcionais `--key-spec` e `--key-usage` para criar uma chave assimétrica ou HMAC KMS. Para obter mais informações, consulte a operação CreateKey.

Importar o material de chave - etapa 2: Fazer download da chave pública de empacotamento e do token de importação

Depois de criar um material AWS KMS key sem chave, baixe uma chave pública de empacotamento e um token de importação para essa chave KMS usando o AWS KMS console ou a GetParametersForImportAPI. A chave pública de empacotamento e o token de importação são um conjunto indivisível que deve ser usado em conjunto.

Você usará a chave pública de empacotamento para criptografar seu material de chave para transporte. Antes de baixar um par de chaves de empacotamento RSA, você seleciona o comprimento (especificação de chave) do par de chaves de encapsulamento RSA e o algoritmo de empacotamento que você usará para criptografar seu material de chave importado para transporte na etapa 3. AWS KMS também suporta a especificação da chave de empacotamento SM2 (somente regiões da China).

Cada conjunto de chave pública de empacotamento e de token de importação é válido por 24 horas. Se você não usá-los para importar material de chaves em até 24 horas após o download, será necessário fazer download de um novo conjunto. É possível fazer download de uma nova chave pública de empacotamento e de conjuntos de tokens de empacotamento a qualquer momento. Isso permitirá que você altere o comprimento da chave de empacotamento RSA (“especificação da chave”) ou substitua um conjunto perdido.

Também é possível baixar uma chave pública de empacotamento e o conjunto de tokens de importação para reimportar o mesmo material de chave para uma chave do KMS. É possível fazer isso para definir ou alterar o tempo de expiração do material de chaves ou para restaurar o material de chaves expirado ou excluído. Você deve baixar e recriptografar seu material de chave toda vez que importá-lo para o. AWS KMS

Uso da chave pública de empacotamento

O download inclui uma chave pública exclusiva para você Conta da AWS, também chamada de chave pública de empacotamento.

Antes de importar o material da chave, você criptografa o material da chave com a chave de empacotamento pública e, em seguida, carrega o material da chave criptografada para. AWS KMS Ao AWS KMS receber seu material de chave criptografada, ele descriptografa o material de chave com a chave privada correspondente e, em seguida, recriptografa o material de chave sob uma chave simétrica AES, tudo dentro de um módulo de segurança de AWS KMS hardware (HSM).

Uso do token de importação

O download inclui um token de importação que contém metadados para garantir que o seu material de chaves seja importado corretamente. Ao carregar seu material de chave criptografada para AWS KMS, você deve carregar o mesmo token de importação que você baixou nesta etapa.

Selecionar uma especificação de chave pública de empacotamento

Para proteger seu material de chaves durante a importação, você o criptografa usando uma chave pública de agrupamento da qual você baixa e um AWS KMS algoritmo de agrupamento compatível. Selecione uma especificação de chave antes de fazer download da chave pública de empacotamento e do token de importação. Todos os pares de chaves de empacotamento são gerados em módulos AWS KMS de segurança de hardware (HSMs). A chave privada nunca sai do HSM em texto simples.

Especificações principais de empacotamento RSA

A especificação de chave da chave pública de empacotamento determina o comprimento das chaves no par de chaves RSA que protege o material de chave durante o transporte para o AWS KMS. Em geral, recomendamos o uso da chave pública de empacotamento mais longa possível. Oferecemos várias especificações de chave pública de empacotamento para oferecer suporte a uma variedade de HSMs e gerenciadores de chaves.

AWS KMS suporta as seguintes especificações principais para as chaves de empacotamento RSA usadas para importar material de chaves de todos os tipos, exceto conforme indicado.

- RSA_4096 (preferencial)
- RSA_3072

- RSA_2048

> **Note**
>
> A combinação a seguir NÃO é compatível: material de chave ECC_NIST_P521, especificação de chave de empacotamento pública RSA_2048 e um algoritmo de empacotamento RSAES_OAEP_SHA_*.
> Não é possível empacotar diretamente o material de chave ECC_NIST_P521 com uma chave de empacotamento pública RSA_2048. Use uma chave de empacotamento maior ou um algoritmo de empacotamento RSA_AES_KEY_WRAP_SHA_*.

Especificação da chave de embalagem SM2 (somente regiões da China)

AWS KMS suporta a seguinte especificação de chave para as chaves de empacotamento SM2 usadas para importar material de chave assimétrico.

- SM2

Selecionar um algoritmo de empacotamento

Para proteger o material de chaves durante a importação, criptografe-o usando a chave pública de empacotamento baixada e um algoritmo de empacotamento.

AWS KMS suporta vários algoritmos de empacotamento RSA padrão e um algoritmo de empacotamento híbrido de duas etapas. Em geral, recomendamos usar o algoritmo de empacotamento mais seguro que seja compatível com o material da chave importada e com a especificação da chave de empacotamento. Normalmente, você escolhe um algoritmo que é compatível com o módulo de segurança de hardware (HSM) ou com o sistema de gerenciamento de chaves que protege o material de chaves.

A tabela a seguir mostra os algoritmos de empacotamento compatíveis com cada tipo de material de chave e chave do KMS. Os algoritmos estão listados em ordem de preferência.

Material de chave	Algoritmo e especificação de empacotamento compatíveis
Chave de criptografia simétrica	Algoritmos de empacotamento:
Chave AES de 256 bits	RSAES_OAEP_SHA_256

Material de chave	Algoritmo e especificação de empacotamento compatíveis
Chave 128-bit SM4 (somente nas regiões da China)	RSAES_OAEP_SHA_1 Algoritmos de empacotamento obsoletos: RAES_PKCS1_V1 **Note** Em 10 de outubro de 2023, AWS KMS não oferece suporte ao algoritmo de encapsulamento RSAES_PKCS1_V1_5. Especificações da chave de empacotamento: RSA_2048 RSA_3072 RSA_4096
Chave privada RSA assimétrica	Algoritmos de empacotamento: RSA_AES_KEY_WRAP_SHA_256 RSA_AES_KEY_WRAP_SHA_1 SM2PKE (somente regiões da China) Especificações da chave de empacotamento: RSA_2048 RSA_3072 RSA_4096 SM2 (somente nas regiões da China)

Material de chave	Algoritmo e especificação de empacotamento compatíveis
Chave privada assimétrica de curva elíptica (ECC) Não é possível usar os algoritmos de empacotamento RSAES_OAEP_SHA_* com a especificação da chave de empacotamento RSA_2048 para empacotar o material da chave ECC_NIST_P521.	Algoritmos de empacotamento: RSA_AES_KEY_WRAP_SHA_256 RSA_AES_KEY_WRAP_SHA_1 RSAES_OAEP_SHA_256 RSAES_OAEP_SHA_1 SM2PKE (somente regiões da China) Especificações da chave de empacotamento: RSA_2048 RSA_3072 RSA_4096 SM2 (somente nas regiões da China)
Chave privada SM2 assimétrica (somente regiões da China)	Algoritmos de empacotamento: RSAES_OAEP_SHA_256 RSAES_OAEP_SHA_1 SM2PKE (somente regiões da China) Especificações da chave de empacotamento: RSA_2048 RSA_3072 RSA_4096 SM2 (somente nas regiões da China)

Material de chave	Algoritmo e especificação de empacotamento compatíveis
Chave de HMAC	Algoritmos de empacotamento: RSAES_OAEP_SHA_256 RSAES_OAEP_SHA_1 Especificações da chave de empacotamento: RSA_2048 RSA_3072 RSA_4096

> **Note**
>
> Os algoritmos de `RSA_AES_KEY_WRAP_SHA_1` empacotamento `RSA_AES_KEY_WRAP_SHA_256` e não são compatíveis com as regiões da China.

- `RSA_AES_KEY_WRAP_SHA_256` - Um algoritmo de empacotamento híbrido de duas etapas que combina a criptografia do seu material de chave com uma chave simétrica AES que você gera e, em seguida, criptografa a chave simétrica AES com a chave de empacotamento pública RSA baixada e o algoritmo de empacotamento RSAES_OAEP_SHA_256.

  É necessário um algoritmo `RSA_AES_KEY_WRAP_SHA_*` de empacotamento para empacotar material de chave privada RSA, exceto nas regiões da China, onde você deve usar o `SM2PKE` algoritmo de empacotamento.
- `RSA_AES_KEY_WRAP_SHA_1` - Um algoritmo de empacotamento híbrido de duas etapas que combina a criptografia do seu material de chave com uma chave simétrica AES que você gera e, em seguida, criptografa a chave simétrica AES com a chave pública de empacotamento RSA baixada e o algoritmo de empacotamento RSAES_OAEP_SHA_1.

  É necessário um algoritmo `RSA_AES_KEY_WRAP_SHA_*` de empacotamento para empacotar material de chave privada RSA, exceto nas regiões da China, onde você deve usar o `SM2PKE` algoritmo de empacotamento.

- `RSAES_OAEP_SHA_256` — O algoritmo de criptografia RSA com Preenchimento da criptografia assimétrica ideal (OAEP) e função de hash SHA-256.
- `RSAES_OAEP_SHA_1` — O algoritmo de criptografia RSA com Preenchimento da criptografia assimétrica ideal (OAEP) e função de hash SHA-1.
- `RSAES_PKCS1_V1_5`(Obsoleto; em 10 de outubro de 2023, AWS KMS não oferece suporte ao algoritmo de encapsulamento RSAES_PKCS1_V1_5) — O algoritmo de criptografia RSA com o formato de preenchimento definido no PKCS #1 Versão 1.5.
- `SM2PKE`(Somente regiões da China) — Um algoritmo de criptografia baseado em curva elíptica definido pela OSCCA no GM/T 0003.4-2012.

Tópicos

- Fazer download da chave pública de empacotamento e do token de importação (console)
- Baixando a chave pública de empacotamento e o token de importação (AWS KMS API)

Fazer download da chave pública de empacotamento e do token de importação (console)

Você pode usar o AWS KMS console para baixar a chave pública de empacotamento e o token de importação.

1. Se você acabou de concluir as etapas para criar uma chave do KMS sem material de chave e está na página Download wrapping key and import token (Baixar chave de empacotamento e token de importação), vá para Step 9.
2. Faça login no console AWS Management Console e abra o AWS Key Management Service (AWS KMS) em https://console.aws.amazon.com/kms.
3. Para alterar o Região da AWS, use o seletor de região no canto superior direito da página.
4. No painel de navegação, escolha Chaves gerenciadas pelo cliente.

> **Tip**
>
> É possível importar material de chave somente para uma chave do KMS simétrica com uma Origin (Origem) de External (Import key material) (Externa [Importar material de chave]). Isso indica que a chave do KMS foi criada sem material de chave. Para adicionar a coluna Origin (Origem) à tabela, no canto superior direito da página, selecione o ícone de configurações

().
Ative Origin (Origem) e escolha Confirm (Confirmar).

5. Escolha o alias ou o ID da chave do KMS com importação pendente.
6. Expanda a seção Cryptographic configuration (Configuração criptográfica) e visualize seus valores. As guias estão abaixo da seção General configuration (Configuração geral).

   É possível importar material de chave somente para uma chave do KMS com uma Origin (Origem) de External (Import key material) (Externa [Importar material de chave]). Para obter informações sobre como criar chaves do KMS com material de chave importado, consulte Importação de material chave para AWS KMS chaves.
7. Escolha a guia Key material (Material de chaves) e, em seguida, Import key material (Importar material de chave).

   A guia Key material (Material de chave) aparece somente para chaves do KMS que tenham um valor Origin (Origem) de External (Import key material) (Externo (Importar material de chave)).
8. Em Selecionar especificação da chave de empacotamento, escolha a configuração da sua chave do KMS. Após a criação dessa chave, não será possível alterar a especificação da chave.
9. Para Select wrapping algorithm, escolha a opção que você usará para criptografar o material de chaves. Para obter mais informações sobre as opções, consulte Selecionar um algoritmo de empacotamento.
10. Escolha Download wrapping key and import token (fazer download da chave de empacotamento e token de importação) e salve o arquivo.

    Se houver a opção Next (Próximo), para continuar o processo agora, selecione Next (Próximo). Para continuar mais tarde, selecione Cancel (Cancelar).
11. Descompacte o arquivo `.zip` que você salvou na etapa anterior (`Import_Parameters_<key_id>_<timestamp>`).

    A pasta contém os seguintes arquivos:

    - Uma chave pública de empacotamento em um arquivo chamado`WrappingPublicKey.bin`.
    - Um token de importação em um arquivo chamado `ImportToken.bin`.
    - Um arquivo de texto chamado README.txt. Este arquivo contém informações sobre a chave pública de empacotamento, o algoritmo de encapsulamento a ser usado para criptografar o

material de chaves e a data e hora em que a chave pública de empacotamento e o token de importação expiram.

12. Para continuar o processo, consulte criptografe o material de chaves.

Baixando a chave pública de empacotamento e o token de importação (AWS KMS API)

Para baixar a chave pública e o token de importação, use a GetParametersForImportAPI. Especifique a chave do KMS que será associada ao material de chave importado. Essa chave do KMS deve ter um valor de Origem de `EXTERNAL`.

Este exemplo especifica o algoritmo de empacotamento `RSA_AES_KEY_WRAP_SHA_256`, a especificação de chave pública de empacotamento RSA_3072 e um exemplo de ID de chave. Substitua esses valores de exemplo por valores válidos para download. Para o ID de chave, é possível usar o ID de chave ou o ARN da chave, mas não é possível usar um alias de nome ou ARN de alias nessa operação.

```
$ 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
```

Quando o comando é bem-sucedido, a saída é semelhante à seguinte:

```
{
    "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)"
}
```

Para preparar os dados para a próxima etapa, o base64 decodifica a chave pública e o token de importação e salva os valores decodificados nos arquivos.

Para o base64 decodificar a chave pública e o token de importação:

1. Copie a chave pública codificada em base64 (representada pela *chave pública codificada em base64* no exemplo de saída), cole-os em um novo arquivo e salve o arquivo. Dê um nome descritivo ao arquivo, como `PublicKey.b64`.
2. Use o OpenSSL para decodificar o conteúdo do arquivo base64 e salve os dados decodificados em um novo arquivo. O exemplo a seguir decodifica os dados no arquivo que você salvou na etapa anterior (`PublicKey.b64`) e salva a saída em um novo arquivo chamado `WrappingPublicKey.bin`.

   ```
   $ openssl enc -d -base64 -A -in PublicKey.b64 -out WrappingPublicKey.bin
   ```

3. Copie o token de importação codificado em base64 (representado pelos *token de importação codificado em base64* no exemplo de saída), cole-os em um novo arquivo e salve o arquivo. Dê ao arquivo um nome descritivo, por exemplo `importtoken.b64`.
4. Use o OpenSSL para decodificar o conteúdo do arquivo base64 e salve os dados decodificados em um novo arquivo. O exemplo a seguir decodifica os dados no arquivo que você salvou na etapa anterior (`ImportToken.b64`) e salva a saída em um novo arquivo chamado `ImportToken.bin`.

   ```
   $ openssl enc -d -base64 -A -in importtoken.b64 -out ImportToken.bin
   ```

Vá para Etapa 3: Criptografar o material de chave.

Importar o material de chave — etapa 3: Criptografar o material de chave

Depois de fazer download da chave pública e importar o token, criptografe seu material de chaves usando a chave pública que você baixou e o algoritmo de empacotamento que você especificou. Se precisar substituir a chave pública ou o token de importação, ou alterar o algoritmo de empacotamento, você deverá baixar uma nova chave pública e importar o token. Para obter informações sobre as chaves públicas e os algoritmos de empacotamento que AWS KMS oferecem suporte, consulte Selecionar uma especificação de chave pública de empacotamento e. Selecionar um algoritmo de empacotamento

O material de chaves deve estar em formato binário. Para obter informações detalhadas, consulte Requisitos para material de chave importada.

> **Note**
>
> Para pares de chaves assimétricas, criptografe e importe somente a chave privada. AWS KMS deriva a chave pública da chave privada.
> A combinação a seguir NÃO é compatível: material de chave ECC_NIST_P521, especificação de chave de empacotamento pública RSA_2048 e um algoritmo de empacotamento RSAES_OAEP_SHA_*.
> Não é possível empacotar diretamente o material de chave ECC_NIST_P521 com uma chave de empacotamento pública RSA_2048. Use uma chave de empacotamento maior ou um algoritmo de empacotamento RSA_AES_KEY_WRAP_SHA_*.
> Os algoritmos de encapsulamento RSA_AES_KEY_WRAP_SHA_256 e RSA_AES_KEY_WRAP_SHA_1 não são suportados nas regiões da China.

Geralmente, você criptografa o material de chaves ao exportá-lo do HSM (módulo de segurança de hardware) ou do sistema de gerenciamento de chaves. Para obter informações sobre como exportar material de chaves em formato binário, consulte a documentação do HSM ou do sistema de gerenciamento de chaves. Você também pode consultar a seção a seguir, que fornece uma demonstração da prova de conceito usando OpenSSL.

Ao criptografar o material de chaves, use o mesmo algoritmo de empacotamento que você especificou quando fez download da chave pública e do token de importação. Para encontrar o algoritmo de empacotamento que você especificou, consulte o evento de CloudTrail log da GetParametersForImportsolicitação associada.

Gerar material de chave para testes

Os comandos do OpenSSL a seguir geram material de chave de cada tipo compatível para testes. Esses exemplos são fornecidos somente para testes e proof-of-concept demonstrações. Para sistemas de produção, use um método mais seguro para gerar o material de chaves, como um módulo de segurança de hardware ou um sistema de gerenciamento de chaves.

Para converter as chaves privadas de pares de chaves assimétricas em formato codificado em DER, canalize o comando de geração de material de chave para o comando `openssl pkcs8` a seguir. O parâmetro `topk8` direciona o OpenSSL a usar uma chave privada como entrada e retornar uma chave formatada PKCS#8. (O comportamento padrão é o oposto.)

```
openssl pkcs8 -topk8 -outform der -nocrypt
```

Os comandos a seguir geram material de chave de teste para cada tipo de chave compatível.

- Chave de criptografia simétrica (32 bytes)

  Esse comando gera uma chave simétrica de 256 bits (sequência aleatória de 32 bytes) e a salva no arquivo `PlaintextKeyMaterial.bin`. Não é necessário codificar esse material de chaves.

  ```
  openssl rand -out PlaintextKeyMaterial.bin 32
  ```

  Somente nas regiões da China, você deve gerar uma chave simétrica de 128 bits (sequência aleatória de 16 bytes).

  ```
  openssl rand -out PlaintextKeyMaterial.bin 16
  ```

- Chaves de HMAC

  Esse comando gera uma sequência de bytes aleatória do tamanho especificado. Não é necessário codificar esse material de chaves.

  O comprimento da chave de HMAC deve corresponder ao comprimento definido pela especificação da chave do KMS. Por exemplo, se a chave do KMS for HMAC_384, você deverá importar uma chave de 384 bits (48 bytes).

  ```
  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
  ```

- Chaves privadas 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
  ```

- Chaves privadas ECC

```
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
```

- Chaves privadas SM2 (somente regiões da China)

```
openssl genpkey -algorithm ec -pkeyopt ec_paramgen_curve:sm2 | openssl pkcs8 -topk8 -
outform der -nocrypt > SM2_PrivateKey.der
```

Exemplos de material de chave de criptografia com OpenSSL

Os exemplos a seguir mostram como usar o OpenSSL para criptografar seu material de chaves com a chave pública que você baixou. Para criptografar seu material de chave usando uma chave pública SM2 (somente regiões da China), use a `SM2OfflineOperationHelper` classe.

> **Important**
>
> Esses exemplos são apenas uma demonstração da prova de conceito. Para sistemas de produção, use um método mais seguro (tal como um HSM ou sistema de gerenciamento de chaves comercial) para gerar e armazenar seu material de chaves.
> A combinação a seguir NÃO é compatível: material de chave ECC_NIST_P521, especificação de chave de empacotamento pública RSA_2048 e um algoritmo de empacotamento RSAES_OAEP_SHA_*.
> Não é possível empacotar diretamente o material de chave ECC_NIST_P521 com uma chave de empacotamento pública RSA_2048. Use uma chave de empacotamento maior ou um algoritmo de empacotamento RSA_AES_KEY_WRAP_SHA_*.

RSAES_OAEP_SHA_1

AWS KMS suporta o RSAES_OAEP_SHA_1 para chaves de criptografia simétricas (SYMMETRIC_DEFAULT), chaves privadas de curva elíptica (ECC), chaves privadas SM2 e chaves HMAC.

O RSAES_OAEP_SHA_1 não é compatível com chaves privadas de RSA. Além disso, não é possível usar uma chave pública de empacotamento RSA_2048 com nenhum algoritmo de empacotamento RSAES_OAEP_SHA_* para empacotar uma chave privada ECC_NIST_P521 (secp521r1). Você dever usar uma chave pública de empacotamento maior ou um algoritmo de empacotamento RSA_AES_KEY_WRAP.

O exemplo a seguir criptografa seu material de chaves com a chave pública que você baixou e com o algoritmo de encapsulamento RSAES_OAEP_SHA_1 e o salva no arquivo `EncryptedKeyMaterial.bin`.

Neste exemplo:

- *`WrappingPublicKey.bin`* é o arquivo que contém a chave pública de empacotamento baixada.
- *`PlaintextKeyMaterial.bin`* é o arquivo que contém o material de chave que você está criptografando, como `PlaintextKeyMaterial.bin`, `HMAC_384_PlaintextKey.bin` ou `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 suporta o RSAES_OAEP_SHA_256 para chaves de criptografia simétricas (SYMMETRIC_DEFAULT), chaves privadas de curva elíptica (ECC), chaves privadas SM2 e chaves HMAC.

O RSAES_OAEP_SHA_256 não é compatível com chaves privadas de RSA. Além disso, não é possível usar uma chave pública de empacotamento RSA_2048 com nenhum algoritmo de empacotamento RSAES_OAEP_SHA_* para empacotar uma chave privada ECC_NIST_P521 (secp521r1). Você dever usar uma chave pública maior ou um algoritmo de empacotamento RSA_AES_KEY_WRAP.

O exemplo a seguir criptografa o material de chaves com a chave pública que você baixou e com o algoritmo de empacotamento RSAES_OAEP_SHA_256 e o salva no arquivo `EncryptedKeyMaterial.bin`.

Neste exemplo:

- *`WrappingPublicKey.bin`* é o arquivo que contém a chave de empacotamento pública baixada. Se você fez download da chave pública do console, esse arquivo será chamado `wrappingKey_`*`KMS key_key_ID_timestamp`* (por exemplo, `wrappingKey_f44c4e20-f83c-48f4-adc6-a1ef38829760_0809092909`).
- *`PlaintextKeyMaterial.bin`* é o arquivo que contém o material de chave que você está criptografando, como `PlaintextKeyMaterial.bin`, `HMAC_384_PlaintextKey.bin` ou `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

O algoritmo de empacotamento RSA_AES_KEY_WRAP_SHA_1 envolve duas operações de criptografia.

1. Criptografe o material de chaves com uma chave simétrica AES que você gera e um algoritmo de criptografia simétrica AES.

2. Criptografe a chave simétrica AES que você usou com a chave pública que você baixou e o algoritmo de empacotamento RSAES_OAEP_SHA_1.

AWS KMS suporta algoritmos de empacotamento RSA_AES_KEY_WRAP_SHA_* para todos os tipos suportados de material de chave importado e todas as especificações de chave pública suportadas. Os algoritmos RSA_AES_KEY_WRAP_SHA_* são os únicos algoritmos de empacotamento compatíveis para agrupar material de chave RSA.

O algoritmo de empacotamento RSA_AES_KEY_WRAP_SHA_1 requer OpenSSL versão 3.x ou superior.

1. Gerar uma chave de criptografia simétrica AES de 256 bits

   Esse comando gera uma chave de criptografia simétrica AES que consiste em 256 bits aleatórios e a salva no arquivo `aes-key.bin`

   ```
   # Generate a 32-byte AES symmetric encryption key
   $ openssl rand -out aes-key.bin 32
   ```

2. Criptografar o material de chave com a chave de criptografia simétrica AES

   Esse comando criptografa o material da chave com a chave de criptografia simétrica AES e salva o material da chave criptografada no arquivo `key-material-wrapped.bin`.

   Neste comando de exemplo:

   - *`PlaintextKeyMaterial.bin`* é o arquivo que contém o material de chave que você está importando, como `PlaintextKeyMaterial.bin`, `HMAC_384_PlaintextKey.bin`, `RSA_3072_PrivateKey.der` ou `ECC_NIST_P521_PrivateKey.der`.
   - *`aes-key.bin`* é o arquivo que contém a chave de criptografia simétrica AES de 256 bits que você gerou no comando anterior.

   ```
   # 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. Criptografar a chave de criptografia simétrica AES com a chave pública

   Esse comando criptografa sua chave de criptografia simétrica AES com a chave pública que você baixou e o algoritmo de empacotamento RSAES_OAEP_SHA_1, a codifica em DER e a salva no arquivo `aes-key-wrapped.bin`.

   Neste comando de exemplo:

   - *`WrappingPublicKey.bin`* é o arquivo que contém a chave de empacotamento pública baixada. Se você fez download da chave pública do console, esse arquivo será chamado `wrappingKey_`*`KMS key_key_ID_timestamp`* (por exemplo, `wrappingKey_f44c4e20-f83c-48f4-adc6-a1ef38829760_0809092909`
   - *`aes-key.bin`* é o arquivo que contém a chave de criptografia simétrica AES de 256 bits que você gerou no primeiro comando dessa sequência de exemplos.

```
# 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. Gerar o arquivo a ser importado

   Concatene o arquivo com o material da chave criptografada e o arquivo com a chave AES criptografada. Salve-os no arquivo `EncryptedKeyMaterial.bin`, que é o arquivo que você importará no Etapa 4: Importar o material de chave.

   Neste comando de exemplo:

   - *`key-material-wrapped.bin`* é o arquivo que contém o material de chaves criptografado.

- *aes-key-wrapped.bin* é o arquivo que contém a chave de criptografia AES criptografada.

```
# 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

O algoritmo de empacotamento RSA_AES_KEY_WRAP_SHA_256 envolve duas operações de criptografia.

1. Criptografe o material de chaves com uma chave simétrica AES que você gera e um algoritmo de criptografia simétrica AES.
2. Criptografe a chave simétrica AES que você usou com a chave pública que você baixou e o algoritmo de empacotamento RSAES_OAEP_SHA_256.

AWS KMS suporta algoritmos de empacotamento RSA_AES_KEY_WRAP_SHA_* para todos os tipos suportados de material de chave importado e todas as especificações de chave pública suportadas. Os algoritmos RSA_AES_KEY_WRAP_SHA_* são os únicos algoritmos de empacotamento compatíveis para agrupar material de chave RSA.

O algoritmo de empacotamento RSAES_OAEP_SHA_256 requer OpenSSL versão 3.x ou superior.

1. Gerar uma chave de criptografia simétrica AES de 256 bits

   Esse comando gera uma chave de criptografia simétrica AES que consiste em 256 bits aleatórios e a salva no arquivo `aes-key.bin`

   ```
   # Generate a 32-byte AES symmetric encryption key
   $ openssl rand -out aes-key.bin 32
   ```

2. Criptografar o material de chave com a chave de criptografia simétrica AES

   Esse comando criptografa o material da chave com a chave de criptografia simétrica AES e salva o material da chave criptografada no arquivo `key-material-wrapped.bin`.

   Neste comando de exemplo:

- *PlaintextKeyMaterial.bin* é o arquivo que contém o material de chave que você está importando, como `PlaintextKeyMaterial.bin`, `HMAC_384_PlaintextKey.bin`, `RSA_3072_PrivateKey.der` ou `ECC_NIST_P521_PrivateKey.der`.
- *aes-key.bin* é o arquivo que contém a chave de criptografia simétrica AES de 256 bits que você gerou no comando anterior.

```
# 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. Criptografar a chave de criptografia simétrica AES com a chave pública

   Esse comando criptografa a chave de criptografia simétrica AES com a chave pública que você baixou e o algoritmo de empacotamento RSAES_OAEP_SHA_256, a codifica em DER e a salva no arquivo `aes-key-wrapped.bin`.

   Neste comando de exemplo:

   - *WrappingPublicKey.bin* é o arquivo que contém a chave de empacotamento pública baixada. Se você fez download da chave pública do console, esse arquivo será chamado `wrappingKey_`*KMS key_key_ID_timestamp* (por exemplo, `wrappingKey_f44c4e20-f83c-48f4-adc6-a1ef38829760_0809092909`
   - *aes-key.bin* é o arquivo que contém a chave de criptografia simétrica AES de 256 bits que você gerou no primeiro comando dessa sequência de exemplos.

```
# 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. Gerar o arquivo a ser importado

   Concatene o arquivo com o material da chave criptografada e o arquivo com a chave AES criptografada. Salve-os no arquivo `EncryptedKeyMaterial.bin`, que é o arquivo que você importará no Etapa 4: Importar o material de chave.

   Neste comando de exemplo:

   - *`key-material-wrapped.bin`* é o arquivo que contém o material de chaves criptografado.
   - *`aes-key-wrapped.bin`* é o arquivo que contém a chave de criptografia AES criptografada.

```
# Combine the encrypted AES key and encrypted key material in a file
$ cat aes-key-wrapped.bin key-material-wrapped.bin > EncryptedKeyMaterial.bin
```

Vá para Etapa 4: Importar o material de chave.

Importar o material de chave — etapa 4: Importar o material de chave

Depois de criptografar o material de chave, você pode importá-lo para uso com uma AWS KMS key. Para importar o material de chaves, você faz upload do material de chaves criptografado de Etapa 3: Criptografar o material de chave e o token de importação que você baixou em Etapa 2: Fazer download da chave pública de empacotamento e do token de importação. É necessário importar o material de chaves para a mesma chave do KMS que especificou quando você baixou a chave pública e o token de importação. Quando o material da chaves é importado com êxito, o estado da chave da chave do KMS muda para `Enabled`, e você pode usar a chave do KMS em operações de criptografia.

Ao importar material de chaves, é possível definir uma hora de expiração opcional para ele. Quando o material de chave perde a validade, o AWS KMS exclui o material de chave e a chave KMS se torna inutilizável. Para usar a chave do KMS em operações criptográficas, você deve reimportar o mesmo material de chaves. Depois de importar o material de chaves, você não pode definir, alterar ou cancelar a data de expiração da importação atual. Para alterar esses valores, você deve deletar e reimportar o mesmo material de chaves.

Para importar material chave, você pode usar o AWS KMS console ou a ImportKeyMaterialAPI. É possível usar a API diretamente, fazendo solicitações HTTP ou usando AWS SDKs, o AWS Command Line Interface ou o AWS Tools for PowerShell.

Quando você importa o material da chave, uma ImportKeyMaterialentrada é adicionada ao seu AWS CloudTrail registro para registrar a `ImportKeyMaterial` operação. A CloudTrail entrada é a mesma se você usa o AWS KMS console ou a AWS KMS API.

Definir um prazo de validade (opcional)

Ao importar o material de chave para a chave do KMS, você pode definir uma data e hora de validade opcionais para o material de chave de até 365 dias a partir da data de importação. Quando o material de chave importado expira, o AWS KMS o exclui. Essa ação altera estado de chave da chave do KMS para `PendingImport`, impedindo que ela seja usada em operações de criptografia. Para usar a chave do KMS, você deve reimportar uma cópia do material de chave original.

Garantir que o material de chave importado expire com frequência pode ajudar a atender aos requisitos regulatórios, mas aumenta o risco dos dados criptografados sob a chave do KMS. Até que você reimporte uma cópia do material da chave original, uma chave do KMS com material de chave expirado ficará inutilizável, e todos os dados criptografados sob a chave do KMS ficarão inacessíveis. Se você não reimportar o material da chave por qualquer motivo, inclusive por perda da cópia do material da chave original, a chave do KMS ficará permanentemente inutilizável, e os dados criptografados sob a chave do KMS ficarão irrecuperáveis.

Para mitigar esse risco, verifique se sua cópia do material de chaves importado está acessível e crie um sistema para excluir e reimportar o material da chave antes que ele expire e interrompa sua workload da AWS. Recomendamos definir um alarme para a expiração do material de chave importado, o que lhe dará tempo suficiente para reimportar o material da chave antes que ele expire. Você também pode usar seus CloudTrail registros para auditar operações que importam (e reimportam) material de chave e excluem material de chave importado, e a AWS KMS operação para excluir material de chave expirado.

Você pode importar material de chave diferente para a chave do KMS, e o AWS KMS não pode restaurar, recuperar ou reproduzir o material da chave excluído. Em vez de definir um prazo de validade, você pode excluir e reimportar o material de chave importado de maneira programática periodicamente, mas os requisitos para reter uma cópia do material da chave original são os mesmos.

Ao importar o material de chave, você determina se o material de chave importado expirará e quando isso ocorrerá. Mas é possível ativar e desativar a expiração ou definir um novo

prazo de validade excluindo e reimportando o material da chave. Use o `ExpirationModel` parâmetro de ImportKeyMaterialpara ativar (`KEY_MATERIAL_EXPIRES`) e desativar a expiração (`KEY_MATERIAL_DOES_NOT_EXPIRE`) e o `ValidTo` parâmetro para definir o tempo de expiração. O tempo máximo é de 365 dias a partir da importação de dados. Não há mínimo, mas o tempo deve estar no futuro.

Importar o material de chave (console)

Você pode usar o AWS Management Console para importar o material de chaves.

1. Se você estiver na página Upload your wrapped key material (Fazer upload de chave empacotada), vá para Step 8.
2. Faça login no AWS Management Console e abra o console do AWS Key Management Service (AWS KMS) em https://console.aws.amazon.com/kms.
3. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.
4. No painel de navegação, escolha Customer managed keys (Chaves gerenciadas pelo cliente).
5. Escolha o alias ou o ID da chave do KMS para a qual você baixou a chave pública e o token de importação.
6. Expanda a seção Cryptographic configuration (Configuração criptográfica) e visualize seus valores. As guias estão na página de detalhes de uma chave do KMS, abaixo da seção General configuration (Configuração geral).

   É possível importar material de chaves somente para uma chave do KMS com uma Origin (Origem) de External (Import key material) (Externa [Importar material de chave]). Para obter informações sobre como criar chaves do KMS com material de chave importado, consulte Importação de material chave para AWS KMS chaves.
7. Escolha a guia Key material (Material de chaves) e, em seguida, Import key material (Importar material de chave). A guia Key material (Material de chave) aparece somente para chaves do KMS com um valor Origin (Origem) de External (Import key material) (Externo (Importar material de chave)).

   Se você baixou o material da chave, o token de importação e criptografou o material da chave, escolha Next (Avançar).
8. Na seção Encrypted key material and import token (Material de chave criptografada e token de importação), faça o seguinte:

a. Em Wrapped key material (material de chave empacotada), escolha Choose file (Escolher arquivo). Faça upload do arquivo que contém o material de chaves encapsulado (criptografado).

b. Em Import token (Importar token), escolha Choose file (Escolher arquivo). Faça upload do arquivo que contém o token de importação obtido por download.

9. Na seção Expiration option (Opção de expiração), determine se o material de chave expira. Para definir uma data e hora de expiração, escolha Key material expires (O material de chaves expira), e use o calendário para selecionar uma data e hora. Você pode especificar uma data de até 365 dias da data e hora atuais.
10. Selecione Upload key material (Fazer upload do material de chaves).

Importar material de chave (API do AWS KMS)

Para importar material chave, use a ImportKeyMaterialoperação. O exemplo a seguir usa a AWS CLI, mas você pode usar qualquer linguagem de programação compatível.

Para usar este exemplo:

1. Substitua *1234abcd-12ab-34cd-56ef-1234567890ab* pelo ID da chave do KMS que você especificou quando baixou a chave pública e o token de importação. Para identificar a chave do KMS, use seu ID de chave ou ARN de chave. Você não pode usar um nome de alias ou ARN de alias para esta operação.
2. Substitua *EncryptedKeyMaterial.bin* pelo nome do arquivo que contém o material de chaves criptografado.
3. Substitua *ImportToken.bin* pelo nome do arquivo que contém o token de importação.
4. Se você quiser que o material da chave importada expire, defina o valor do parâmetro `expiration-model` para seu valor padrão, `KEY_MATERIAL_EXPIRES`, ou omita o parâmetro `expiration-model`. Em seguida, substitua o valor do parâmetro `valid-to` com a data e a hora em que você deseja que o material da chave expire. A data e a hora podem ser de até 365 dias a partir do momento da solicitação.

```
$ 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 você não quiser que o material da chave importada expire, defina o valor do parâmetro `expiration-model` como `KEY_MATERIAL_DOES_NOT_EXPIRE` e omita o parâmetro `valid-to` do 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 o comando não for bem-sucedido, você poderá ver uma `KMSInvalidStateException` ou `NotFoundException`. Você poderá repetir a solicitação.

Armazenamentos de chaves personalizados

Um armazenamento de chaves é um local seguro para o armazenamento de chaves de criptografia. O armazenamento de chaves padrão no AWS KMS também oferece suporte a métodos para gerar e gerenciar as chaves que o armazena. Por padrão, material de chave de criptografia para AWS KMS keys que você cria no AWS KMS é gerado e protegido por módulos de segurança de hardware (HSMs), que são módulos criptográficos validados por FIPS 140-2. O material de chave de suas chaves do KMS nunca deixa seus HSMs sem criptografia.

Porém, se você precisar de ainda mais controle dos HSMs, poderá criar um armazenamento de chaves personalizado.

Um armazenamento de chaves personalizado é um armazenamento de chaves lógicas no AWS KMS baseado em um gerenciador de chaves fora do AWS KMS que você possui e gerencia. Armazenamentos de chaves personalizado unem a interface conveniente e completa de gerenciamento de chaves do AWS KMS com a capacidade de possuir e controlar material de chaves personalizado e operações de criptografia. Ao usar uma chave do KMS em um armazenamento de chaves personalizado, as operações de criptografia são executadas pelo gerenciador de chaves usando chaves de criptografia. Como resultado, você assume mais responsabilidade pela disponibilidade e durabilidade das chaves de criptografia e pela operação dos HSMs.

O AWS KMS é compatível com dois tipos de armazenamento de chaves.

- Um armazenamento de chaves do AWS CloudHSM é um armazenamento de chaves personalizado do AWS KMS baseado em um cluster do AWS CloudHSM. Quando você cria uma chave do KMS no seu armazenamento de chaves do AWS CloudHSM, o AWS KMS gera uma chave simétrica Advanced Encryption Standard (AES) de 256 bits, persistente e não exportável no cluster do AWS CloudHSM associado. Esse material de chaves nunca deixa os clusters do AWS CloudHSM sem estarem criptografados. Ao usar uma chave do KMS no armazenamento de chaves do AWS CloudHSM, as operações de criptografia são executadas nos HSMs do cluster. Os clusters do AWS CloudHSM são baseados em módulos de segurança de hardware (HSMs) certificados pelo FIPS 140-2 Nível 3.
- Um armazenamento de chaves externas é um armazenamento de chaves do AWS KMS personalizado com base em um gerenciador de chaves externas fora da AWS que você possui e controla. Ao usar uma chave do KMS em um armazenamento de chaves externas, todas as operações de criptografia e descriptografia são executadas pelo gerenciador de chaves externas usando suas chaves de criptografia. Os armazenamentos de chaves externas são criados para oferecer suporte a uma variedade de gerenciadores de chaves externas de diferentes fornecedores.

  O AWS KMS nunca visualiza, acessa ou interage diretamente com seu gerenciador de chaves externas ou chaves de criptografia. Ao criptografar ou descriptografar com uma chave do KMS em um armazenamento de chaves externas, a operação é executada pelo gerenciador de chaves externas usando suas chaves externas. Você retém o controle total sobre suas chaves de criptografia, inclusive a capacidade de recusar ou interromper uma operação de criptografia sem interagir com a AWS. Porém, por causa da distância e do processamento adicional, as chaves do KMS em um armazenamento de chaves externas podem ter menor latência e performance e podem ter características de disponibilidade diferentes das chaves do KMS com material de chave no AWS KMS. Para obter mais informações sobre gerenciadores de chaves compatíveis com o atributo de armazenamento de chaves externo AWS KMS, consulte Quais fornecedores externos oferecem suporte à especificação XKS Proxy? em Perguntas frequentes sobre o AWS Key Management Service.

Esses dois tipos de armazenamentos de chaves personalizado são bem diferentes do armazenamento de chaves padrão do AWS KMS e são diferentes um do outro. Seus modelos de segurança, foco de responsabilidade, performance, preço e casos de uso também são muito diferentes. Antes de escolher um armazenamento de chaves personalizado, leia a documentação relacionada e confirme se a responsabilidade extra de configuração e manutenção é uma boa compensação pelo controle adicional. Porém, se as normas e regulamentações sob os quais você

opera exigirem controle direto do material da chave, um armazenamento de chaves personalizado poderá ser uma boa opção.

Recursos sem suporte

O AWS KMS não oferece suporte aos seguintes recursos em armazenamentos de chaves personalizados.

- Chaves do KMS assimétricas
- Pares de chaves de dados assimétricas
- Chaves do KMS de HMAC
- Chaves do KMS com material de chave importado
- Alternância automática de chaves
- Chaves de várias regiões

Tópicos

- AWS CloudHSM lojas principais
- Armazenamentos de chaves externas

AWS CloudHSM lojas principais

Um armazenamento de AWS CloudHSM chaves é um armazenamento de chaves personalizado apoiado por um AWS CloudHSM cluster. Quando você cria um AWS KMS keyem um armazenamento de chaves personalizado, AWS KMS gera e armazena material de chave não extraível para a chave KMS em um AWS CloudHSM cluster que você possui e gerencia. Ao usar uma chave do KMS em um armazenamento de chaves personalizado, as operações de criptografia são executadas nos HSMs no cluster. Esse recurso combina a conveniência e a ampla integração AWS KMS com o controle adicional de um AWS CloudHSM cluster em seu Conta da AWS.

AWS KMS fornece suporte completo de console e API para criar, usar e gerenciar seus armazenamentos de chaves personalizadas. Use as chaves do KMS no seu armazenamento de chaves personalizado da mesma maneira que você usa qualquer chave do KMS. Por exemplo, você pode usar as chaves do KMS para gerar chaves de dados e criptografar dados. Você também pode usar as chaves KMS em seu armazenamento de chaves personalizadas com AWS serviços que oferecem suporte a chaves gerenciadas pelo cliente.

Eu preciso de um armazenamento de chaves personalizado?

Para a maioria dos usuários, o armazenamento de AWS KMS chaves padrão, protegido por módulos criptográficos validados pelo FIPS 140-2, atende aos requisitos de segurança. Não é necessário adicionar uma camada extra de responsabilidade de manutenção nem uma dependência em um serviço adicional.

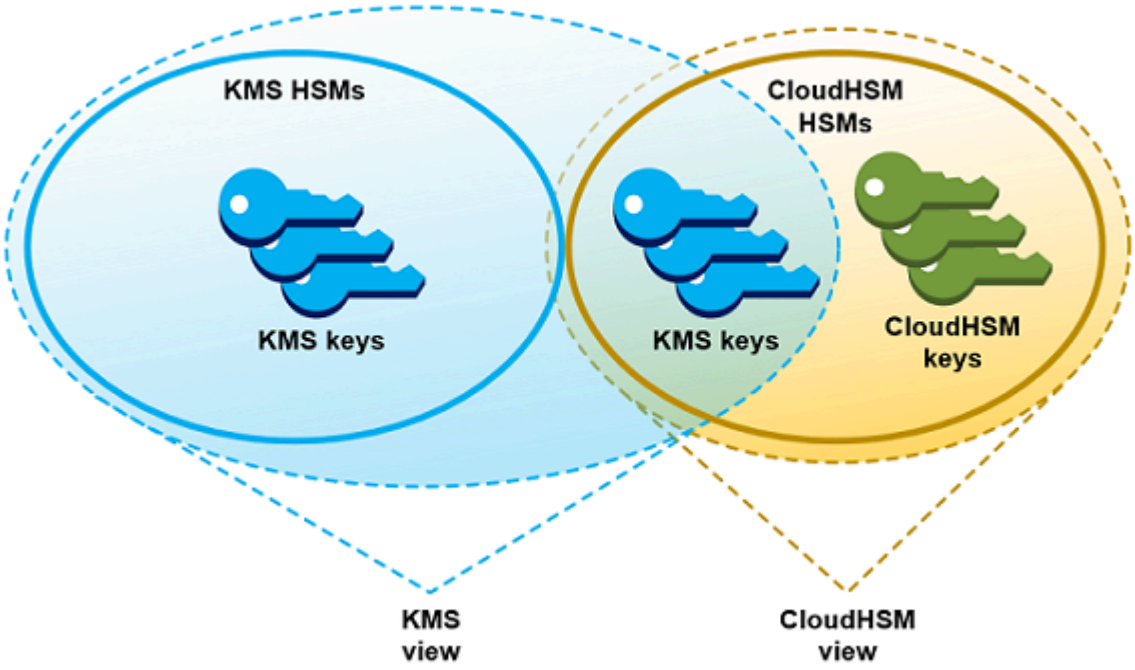
No entanto, você pode considerar a criação de um armazenamento de chaves personalizado se a sua organização tiver um dos seguintes requisitos:

- Algumas chaves precisam ser explicitamente protegidas em um único HSM locatário ou em um HSM sobre o qual você tem controle direto.
- Você precisa da capacidade de remover imediatamente o material chave do AWS KMS.
- Você precisa ser capaz de auditar todo o uso de suas chaves, independentemente de AWS KMS ou AWS CloudTrail.

Como funcionam os armazenamentos de chaves personalizados?

Cada armazenamento de chaves personalizadas está associado a um AWS CloudHSM cluster no seu Conta da AWS. Quando você conecta o armazenamento de chaves personalizadas ao cluster, AWS KMS cria a infraestrutura de rede para suportar a conexão. Em seguida, ele faz login no AWS CloudHSM cliente-chave no cluster usando as credenciais de um usuário criptográfico dedicado no cluster.

Você cria e gerencia seus armazenamentos de chaves personalizadas AWS KMS e cria e gerencia seus clusters de HSM em AWS CloudHSM. Ao criar AWS KMS keys em um armazenamento de chaves AWS KMS personalizado, você visualiza e gerencia as chaves KMS em AWS KMS. Mas você também pode visualizar e gerenciar o material de chaves deles AWS CloudHSM, assim como faria com outras chaves no cluster.



Você pode criar chaves KMS de criptografia simétrica com o material de chaves gerado AWS KMS em seu armazenamento de chaves personalizadas. Em seguida, use as mesmas técnicas para visualizar e gerenciar as chaves KMS em seu armazenamento de chaves personalizadas que você usa para chaves KMS no AWS KMS armazenamento de chaves. É possível controlar o acesso com políticas de chaves e do IAM, criar etiquetas e aliases, habilitar e desabilitar as chaves do KMS e programar a exclusão de chaves. Você pode usar as chaves KMS para operações criptográficas e usá-las com AWS serviços que se integram a. AWS KMS

Além disso, você tem controle total sobre o AWS CloudHSM cluster, incluindo a criação e exclusão de HSMs e o gerenciamento de backups. Você pode usar o AWS CloudHSM cliente e as bibliotecas de software compatíveis para visualizar, auditar e gerenciar o material de chaves de suas chaves KMS. Embora o armazenamento de chaves personalizadas esteja desconectado, AWS KMS não é possível acessá-lo e os usuários não podem usar as chaves KMS no armazenamento de chaves personalizadas para operações criptográficas. Essa camada adicional de controle torna os armazenamentos de chaves personalizados uma excelente solução para as organizações que necessitam dela.

Por onde começar?

Para criar e gerenciar um armazenamento de AWS CloudHSM chaves, você usa recursos de AWS KMS AWS CloudHSM e.

1. Comece em AWS CloudHSM. Crie um cluster do AWS CloudHSM ativo ou selecione um cluster existente. O cluster deve conter pelo menos dois HSMs ativos em diferentes zonas de disponibilidade. Crie uma conta de usuário de criptografia (CU) dedicado nesse cluster para o AWS KMS.
2. Em AWS KMS, crie um armazenamento de chaves personalizado associado ao AWS CloudHSM cluster selecionado. AWS KMS fornece uma interface de gerenciamento completa que permite criar, visualizar, editar e excluir seus repositórios de chaves personalizados.
3. Quando você estiver pronto para usar seu armazenamento de chaves personalizadas, conecte-o ao AWS CloudHSM cluster associado. AWS KMS cria a infraestrutura de rede necessária para suportar a conexão. Ele faz login no cluster usando as credenciais da conta de usuário de criptografia dedicado para que possa gerar e gerenciar o material de chaves no cluster.
4. Agora, você pode criar chaves do KMS de criptografia simétrica em seu armazenamento personalizado de chaves. Basta especificar esse armazenamento de chaves personalizado ao criar a chave do KMS.

Se você ficar preso em alguma etapa, é possível encontrar ajuda no tópico Solucionar problemas de um armazenamento de chaves personalizado. Se a sua pergunta não for respondida, use o link de comentários na parte inferior de cada página deste guia ou publique uma pergunta no fórum de discussão do AWS Key Management Service.

Cotas

AWS KMS permite até 10 armazenamentos de chaves personalizadas em cada Conta da AWS região, incluindo armazenamentos de AWS CloudHSM chaves e armazenamentos de chaves externos, independentemente do estado da conexão. Além disso, há cotas de AWS KMS solicitação sobre o uso de chaves KMS em um AWS CloudHSM armazenamento de chaves.

Definição de preço

Para obter informações sobre o custo dos armazenamentos de chaves AWS KMS personalizadas e das chaves gerenciadas pelo cliente em um repositório de chaves personalizadas, consulte AWS Key Management Service preços. Para obter informações sobre o custo de AWS CloudHSM clusters e HSMs, consulte AWS CloudHSM Preços.

Regiões

AWS KMS oferece suporte às AWS CloudHSM principais lojas em todos os Regiões da AWS lugares onde AWS KMS há suporte, exceto na Ásia-Pacífico (Melbourne), China (Pequim), China (Ningxia) e Europa (Espanha).

Recursos sem suporte

AWS KMS não oferece suporte aos seguintes recursos em armazenamentos de chaves personalizadas.

- Chaves do KMS assimétricas
- Pares de chaves de dados assimétricas
- Chaves do KMS de HMAC
- Chaves do KMS com material de chave importado
- Alternância automática de chaves
- Chaves de várias regiões

Tópicos

- Conceitos de armazenamento de chaves do AWS CloudHSM
- Controlar o acesso ao armazenamento de chaves do AWS CloudHSM
- Gerenciar um armazenamento de chaves personalizado do CloudHSM
- Gerenciar chaves do KMS em um armazenamento de chaves do CloudHSM
- Solucionar problemas de um armazenamento de chaves personalizado

Conceitos de armazenamento de chaves do AWS CloudHSM

Este tópico explica alguns dos conceitos usados nos armazenamentos de chaves do AWS CloudHSM.

Armazenamento de chaves do AWS CloudHSM

Um armazenamento de chaves do AWS CloudHSM é um armazenamento de chaves personalizado associado a um cluster do AWS CloudHSM que você possui e gerencia. Os clusters do AWS CloudHSM são baseados em módulos de segurança de hardware (HSMs) certificados pelo FIPS 140-2 Nível 3.

Quando você cria uma chave do KMS no seu armazenamento de chaves do AWS CloudHSM, o AWS KMS gera uma chave simétrica Advanced Encryption Standard (AES) de 256 bits, persistente e

não exportável no cluster do AWS CloudHSM associado. Esse material de chaves nunca deixa seus HSMs sem estarem criptografados. Ao usar uma chave do KMS em um armazenamento de chaves do AWS CloudHSM, as operações de criptografia são executadas nos HSMs no cluster.

Armazenamentos de chaves do AWS CloudHSM combinam a interface conveniente e abrangente de gerenciamento de chaves do AWS KMS com os controles adicionais fornecidos por um cluster do AWS CloudHSM em sua Conta da AWS. Esse recurso integrado permite que você crie, gerencie e use chaves do KMS no AWS KMS, ao mesmo tempo em que mantém controle total sobre os HSMs que armazenam seu material de chaves, incluindo gerenciamento de clusters, HSMs e backups. Você pode usar o console e as APIs do AWS KMS para gerenciar o armazenamento de chaves do AWS CloudHSM e suas chaves do KMS. Você também pode usar o console do AWS CloudHSM, as APIs, o software cliente e a bibliotecas de software associadas para gerenciar o cluster associado.

Você pode visualizar e gerenciar seu armazenamento de chaves do AWS CloudHSM, editar suas propriedades e conectá-lo e desconectá-lo do cluster do AWS CloudHSM associado. Se precisar excluir um armazenamento de chaves do AWS CloudHSM, você deverá primeiro excluir as chaves do KMS no armazenamento de chaves do AWS CloudHSM, agendando a exclusão e esperando até que o período de tolerância expire. A exclusão do armazenamento de chaves do AWS CloudHSM remove o recurso do AWS KMS, mas não afeta o cluster do AWS CloudHSM.

AWS CloudHSMCluster do

Todo armazenamento de chaves do AWS CloudHSM é associado a um cluster do AWS CloudHSM. Quando você cria uma AWS KMS key no armazenamento de chaves do AWS CloudHSM, o AWS KMS cria seu material de chaves no cluster associado. Quando você usa uma chave do KMS no armazenamento de chaves do AWS CloudHSM, a operação de criptografia é realizada no cluster associado.

Cada cluster do AWS CloudHSM pode ser associado a apenas um armazenamento de chaves do AWS CloudHSM. O cluster que você escolher não pode ser associado a outro armazenamento de chaves do AWS CloudHSM ou compartilhar um histórico de backup com um cluster associado a outro armazenamento de chaves do AWS CloudHSM. O cluster deve estar inicializado e ativo, além de estar na mesma Conta da AWS e região que o armazenamento de chaves do AWS CloudHSM. Você pode criar um novo cluster ou usar um existente. O AWS KMS não requer o uso exclusivo do cluster. Para criar chaves do KMS no armazenamento de chaves do AWS CloudHSM, seu cluster associado deve conter pelo menos dois HSMs ativos. Todas as outras operações exigem apenas um HSM.

Você especifica o cluster do AWS CloudHSM ao criar o armazenamento de chaves do AWS CloudHSM, e não é possível alterá-lo. No entanto, você pode substituir qualquer cluster que compartilha um histórico de backup pelo cluster original. Isso permite a você excluir o cluster, se necessário, e substituí-lo por um cluster criado a partir de um de seus backups. Você mantém controle total do cluster do AWS CloudHSM associado para que você possa gerenciar usuários e chaves, criar e excluir HSMs e usar e gerenciar backups.

Quando você estiver pronto para usar o armazenamento de chaves do AWS CloudHSM, conecte-o ao cluster do AWS CloudHSM associado. Você pode conectar e desconectar o armazenamento de chaves personalizado a qualquer momento. Se o armazenamento de chaves personalizado estiver conectado, você poderá criar e usar suas chaves do KMS. Se estiver desconectado, você poderá visualizar e gerenciar o armazenamento de chaves do AWS CloudHSM e as respectivas chaves do KMS. No entanto, você não poderá criar novas chaves do KMS nem usar as chaves do KMS no armazenamento de chaves do AWS CloudHSM para operações de criptografia.

Usuário de criptografia **`kmsuser`**

Para criar e gerenciar o material de chave no cluster do AWS CloudHSM associada em seu nome, o AWS KMS usa um usuário de criptografia (CU) do AWS CloudHSM no cluster chamado `kmsuser`. O CU `kmsuser` é uma conta CU padrão automaticamente sincronizada a todos os HSMs no cluster e salva em backups do cluster.

Antes de criar o armazenamento de chaves do AWS CloudHSM, você cria uma conta de usuário de criptografia `kmsuser` em seu cluster do AWS CloudHSM usando o comando createUser em cloudhsm_mgmt_util. Ao criar o armazenamento de chaves do AWS CloudHSM, você fornece a senha da conta `kmsuser` ao AWS KMS. Quando você se conecta ao armazenamento de chaves personalizado, o AWS KMS faz login no cluster como CU `kmsuser` e alterna sua senha. O AWS KMS criptografa sua senha de `kmsuser` antes de armazená-la em segurança. Quando a senha é alternada, a nova senha é criptografada e armazenada da mesma maneira.

O AWS KMS permanece conectado como `kmsuser` enquanto o armazenamento de chaves do AWS CloudHSM está conectado. Você não deve usar essa conta CU para outros fins. No entanto, você mantém o controle final do CU da conta `kmsuser`. A qualquer momento, você pode encontrar os identificadores de chave das chaves que o `kmsuser` possui. Se necessário, você pode desconectar o armazenamento de chaves personalizado, alterar a senha de `kmsuser`, fazer login no cluster como `kmsuser` e exibir e gerenciar as chaves pertencentes ao `kmsuser`.

Para obter instruções sobre como criar sua conta CU `kmsuser`, consulte Criar o Usuário de criptografia `kmsuser`.

Chaves do KMS em um armazenamento de chaves do AWS CloudHSM

Você pode usar o AWS KMS ou a API do AWS KMS para criar AWS KMS keys em um armazenamento de chaves do AWS CloudHSM. Use a mesma técnica que você usaria em qualquer chave do KMS. A única diferença é que você deve identificar o armazenamento de chaves do AWS CloudHSM e especificar que a origem do material de chave é o cluster do AWS CloudHSM.

Quando você cria uma chave do KMS em um armazenamento de chaves do AWS CloudHSM, o AWS KMS cria a chave do KMS no AWS KMS e gera uma chave de backup simétrica Advanced Encryption Standard (AES) de 256 bits, persistente e não exportável em seu cluster associado. Quando você usa a chave do AWS KMS em uma operação criptográfica, a operação é executada no cluster do AWS CloudHSM usando a chave AES baseada em cluster. Embora o AWS CloudHSM seja compatível com chaves simétricas e assimétricas de diferentes tipos, os armazenamentos de chave do AWS CloudHSM são compatíveis apenas com chaves de criptografia simétrica AES.

Você pode visualizar as chaves do KMS em um armazenamento de chaves do AWS CloudHSM no console do AWS KMS e usar opções do console para exibir o ID do armazenamento de chaves personalizado. Você também pode usar a DescribeKeyoperação para encontrar o ID do armazenamento de AWS CloudHSM chaves e o ID AWS CloudHSM do cluster.

As chaves do KMS em um armazenamento de chaves do AWS CloudHSM funcionam como qualquer outra chave do KMS no AWS KMS. Os usuários autorizados precisam das mesmas permissões para usar e gerenciar as chaves do KMS. Você pode usar os mesmos procedimentos do console e operações de API para visualizar e gerenciar as chaves do KMS em um armazenamento de chaves do AWS CloudHSM. Isso inclui a habilitar e desabilitar chaves do KMS, criar e usar etiquetas e aliases e definir e alterar políticas de chaves e do IAM. Você pode usar chaves do KMS em um armazenamento de chaves do AWS CloudHSM para operações de criptografia e usá-las com serviços da AWS integrados que ofereçam suporte ao uso de chaves gerenciadas pelo cliente. No entanto, não é possível habilitar a alternância de chaves automática ou importar material de chave para uma chave do KMS em um armazenamento de chaves do AWS CloudHSM.

Também é possível usar o mesmo processo para agendar a exclusão de uma chave do KMS em um armazenamento de chaves do AWS CloudHSM. Após o período de espera, o AWS KMS excluirá a chave do KMS. Em seguida, ele fará o possível para excluir o material de chave referente à chave do KMS do cluster do AWS CloudHSM associado. No entanto, pode ser necessário excluir manualmente o material de chaves órfãs do cluster e de seus backups.

Controlar o acesso ao armazenamento de chaves do AWS CloudHSM

Você pode usar políticas do IAM para controlar o acesso ao seu armazenamento de chaves do AWS CloudHSM e ao cluster do AWS CloudHSM. Você pode usar políticas de chaves, políticas do IAM e concessões para controlar o acesso às AWS KMS keys no seu armazenamento de chaves do AWS CloudHSM. Recomendamos que você forneça aos usuários, grupos e funções apenas as permissões que precisam para as tarefas que possivelmente executarão.

Tópicos

- Autorizar gerenciadores e usuários de armazenamento de chaves do AWS CloudHSM
- Autorizar o AWS KMS a gerenciar recursos do AWS CloudHSM e do Amazon EC2

Autorizar gerenciadores e usuários de armazenamento de chaves do AWS CloudHSM

Ao criar seu armazenamento de chaves do AWS CloudHSM, verifique se as entidades principais que usam e gerenciam têm apenas as permissões necessárias. A lista a seguir descreve as permissões mínimas necessárias para gerenciadores e usuários de armazenamento de chaves do AWS CloudHSM.

- As entidades principais que criam e gerenciam o armazenamento de chaves do AWS CloudHSM precisam das seguintes permissões para usar as operações de API do armazenamento de chaves do AWS CloudHSM.
  - `cloudhsm:DescribeClusters`
  - `kms:CreateCustomKeyStore`
  - `kms:ConnectCustomKeyStore`
  - `kms:DeleteCustomKeyStore`
  - `kms:DescribeCustomKeyStores`
  - `kms:DisconnectCustomKeyStore`
  - `kms:UpdateCustomKeyStore`
  - `iam:CreateServiceLinkedRole`
- As entidades principais que criam e gerenciam o cluster do AWS CloudHSM associado ao armazenamento de chaves do AWS CloudHSM precisam de permissão para criar e inicializar um cluster do AWS CloudHSM. Isso inclui permissão para criar ou usar uma Amazon Virtual Private Cloud (VPC), criar sub-redes e criar uma instância do Amazon EC2. Também pode ser necessário criar e excluir HSMs, além de gerenciar backups. Para obter as listas das permissões necessárias,

consulte Identity and access management for AWS CloudHSM (Gerenciamento de identidade e acesso para o) no Guia do usuário do AWS CloudHSM.

- As entidades principais que criam e gerenciam AWS KMS keys em seu armazenamento de chaves do AWS CloudHSM exigem as mesmas permissões que as que criam e gerenciam qualquer chave do KMS no AWS KMS. A política de chaves padrão para a chave do KMS em um armazenamento de chaves do AWS CloudHSM é idêntica à política de chaves padrão para chaves do KMS no AWS KMS. O controle de acesso por atributo (ABAC), que usa etiquetas e aliases para controlar o acesso a chaves do KMS, também é eficaz em chaves do KMS em armazenamentos de chaves do AWS CloudHSM.
- As entidades principais que usam as chaves do KMS no seu armazenamento de chaves do AWS CloudHSM para operações de criptografia precisam de permissão para executar a operação de criptografia com as chaves do KMS, como kms:Decrypt. Você pode fornecer essas permissões em uma política de chaves, política do IAM. No entanto, elas não precisam de permissões adicionais para usar uma chave do KMS em um armazenamento de chaves do AWS CloudHSM.

Autorizar o AWS KMS a gerenciar recursos do AWS CloudHSM e do Amazon EC2

Para oferecer suporte aos armazenamentos de chaves do AWS CloudHSM, o AWS KMS precisa de permissão para obter informações sobre seus clusters do AWS CloudHSM. Ele também precisa de permissão para criar a infraestrutura de rede que conecta seu armazenamento de chaves do AWS CloudHSM ao cluster do AWS CloudHSM. Para obter essas permissões, AWS KMS crie a função AWSServiceRoleForKeyManagementServiceCustomKeyStoresvinculada ao serviço em seu. Conta da AWS Os usuários que criam armazenamentos de chaves do AWS CloudHSM devem ter a permissão `iam:CreateServiceLinkedRole` que permite criar perfis vinculados ao serviço.

Tópicos

- Sobre a função vinculada ao serviço do AWS KMS
- Criar a função vinculada ao serviço
- Editar a descrição de uma função vinculada ao serviço
- Excluir a função vinculada ao serviço

Sobre a função vinculada ao serviço do AWS KMS

Uma função vinculada ao serviço é uma função do IAM que oferece permissão a um serviço da AWS para chamar outros serviços da AWS em seu nome. Ela foi projetada para facilitar o uso dos recursos de vários serviços integrados da AWS sem a necessidade de criar e manter políticas

complexas do IAM. Para ter mais informações, consulte Usar perfis vinculados ao serviço do AWS KMS.

Para armazenamentos de AWS CloudHSM chaves, AWS KMS cria a função AWSServiceRoleForKeyManagementServiceCustomKeyStoresvinculada ao serviço com a AWSKeyManagementServiceCustomKeyStoresServiceRolePolicypolítica. Essa política concede as seguintes permissões à função:

- cloudHSM:describe* — detecta alterações no AWS CloudHSM cluster que está anexado ao seu armazenamento de chaves personalizadas.
- ec2: CreateSecurityGroup — usado quando você conecta um armazenamento de AWS CloudHSM chaves para criar o grupo de segurança que permite o fluxo de tráfego de rede entre AWS KMS e seu AWS CloudHSM cluster.
- ec2: AuthorizeSecurityGroupIngress — usado quando você conecta um armazenamento de AWS CloudHSM chaves para permitir o acesso à rede AWS KMS a partir da VPC que contém AWS CloudHSM seu cluster.
- ec2: CreateNetworkInterface — usado quando você conecta um armazenamento de AWS CloudHSM chaves para criar a interface de rede usada para comunicação entre AWS KMS e o AWS CloudHSM cluster.
- ec2: RevokeSecurityGroupEgress — usado quando você conecta um armazenamento de AWS CloudHSM chaves para remover todas as regras de saída do grupo de segurança criado. AWS KMS
- ec2: DeleteSecurityGroup — usado quando você desconecta um armazenamento de AWS CloudHSM chaves para excluir grupos de segurança que foram criados quando você conectou o armazenamento de AWS CloudHSM chaves.
- ec2: DescribeSecurityGroups — usado para monitorar alterações no grupo de segurança AWS KMS criado na VPC que contém AWS CloudHSM seu cluster para AWS KMS que possa fornecer mensagens de erro claras em caso de falhas.
- ec2: DescribeVpcs — usado para monitorar alterações na VPC que contém AWS CloudHSM seu cluster para AWS KMS que possa fornecer mensagens de erro claras em caso de falhas.
- ec2: DescribeNetworkAcls — usado para monitorar alterações nas ACLs de rede da VPC que contém seu AWS CloudHSM cluster para que AWS KMS possa fornecer mensagens de erro claras em caso de falhas.

- ec2: DescribeNetworkInterfaces — usado para monitorar alterações nas interfaces de rede AWS KMS criadas na VPC que contém AWS CloudHSM seu cluster para AWS KMS que possa fornecer mensagens de erro claras em caso de falhas.

```
{
  "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": "*"
    }
  ]
}
```

Como a função AWSServiceRoleForKeyManagementServiceCustomKeyStoresvinculada ao serviço é confiável somentecks.kms.amazonaws.com, somente AWS KMS pode assumir essa função vinculada ao serviço. Essa função está limitada às operações de que o AWS KMS precisa para visualizar seus clusters do AWS CloudHSM e conectar um armazenamento de chaves do AWS CloudHSM ao cluster do AWS CloudHSM associado. Ele não concede permissões adicionais ao AWS KMS. Por exemplo, o AWS KMS não tem permissão para criar, gerenciar ou excluir clusters, HSMs ou backups do AWS CloudHSM.

Regiões

Assim como o recurso de lojas AWS CloudHSM principais, a AWSServiceRoleForKeyManagementServiceCustomKeyStoresfunção é suportada em todos os Regiões da AWS lugares AWS KMS e AWS CloudHSM está disponível. Para obter uma lista das Regiões da AWS com suporte por cada serviço, consulte Endpoints e cotas do AWS Key

Management Service e Endpoints e cotas do AWS CloudHSM em Referência geral da Amazon Web Services.

Para obter mais informações sobre como os serviços da AWS usam perfis vinculados a serviços, consulte Uso de perfis vinculados a serviço, no Guia do usuário do IAM.

Criar a função vinculada ao serviço

AWS KMScria automaticamente a função AWSServiceRoleForKeyManagementServiceCustomKeyStoresvinculada ao serviço em sua Conta da AWS quando você cria um armazenamento de AWS CloudHSM chaves, se a função ainda não existir. Não é possível criar ou criar outra vez essa função vinculada a serviço diretamente.

Editar a descrição de uma função vinculada ao serviço

Você não pode editar o nome da função ou as declarações da política na função vinculada ao serviço AWSServiceRoleForKeyManagementServiceCustomKeyStores, mas você pode editar a descrição da função. Para obter mais informações, consulte Editar um perfil vinculado ao serviço, no Guia do usuário do IAM.

Excluir a função vinculada ao serviço

AWS KMSnão exclui a função AWSServiceRoleForKeyManagementServiceCustomKeyStoresvinculada ao serviço de sua, Conta da AWS mesmo que você tenha excluído todos os seus armazenamentos de AWS CloudHSM chaves. Embora atualmente não haja nenhum procedimento para excluir a função AWSServiceRoleForKeyManagementServiceCustomKeyStoresvinculada ao serviço, não assume essa função AWS KMS nem usa suas permissões, a menos que você tenha armazenamentos de chaves ativosAWS CloudHSM.

Gerenciar um armazenamento de chaves personalizado do CloudHSM

Usando o AWS Management Console e a API do AWS KMS, é possível gerenciar um armazenamento de chaves personalizado. Por exemplo, você pode visualizar um armazenamento de chaves personalizado, editar suas propriedades, conectar-se e desconectar-se do cluster do AWS CloudHSM associado e excluir o armazenamento de chaves personalizado.

Tópicos

- Criar um armazenamento de chaves do AWS CloudHSM

- Visualizar um armazenamento de chaves do AWS CloudHSM
- Editar as configurações do armazenamento de chaves do AWS CloudHSM
- Conectar e desconectar um armazenamento de chaves do AWS CloudHSM
- Excluir um armazenamento de chaves do AWS CloudHSM

Criar um armazenamento de chaves do AWS CloudHSM

Você pode criar um ou vários armazenamentos de chaves do AWS CloudHSM em sua conta. Cada armazenamento de chaves do AWS CloudHSM está associado a um cluster do AWS CloudHSM na mesma Conta da AWS e região. Antes de criar o armazenamento de chaves do AWS CloudHSM, você precisa organizar os pré-requisitos. Antes de usar o armazenamento de chaves do AWS CloudHSM, você deve conectá-lo ao cluster do AWS CloudHSM.

> **Note**
>
> Se você tentar criar um armazenamento de chaves do AWS CloudHSM com os mesmos valores de propriedade de um armazenamento de chaves do AWS CloudHSM existente desconectado, o AWS KMS não criará um novo armazenamento de chaves do AWS CloudHSM e não gerará uma exceção nem exibirá um erro. Em vez disso, o AWS KMS reconhecerá a duplicata como a possível consequência de uma nova tentativa e retornará o ID do armazenamento de chaves do AWS CloudHSM existente.

> **Tip**
>
> Não é necessário conectar seu armazenamento de chaves do AWS CloudHSM imediatamente. Você pode deixá-lo em um estado desconectado até estar pronto para usá-lo. No entanto, para verificar se ele está configurado corretamente, convém conectá-lo, visualizar o estado da conexão e desconectá-lo.

Tópicos

- Organizar os pré-requisitos
- Criar um armazenamento de chaves do AWS CloudHSM (console)
- Criar um armazenamento de chaves do AWS CloudHSM (API)

Organizar os pré-requisitos

Cada armazenamento de chaves do AWS CloudHSM é baseado em um cluster do AWS CloudHSM. Para criar um armazenamento de chaves do AWS CloudHSM, você deve especificar um cluster do AWS CloudHSM ativo que ainda não está associado a outro armazenamento de chaves. Você também precisa criar um usuário de criptografia (CU) dedicado nos HSMs do cluster que o AWS KMS pode usar para criar e gerenciar chaves em seu nome.

Antes de criar um armazenamento de chaves do AWS CloudHSM, faça o seguinte:

Selecionar um cluster do AWS CloudHSM

Todo armazenamento de chaves do AWS CloudHSM é associado, precisamente, a um cluster do AWS CloudHSM. Quando você cria uma AWS KMS keys no armazenamento de chaves do AWS CloudHSM, o AWS KMS cria os metadados da chave do KMS, como um ID e um nome do recurso da Amazon (ARN) no AWS KMS. Ele cria o material de chaves nos HSMs do cluster associado. Você pode criar um novo cluster do AWS CloudHSM ou usar um existente. O AWS KMS não requer acesso exclusivo ao cluster.

O cluster do AWS CloudHSM que você seleciona fica permanentemente associado ao armazenamento de chaves do AWS CloudHSM. Depois de criar o armazenamento de chaves do AWS CloudHSM, você pode alterar o ID do cluster associado, mas o cluster que você especificar deverá compartilhar um histórico de backup com o cluster original. Para usar um cluster não relacionado, você precisa criar um novo armazenamento de chaves do AWS CloudHSM.

O cluster do AWS CloudHSM que você selecionar deve ter as seguintes características:

- O cluster deve estar ativo.

  Você deve criar o cluster, iniciá-lo, instalar o software cliente do AWS CloudHSM para a sua plataforma e ativar o cluster. Para obter instruções detalhadas, consulte Conceitos básicos do AWS CloudHSM no Guia do usuário do AWS CloudHSM.
- O cluster deve estar na mesma conta e região que o armazenamento de chaves do AWS CloudHSM. Você não pode associar um armazenamento de chaves do AWS CloudHSM em uma região a um cluster em uma região diferente. Para criar uma infraestrutura de chaves em várias regiões, você deverá criar armazenamentos de chaves do AWS CloudHSM e clusters em cada região.
- Não é possível associar o cluster a outro armazenamento personalizado de chaves na mesma conta e região. É necessário associar cada armazenamento de chaves do AWS

CloudHSM na conta e região a um cluster diferente do AWS CloudHSM. Você não pode especificar um cluster que já esteja associado a um armazenamento de chaves personalizado, tampouco um cluster que compartilhe um histórico de backup com um cluster associado. Os clusters que compartilham um histórico de backup têm o mesmo certificado do cluster. Para visualizar o certificado de cluster de um cluster, use o AWS CloudHSM console ou a DescribeClustersoperação.

Se você fizer backup de um cluster do AWS CloudHSM em uma região diferente, ele será considerado um cluster diferente e você poderá associar o backup a um armazenamento personalizado de chaves na região dele. No entanto, mesmo que tenham a mesma chave de reserva, as chaves do KMS nos dois armazenamentos personalizados de chaves não são interoperáveis. O AWS KMS vincula metadados ao texto cifrado, de modo que só é possível descriptografá-los com a chave do KMS que os criptografaram.

- O cluster deve ser configurado com sub-redes privadas em pelo menos duas zonas de disponibilidade na região. Como o AWS CloudHSM não é compatível com todas as zonas de disponibilidade, recomendamos que você crie sub-redes privadas em todas as zonas de disponibilidade na região. Você não pode reconfigurar as sub-redes para um cluster existente, mas pode criar um cluster a partir de um backup com diferentes sub-redes na configuração do cluster.

  > **Important**
  >
  > Depois de criar seu armazenamento de chaves do AWS CloudHSM, não exclua nenhuma das sub-redes privadas configuradas para seu cluster do AWS CloudHSM. Se o AWS KMS não conseguiu localizar todas as sub-redes na configuração do cluster, as tentativas de se conectar ao armazenamento de chaves personalizadas falharão com um estado de erro de conexão `SUBNET_NOT_FOUND`. Para obter detalhes, consulte Como corrigir uma falha de conexão.

- O grupo de segurança para o cluster (`cloudhsm-cluster-<cluster-id>-sg`) deve incluir regras de entrada e de saída que permitam tráfego TCP nas portas 2223-2225. O Source (Origem) nas regras de entrada e o Destination (Destino) nas regras de saída deve corresponder ao ID do grupo de segurança. Essas regras são definidas por padrão quando você cria o cluster. Não as exclua nem as altere.
- O cluster deve conter pelo menos dois HSMs ativos em diferentes zonas de disponibilidade. Para verificar o número de HSMs, use o AWS CloudHSM console ou a DescribeClustersoperação. Se necessário, você pode adicionar um HSM.

Localizar o certificado da âncora de confiança

Quando você cria um armazenamento de chaves personalizado, é necessário carregar o certificado da âncora de confiança para o cluster do AWS CloudHSM para o AWS KMS. O AWS KMS precisa do certificado da âncora de confiança para conectar o armazenamento de chaves do AWS CloudHSM ao cluster do AWS CloudHSM.

Cada cluster do AWS CloudHSM ativo tem um certificado da âncora de confiança. Ao inicializar o cluster, você gera esse certificado, salve-o no `customerCA.crt` arquivo e copie-o em hosts que se conectam ao cluster.

Criar o usuário de criptografia **`kmsuser`** para o AWS KMS

Para administrar o armazenamento de chaves do AWS CloudHSM, o AWS KMS faz login na conta do usuário de criptografia `kmsuser` no cluster selecionado. Antes de criar o armazenamento de chaves do AWS CloudHSM, você deve criar o usuário de criptografia do `kmsuser`. Ao criar o armazenamento de chaves do AWS CloudHSM, você fornece a senha do `kmsuser` para o AWS KMS. Quando você conecta o armazenamento de chaves do AWS CloudHSM ao cluster do AWS CloudHSM associado, o AWS KMS faz login no cluster como `kmsuser` e alterna a senha do `kmsuser`

> **Important**
>
> Não especifique a opção `2FA` ao criar o CU do `kmsuser`. Se você fizer isso, o AWS KMS não poderá fazer login, e o armazenamento de chaves do AWS CloudHSM não poderá ser conectado a esse cluster do AWS CloudHSM. Ao especificar o código de autenticação de dois fatores, você não pode desfazê-lo. Em vez disso, você deve excluir o CU e recriá-lo.

Para criar o CU do `kmsuser`, use o procedimento a seguir.

1. Inicie cloudhsm_mgmt_util conforme descrito no tópico Getting started with CloudHSM Management Utility (CMU) (Conceitos básicos do CloudHSM Management Utility [CMU]) do Guia do usuário do AWS CloudHSM.
2. Use o comando createUser em cloudhsm_mgmt_util para criar um CU chamado `kmsuser`. A senha deve conter de 7 a 32 caracteres alfanuméricos. Ela diferencia maiúsculas de minúsculas e não pode conter caracteres especiais.

   Por exemplo, o seguinte comando cria um CU do `kmsuser` com uma senha de `kmsPswd`.

```
aws-cloudhsm> createUser CU kmsuser kmsPswd
```

Criar um armazenamento de chaves do AWS CloudHSM (console)

Ao criar um armazenamento de chaves do AWS CloudHSM no AWS Management Console, você pode adicionar e criar os pré-requisitos como parte de seu fluxo de trabalho. No entanto, o processo é mais rápido quando eles são organizados com antecedência.

1. Faça login no AWS Management Console e abra o console do AWS Key Management Service (AWS KMS) em https://console.aws.amazon.com/kms.
2. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.
3. No painel de navegação, selecione Custom key stores (Repositórios de chaves personalizados), AWS CloudHSM key stores (Repositórios de chaves do).
4. Selecione Create key store (Criar armazenamento de chaves).
5. Digite um nome amigável para o armazenamento de chaves personalizado. O nome deve ser exclusivo entre todos os outros armazenamentos de chaves personalizados de sua conta.

   > **Important**
   >
   > Não inclua informações confidenciais ou sigilosas nesse campo. Esse campo pode ser exibido em texto simples em CloudTrail registros e outras saídas.

6. Selecione um cluster do AWS CloudHSM para o armazenamento de chaves do AWS CloudHSM. Ou, para criar um novo cluster do AWS CloudHSM, escolha o link Create an AWS CloudHSM cluster (Criar um cluster do).

   O menu exibe clusters do AWS CloudHSM em sua conta e região que ainda não estão associados a um armazenamento de chaves do AWS CloudHSM. O cluster deve cumprir os requisitos para associação com um armazenamento de chaves personalizado.
7. Escolha Choose file (Escolher arquivo) e carregue o certificado da âncora de confiança para o cluster do AWS CloudHSM que você escolheu. Esse é o arquivo `customerCA.crt` que você criou ao inicializar o cluster.
8. Insira a senha do usuário de criptografia `kmsuser` (CU) que você criou no cluster selecionado.
9. Escolha Criar.

Se o procedimento for bem-sucedido, o novo armazenamento de chaves do AWS CloudHSM será exibido na lista de armazenamentos de chaves do AWS CloudHSM na conta e região. Se ele for malsucedido, será exibida uma mensagem de erro descrevendo o problema e fornecendo ajuda para corrigi-lo. Se precisar de ajuda adicional, consulte Solucionar problemas de um armazenamento de chaves personalizado.

Se você tentar criar um armazenamento de chaves do AWS CloudHSM com os mesmos valores de propriedade de um armazenamento de chaves do AWS CloudHSM existente desconectado, o AWS KMS não criará um novo armazenamento de chaves do AWS CloudHSM e não gerará uma exceção nem exibirá um erro. Em vez disso, o AWS KMS reconhecerá a duplicata como a possível consequência de uma nova tentativa e retornará o ID do armazenamento de chaves do AWS CloudHSM existente.

Próximo: os novos armazenamentos de chaves do AWS CloudHSM não são conectados automaticamente. Antes de criar AWS KMS keys no armazenamento de chaves do AWS CloudHSM, conecte o armazenamento de chaves personalizado ao cluster do AWS CloudHSM associado.

Criar um armazenamento de chaves do AWS CloudHSM (API)

Você pode usar a CreateCustomKeyStoreoperação para criar um novo armazenamento de AWS CloudHSM chaves associado a um AWS CloudHSM cluster na conta e na região. Estes exemplos usam a AWS Command Line Interface (AWS CLI), mas você pode usar qualquer linguagem de programação compatível.

A operação `CreateCustomKeyStore` exige os seguintes valores de parâmetros.

- CustomKeyStoreName — Um nome amigável para o armazenamento de chaves personalizadas que é exclusivo na conta.

  > **Important**
  >
  > Não inclua informações confidenciais ou sigilosas nesse campo. Esse campo pode ser exibido em texto simples em CloudTrail registros e outras saídas.

- CloudHsmClusterId — O ID do cluster de um AWS CloudHSM cluster que atende aos requisitos de um armazenamento de AWS CloudHSM chaves.
- KeyStorePassword — A senha da conta `kmsuser` UC no cluster especificado.
- TrustAnchorCertificate — O conteúdo do `customerCA.crt` arquivo que você criou quando inicializou o cluster.

O exemplo a seguir usa um ID de cluster fictício. Antes de executar o comando, substitua-o por um ID de cluster válido.

```
$ 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 estiver usando a AWS CLI, você pode especificar o arquivo do certificado da âncora de confiança, em vez de seu conteúdo. No exemplo a seguir, o arquivo `customerCA.crt` no diretório raiz.

```
$ 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
```

Quando a operação é bem-sucedida, `CreateCustomKeyStore` retorna o ID do armazenamento de chaves personalizado, conforme exibido na resposta de exemplo a seguir.

```
{
    "CustomKeyStoreId": cks-1234567890abcdef0
}
```

Se a operação falhar, corrija o erro indicado pela exceção e tente novamente. Para obter ajuda adicional, consulte Solucionar problemas de um armazenamento de chaves personalizado.

Se você tentar criar um armazenamento de chaves do AWS CloudHSM com os mesmos valores de propriedade de um armazenamento de chaves do AWS CloudHSM existente desconectado, o AWS KMS não criará um novo armazenamento de chaves do AWS CloudHSM e não gerará uma exceção nem exibirá um erro. Em vez disso, o AWS KMS reconhecerá a duplicata como a possível consequência de uma nova tentativa e retornará o ID do armazenamento de chaves do AWS CloudHSM existente.

Próximo: para usar o armazenamento de chaves do AWS CloudHSM, conecte-o ao cluster do AWS CloudHSM.

Visualizar um armazenamento de chaves do AWS CloudHSM

Você pode ver os AWS CloudHSM principais armazenamentos em cada conta e região usando o AWS KMS console ou a DescribeCustomKeyStoresoperação.

Consulte também:

- Visualizar um armazenamento de chaves externas
- Visualizar chaves do KMS em um armazenamento de chaves do AWS CloudHSM
- Registrando chamadas de AWS KMS API com AWS CloudTrail

Tópicos

- Visualizar um armazenamento de chaves do AWS CloudHSM (console)
- Visualizar um armazenamento de chaves do AWS CloudHSM (API)

Visualizar um armazenamento de chaves do AWS CloudHSM (console)

Ao visualizar armazenamentos de chaves do AWS CloudHSM no AWS Management Console, você poderá ver as seguintes informações:

- O nome e ID do armazenamento de chaves personalizado
- O ID do cluster do AWS CloudHSM associado
- O número de HSMs no cluster
- O estado da conexão atual

Um estado de conexão (Status) com o valor Disconnected (Desconectado) indica que o armazenamento de chaves personalizado é novo e nunca foi conectado ou foi intencionalmente desconectado do cluster do AWS CloudHSM. No entanto, se as suas tentativas de usar uma chave do KMS em um armazenamento de chaves personalizado conectado falharem, pode ser indício de um problema com o armazenamento de chaves personalizado ou com o cluster do AWS CloudHSM. Para obter ajuda, consulte Como corrigir uma chave do KMS com falha.

Para visualizar armazenamentos de chaves do AWS CloudHSM em uma determinada conta e região, use o procedimento a seguir.

1. Faça login no AWS Management Console e abra o console do AWS Key Management Service (AWS KMS) em https://console.aws.amazon.com/kms.

2. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.
3. No painel de navegação, selecione Custom key stores (Repositórios de chaves personalizados), AWS CloudHSM key stores (Repositórios de chaves do).

Para personalizar a exibição, clique no ícone de engrenagem que aparece abaixo do botão Create key store (Criar armazenamento de chaves).

Visualizar um armazenamento de chaves do AWS CloudHSM (API)

Para visualizar suas lojas de AWS CloudHSM chaves, use a DescribeCustomKeyStoresoperação. Por padrão, essa operação retorna todos os armazenamentos de chaves personalizados na conta e região. No entanto, você pode usar o parâmetro `CustomKeyStoreId` ou `CustomKeyStoreName` (mas não ambos) para limitar o resultado para um determinado armazenamento de chaves personalizado. Para armazenamentos de chaves do AWS CloudHSM, a saída consiste no ID e nome do armazenamento de chaves personalizado, no tipo de armazenamento de chaves personalizado, no ID do cluster do AWS CloudHSM associado e no estado da conexão. Se o estado da conexão indica um erro, o resultado também inclui um código de erro que descreve o motivo do erro.

Os exemplos nesta seção usam a AWS Command Line Interface (AWS CLI), mas você pode usar qualquer linguagem de programação compatível.

Por exemplo, o comando a seguir retorna todos os armazenamentos de chaves personalizados na conta e região. Você pode usar os parâmetros `Marker` e `Limit` para percorrer os armazenamentos de chaves personalizados do resultado.

```
$ aws kms describe-custom-key-stores
```

O comando de exemplo a seguir usa o parâmetro `CustomKeyStoreName` para obter apenas o armazenamento de chaves personalizado com o nome amigável `ExampleCloudHSMKeyStore`. É possível usar o parâmetro `CustomKeyStoreName` ou `CustomKeyStoreId` (mas não ambos) em cada comando.

O exemplo de resultado a seguir representa um armazenamento de chaves do AWS CloudHSM que está conectado ao cluster do AWS CloudHSM.

> **Note**
>
> O campo `CustomKeyStoreType` foi adicionado à resposta `DescribeCustomKeyStores` para distinguir os armazenamentos de chaves do AWS CloudHSM dos armazenamentos de chaves externas.

```
$ 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>"
      }
   ]
}
```

Um `ConnectionState` `Disconnected` indica que um armazenamento de chaves personalizado nunca foi conectado, ou foi intencionalmente desconectado do cluster do AWS CloudHSM. No entanto, se as tentativas de usar uma chave do KMS em um armazenamento de chaves do AWS CloudHSM conectado falharem, pode ser indício de um problema com o armazenamento de chaves do AWS CloudHSM ou com o cluster do AWS CloudHSM. Para obter ajuda, consulte Como corrigir uma chave do KMS com falha.

Quando o `ConnectionState` do armazenamento de chaves personalizado `FAILED`, a resposta `DescribeCustomKeyStores` inclui um elemento `ConnectionErrorCode` que explica o motivo desse erro.

Por exemplo, no resultado a seguir, o valor `INVALID_CREDENTIALS` indica que a conexão do armazenamento de chaves personalizado falhou porque a senha `kmsuser` é inválido. Para obter ajuda com relação a esta e outras falhas de erro de conexão, consulte Solucionar problemas de um armazenamento de chaves personalizado.

```
$ 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>"
      }
   ]
}
```

Editar as configurações do armazenamento de chaves do AWS CloudHSM

Você pode alterar as configurações de um armazenamento de chaves do AWS CloudHSM existente. O armazenamento de chaves personalizado deve estar desconectado do cluster do AWS CloudHSM.

Para editar as configurações de armazenamento de chaves do AWS CloudHSM:

1. Desconectar o armazenamento de chaves personalizado do cluster do AWS CloudHSM. Enquanto o armazenamento de chaves personalizado estiver desconectado, não é possível criar AWS KMS keys (chaves do KMS) nele nem usar as chaves do KMS que ele contém para operações de criptografia.
2. Editar uma ou mais das configurações do armazenamento de chaves do AWS CloudHSM.
3. Reconectar o armazenamento de chaves personalizado ao cluster do AWS CloudHSM.

Você pode editar as seguintes configurações em um armazenamento de chaves personalizado:

O nome amigável do armazenamento de chaves personalizado.

Inserir um novo nome amigável. O novo nome deve ser exclusivo entre todos os outros armazenamentos de chaves personalizados de sua Conta da AWS.

> **Important**
>
> Não inclua informações confidenciais ou sigilosas nesse campo. Esse campo pode ser exibido em texto simples em CloudTrail registros e outras saídas.

O ID de cluster do cluster do AWS CloudHSM associado.

Editar esse valor para substituir um cluster de AWS CloudHSM relacionado para o original. Você poderá usar esse recurso para reparar um armazenamento de chaves personalizado caso o seu cluster do AWS CloudHSM seja corrompido ou excluído.

Especifique um cluster do AWS CloudHSM que compartilha um histórico de backup com o cluster original e cumpre os requisitos de associação com um armazenamento de chaves personalizado, incluindo dois HSMs ativos em diferentes zonas de disponibilidade. Os clusters que compartilham um histórico de backup têm o mesmo certificado do cluster. Para visualizar o certificado de cluster de um cluster, use a DescribeClustersoperação. Você não pode usar o recurso de edição para associar o armazenamento de chaves personalizado a um cluster do AWS CloudHSM não relacionado.

A senha atual do **`kmsuser`** usuário de criptografia (CU).

Informa ao AWS KMS a senha atual do CU `kmsuser` no cluster do AWS CloudHSM. Essa ação não altera a senha do CU `kmsuser` no cluster do AWS CloudHSM.

Se você alterar a senha do CU `kmsuser` no cluster do AWS CloudHSM, use esse recurso para informar ao AWS KMS a nova senha `kmsuser`. Caso contrário, o AWS KMS não poderá fazer login no cluster, e todas as tentativas de conectar o armazenamento de chaves personalizado ao cluster falham.

Tópicos

- Editar um armazenamento de chaves do AWS CloudHSM (console)
- Editar um armazenamento de chaves do AWS CloudHSM (API)

Editar um armazenamento de chaves do AWS CloudHSM (console)

Ao editar o armazenamento de chaves do AWS CloudHSM, você pode alterar qualquer um ou todos os valores configuráveis.

1. Faça login no AWS Management Console e abra o console do AWS Key Management Service (AWS KMS) em https://console.aws.amazon.com/kms.
2. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.
3. No painel de navegação, selecione Custom key stores (Repositórios de chaves personalizados), AWS CloudHSM key stores (Repositórios de chaves do).

4. Escolha a linha do armazenamento de chaves do AWS CloudHSM que deseja editar.

   Se o valor na coluna Connection state (Estado da conexão) não for Disconnected (Desconectado), você deverá desconectar o armazenamento de chaves personalizado para editá-lo. (No menu Key store actions (Ações do armazenamento de chaves), escolha Disconnect [Desconectar].)

   Enquanto um armazenamento de chaves do AWS CloudHSM está desconectado, é possível gerenciar o armazenamento de chaves do AWS CloudHSM e suas chaves do KMS, mas não é possível criar nem usar chaves do KMS no armazenamento de chaves do AWS CloudHSM.
5. No menu Key store actions (Ações do armazenamento de chaves), escolha Edit (Editar).
6. Faça uma ou mais das ações a seguir.

   - Digite um novo nome amigável para o armazenamento de chaves personalizado.
   - Digite o ID de cluster de um cluster do AWS CloudHSM associado.
   - Digite a senha atual do usuário de criptografia `kmsuser` no cluster do AWS CloudHSM associado.
7. Escolha Save (Salvar).

   Se o procedimento for bem-sucedido, uma mensagem descreverá as configurações que você editou. Se for malsucedido, será exibida uma mensagem de erro descrevendo o problema e fornecendo ajuda para corrigi-lo. Se precisar de ajuda adicional, consulte Solucionar problemas de um armazenamento de chaves personalizado.
8. Reconecte o armazenamento de chaves personalizado.

   Para usar o armazenamento de chaves do AWS CloudHSM, você deve reconectá-lo após a edição. Você pode deixar o armazenamento de chaves do AWS CloudHSM desconectado. Porém, enquanto estiver desconectado, não é possível criar as chaves do KMS no armazenamento de chaves do AWS CloudHSM nem usá-las no armazenamento de chaves do AWS CloudHSM em operações de criptografia.

Editar um armazenamento de chaves do AWS CloudHSM (API)

Para alterar as propriedades de um armazenamento de AWS CloudHSM chaves, use a UpdateCustomKeyStoreoperação. Você pode alterar várias propriedades de um armazenamento de chaves personalizado no mesmo comando. Se a operação tiver êxito, o AWS KMS retornará

uma resposta HTTP 200 e um objeto JSON sem propriedades. Para verificar se as alterações são efetivas, use a DescribeCustomKeyStoresoperação.

Os exemplos nesta seção usam a AWS Command Line Interface (AWS CLI), mas você pode usar qualquer linguagem de programação compatível.

Comece usando DisconnectCustomKeyStorepara desconectar o armazenamento de chaves personalizadas de seu AWS CloudHSM cluster. Substitua o exemplo de ID de armazenamento de chaves personalizado, cks-1234567890abcdef0, por um ID real.

```
$ aws kms disconnect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

O primeiro exemplo usa UpdateCustomKeyStorepara alterar o nome amigável do armazenamento de AWS CloudHSM chaves para`DevelopmentKeys`. O comando usa o parâmetro `CustomKeyStoreId` para identificar o armazenamento de chaves do AWS CloudHSM e `CustomKeyStoreName` para especificar o novo nome para o armazenamento de chaves personalizado.

```
$ aws kms update-custom-key-store --custom-key-store-id cks-1234567890abcdef0 --new-
custom-key-store-name DevelopmentKeys
```

O exemplo a seguir altera o cluster associado a um armazenamento de chaves do AWS CloudHSM por outro backup do mesmo cluster. O comando usa o parâmetro `CustomKeyStoreId` para identificar o armazenamento de chaves do AWS CloudHSM e o parâmetro `CloudHsmClusterId` para especificar o novo ID do cluster.

```
$ aws kms update-custom-key-store --custom-key-store-id cks-1234567890abcdef0 --cloud-
hsm-cluster-id cluster-1a23b4cdefg
```

O exemplo a seguir mostra ao AWS KMS que a senha `kmsuser` atual é `ExamplePassword`. O comando usa o parâmetro `CustomKeyStoreId` para identificar o armazenamento de chaves do AWS CloudHSM e o parâmetro `KeyStorePassword` para especificar a senha atual.

```
$ aws kms update-custom-key-store --custom-key-store-id cks-1234567890abcdef0 --key-
store-password ExamplePassword
```

O comando final reconecta o armazenamento de chaves do AWS CloudHSM ao cluster do AWS CloudHSM. É possível deixar o armazenamento de chaves personalizado no estado desconectado,

mas ele precisa estar conectado para que seja possível criar chaves do KMS ou usar as chaves do KMS existentes para operações de criptografia. Substitua o ID de exemplo do armazenamento de chaves personalizado por um ID real.

```
$ aws kms connect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

Conectar e desconectar um armazenamento de chaves do AWS CloudHSM

Os novos armazenamentos de chaves do AWS CloudHSM não são conectados. Antes de criar e usar AWS KMS keys no armazenamento de chaves do AWS CloudHSM, você precisa conectá-lo ao cluster do AWS CloudHSM associado. Você pode conectar e desconectar seu armazenamento de chaves do AWS CloudHSM a qualquer momento e visualizar o estado da conexão.

Não é necessário conectar seu armazenamento de chaves do AWS CloudHSM. Você pode deixar um armazenamento de chaves do AWS CloudHSM em estado desconectado indefinidamente e conectá-lo somente quando precisar usá-lo. No entanto, você pode desejar testar a conexão periodicamente para verificar se as configurações estão corretas e se ele pode ser conectado.

> **Note**
>
> Os armazenamentos de chaves do AWS CloudHSM têm um estado de conexão `DISCONNECTED` somente quando nunca foram conectados ou quando você os desconecta explicitamente. Se o estado da conexão do armazenamento de chaves do AWS CloudHSM for `CONNECTED`, mas você estiver com problemas para usá-lo, certifique-se de que seu cluster do AWS CloudHSM esteja ativo e contenha pelo menos um HSM ativo. Para obter ajuda com falhas de conexão, consulte the section called “Solucionar problemas de um armazenamento de chaves personalizado”.

Tópicos

- Conectar um armazenamento de chaves do AWS CloudHSM
- Desconectar um armazenamento de chaves do AWS CloudHSM
- Conectar um armazenamento de chaves do AWS CloudHSM (console)
- Conectar um armazenamento de chaves personalizado (API)
- Desconectar um armazenamento de chaves do AWS CloudHSM (console)
- Desconectar um armazenamento de chaves do AWS CloudHSM (API)

Conectar um armazenamento de chaves do AWS CloudHSM

Quando você conecta um armazenamento de chaves do AWS CloudHSM, o AWS KMS localiza o cluster do AWS CloudHSM associado, estabelece conexão com ele, faz login no cliente do AWS CloudHSM como o usuário de criptografia do `kmsuser` e alterna a senha de `kmsuser`. O AWS KMS permanecerá conectado ao cliente do AWS CloudHSM enquanto o armazenamento de chaves do AWS CloudHSM estiver conectado.

Para estabelecer a conexão, o AWS KMS cria grupos de segurança chamados `kms-<custom key store ID>` na virtual private cloud (VPC) do cluster. O grupo de segurança tem uma única regra que permite o tráfego de entrada dos grupos de segurança do cluster. O AWS KMS também cria uma interface de rede elástica (ENI) em cada zona de disponibilidade da sub-rede privada para o cluster. O AWS KMS adiciona as ENIs ao grupo de segurança `kms-<cluster ID>` e os grupos de segurança para o cluster. A descrição de cada ENI é `KMS managed ENI for cluster <cluster-ID>`.

O processo de conexão pode demorar um período prolongado para ser concluído; até 20 minutos.

Antes de conectar o armazenamento de chaves do AWS CloudHSM, verifique se ele atende aos requisitos.

- Seu cluster do AWS CloudHSM associado deve conter pelo menos um HSM ativo. Para encontrar o número de HSMs no cluster, visualize o cluster no AWS CloudHSM console ou use a DescribeClustersoperação. Se necessário, você pode adicionar um HSM.
- O cluster deve ter uma conta de usuário de criptografia `kmsuser`, mas esse usuário não pode estar registrado no cluster quando você conecta o armazenamento de chaves do AWS CloudHSM. Para obter ajuda com o logout, consulte Como fazer logout e se conectar novamente.
- O estado da conexão do armazenamento de chaves do AWS CloudHSM não pode ser `DISCONNECTING` ou `FAILED`. Para ver o estado da conexão, use o AWS KMS console ou a DescribeCustomKeyStoresresposta. Se o estado da conexão for `FAILED`, desconecte o armazenamento de chaves personalizado, corrija o problema e conecte-o.

Para obter ajuda com falhas de conexão, consulte Como corrigir uma falha de conexão.

Quando seu armazenamento de chaves do AWS CloudHSM está conectado, é possível criar chaves do KMS nele e usar chaves do KMS existentes em operações de criptografia.

Desconectar um armazenamento de chaves do AWS CloudHSM

Quando você desconecta um armazenamento de chaves do AWS CloudHSM, o AWS KMS faz logout do cliente do AWS CloudHSM, desconecta-se do cluster do AWS CloudHSM associado e remove a infraestrutura de rede que ele criou para oferecer suporte à conexão.

Enquanto um armazenamento de chaves do AWS CloudHSM está desconectado, é possível gerenciar o armazenamento de chaves do AWS CloudHSM e suas chaves do KMS, mas não é possível criar nem usar chaves do KMS no armazenamento de chaves do AWS CloudHSM. O estado da conexão do armazenamento de chaves é `DISCONNECTED`, e o estado da chave das chaves do KMS no armazenamento de chaves personalizado é `Unavailable`, a menos que elas estejam com `PendingDeletion`. Você pode reconectar o armazenamento de chaves do AWS CloudHSM a qualquer momento.

Quando você desconecta um armazenamento de chaves personalizado, as chaves do KMS do armazenamento de chaves tornam-se inutilizáveis imediatamente (sujeitas a consistência posterior). Porém, os recursos criptografados com chaves de dados protegidas pela chave do KMS não serão afetados até que a chave do KMS seja usada novamente, por exemplo, para descriptografar a chave de dados. Esse problema afeta os Serviços da AWS, pois muitos deles usam chaves de dados para proteger recursos. Para obter detalhes, consulte Como as chaves do KMS inutilizáveis afetam as chaves de dados.

> **Note**
>
> Enquanto um armazenamento de chaves personalizado estiver desconectado, todas as tentativas de criar chaves do KMS nele ou de usar chaves do KMS existentes em operações de criptografia falharão. Essa ação pode impedir que os usuários armazenem e acessem dados sigilosos.

Para avaliar melhor o efeito de desconectar o armazenamento de chaves personalizado, identifique as chaves do KMS no armazenamento de chaves personalizado e determine seu uso anterior.

Você pode desconectar o armazenamento de chaves do AWS CloudHSM por motivos como estes:

- Para mudar a senha do **`kmsuser`**. O AWS KMS altera a senha `kmsuser` toda vez que se conecta ao cluster do AWS CloudHSM. Para forçar uma mudança de senha, basta desconectar e reconectar.

- Para auditar o material de chave das chaves do KMS no cluster do AWS CloudHSM. Quando você desconecta o armazenamento de chaves personalizado, o AWS KMS faz logout da conta do usuário de criptografia `kmsuser` no cliente AWS CloudHSM. Isso permite fazer login no cluster como o CU `kmsuser` e auditar e gerenciar o material de chave para a chave do KMS.
- Para desabilitar imediatamente todas as chaves do KMS no armazenamento de chaves do AWS CloudHSM. Você pode desativar e reativar as chaves KMS em um armazenamento de AWS CloudHSM chaves usando a operação AWS Management Console ou. DisableKey Essas operações são concluídas rapidamente, mas atuam em uma chave do KMS de cada vez. A desconexão do armazenamento de chaves do AWS CloudHSM altera imediatamente o estado de chave de todas as chaves do KMS no armazenamento de chaves do AWS CloudHSM para `Unavailable`, o que impede que elas sejam usadas em operações de criptografia.
- Para reparar uma falha na tentativa de conexão. Se ocorrer falha em uma tentativa de conectar-se a um armazenamento de chaves do AWS CloudHSM (o estado da conexão do armazenamento de chaves personalizado apresentado é `FAILED`), você deve desconectar o armazenamento de chaves do AWS CloudHSM antes de tentar se conectar novamente.

Conectar um armazenamento de chaves do AWS CloudHSM (console)

Para conectar um armazenamento de chaves do AWS CloudHSM ao AWS Management Console, comece selecionando o armazenamento de chaves do AWS CloudHSM na página Custom key stores (Armazenamentos de chaves personalizados). O processo de conexão pode levar até 20 minutos.

1. Faça login no AWS Management Console e abra o console do AWS Key Management Service (AWS KMS) em https://console.aws.amazon.com/kms.
2. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.
3. No painel de navegação, selecione Custom key stores (Repositórios de chaves personalizados), AWS CloudHSM key stores (Repositórios de chaves do).
4. Escolha a linha do armazenamento de chaves do AWS CloudHSM que deseja conectar.

   Se o status do armazenamento de chaves do AWS CloudHSM for Failed (Falha), você deve desconectar o armazenamento de chaves personalizado antes de conectá-lo.
5. No menu Key store actions (Ações do armazenamento de chaves), escolha Connect (Conectar).

O AWS KMS inicia o processo de conexão do seu armazenamento de chaves personalizado. Ele localiza o cluster do AWS CloudHSM associado, cria a infraestrutura de rede necessária, se conecta,

faz login no cluster do AWS CloudHSM como CU do `kmsuser` e muda a senha do `kmsuser`. Quando a operação é concluída, o estado de conexão é alterado para Connected (Conectado).

Se houver falha na operação, uma mensagem descrevendo o motivo da falha será exibida. Antes de tentar se conectar novamente, visualize o estado da conexão do armazenamento de chaves do AWS CloudHSM. Se for Failed (Falha), você deve desconectar o armazenamento de chaves personalizado antes de conectá-lo novamente. Se precisar de ajuda, consulte Solucionar problemas de um armazenamento de chaves personalizado.

Próximo: the section called “Criar chaves do KMS em um armazenamento de chaves do AWS CloudHSM”.

Conectar um armazenamento de chaves personalizado (API)

Para conectar um armazenamento de AWS CloudHSM chaves desconectado, use a ConnectCustomKeyStoreoperação. O cluster do AWS CloudHSM associado deve conter pelo menos um HSM ativo, e o estado da conexão não pode ser `FAILED`.

O processo de conexão demora um período prolongado para ser concluído; até 20 minutos. A menos que se antecipe à falha, a operação retornará uma resposta HTTP 200 e um objeto JSON sem propriedades. No entanto, essa resposta inicial não indica que a conexão foi bem-sucedida. Para determinar o estado da conexão do armazenamento de chaves personalizadas, veja a DescribeCustomKeyStoresresposta.

Os exemplos nesta seção usam a AWS Command Line Interface (AWS CLI), mas você pode usar qualquer linguagem de programação compatível.

Para identificar o armazenamento de chaves do AWS CloudHSM, use o ID do armazenamento de chaves personalizado. Você pode encontrar o ID na página Armazenamentos de chaves personalizadas no console ou usando a DescribeCustomKeyStoresoperação sem parâmetros. Antes de executar esse exemplo, substitua o ID de exemplo por um válido.

```
$ aws kms connect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

Para verificar se o armazenamento de AWS CloudHSM chaves está conectado, use a DescribeCustomKeyStoresoperação. Por padrão, essa operação retorna todos os armazenamentos de chaves personalizados em sua conta e região. No entanto, você pode usar o parâmetro `CustomKeyStoreId` ou `CustomKeyStoreName` (mas não ambos) para limitar a resposta para determinados armazenamentos de chaves personalizados. O valor `ConnectionState`

`CONNECTED` indica que o armazenamento de chaves personalizado está conectado ao cluster do AWS CloudHSM.

> **Note**
>
> O campo `CustomKeyStoreType` foi adicionado à resposta `DescribeCustomKeyStores` para distinguir os armazenamentos de chaves do AWS CloudHSM dos armazenamentos de chaves externas.

```
$ 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 ocorrer falha no valor `ConnectionState`, o elemento `ConnectionErrorCode` indica o motivo da falha. Nesse caso, o AWS KMS não conseguiu encontrar um cluster do AWS CloudHSM em sua conta com o ID do cluster `cluster-1a23b4cdefg`. Se você excluiu o cluster, você pode restaurá-lo a partir de um backup do cluster original e editar o ID do cluster para o armazenamento de chaves personalizado. Para obter ajuda para responder a um código de erro de conexão, consulte Como corrigir uma falha de conexão.

```
$ 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"
   ],
}
```

Próximo: Criar chaves do KMS em um armazenamento de chaves do AWS CloudHSM.

Desconectar um armazenamento de chaves do AWS CloudHSM (console)

Para desconectar um armazenamento de chaves do AWS CloudHSM no AWS Management Console, comece escolhendo o armazenamento de chaves do AWS CloudHSM na página Custom key stores (Armazenamentos de chaves personalizados).

1. Faça login no AWS Management Console e abra o console do AWS Key Management Service (AWS KMS) em https://console.aws.amazon.com/kms.
2. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.
3. No painel de navegação, selecione Custom key stores (Repositórios de chaves personalizados), AWS CloudHSM key stores (Repositórios de chaves do).
4. Escolha a linha do armazenamento de chaves externas que deseja desconectar.
5. No menu Key store actions (Ações do armazenamento de chaves), escolha Disconnect (Desconectar).

Quando a operação é concluída, o estado de conexão é alterado de Disconnecting (Desconectando) para Disconnected (Desconectado). Se ocorrer falha na operação, será exibida uma mensagem de erro descrevendo o problema e fornecendo ajuda para corrigi-lo. Se precisar de ajuda adicional, consulte Solucionar problemas de um armazenamento de chaves personalizado.

Desconectar um armazenamento de chaves do AWS CloudHSM (API)

Para desconectar um armazenamento de AWS CloudHSM chaves conectado, use a DisconnectCustomKeyStoreoperação. Se a operação tiver êxito, o AWS KMS retornará uma resposta HTTP 200 e um objeto JSON sem propriedades.

Os exemplos nesta seção usam a AWS Command Line Interface (AWS CLI), mas você pode usar qualquer linguagem de programação compatível.

Esse exemplo desconecta um armazenamento de chaves do AWS CloudHSM. Antes de executar esse exemplo, substitua o ID de exemplo por um válido.

```
$ aws kms disconnect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

Para verificar se o armazenamento de AWS CloudHSM chaves está desconectado, use a DescribeCustomKeyStoresoperação. Por padrão, essa operação retorna todos os armazenamentos de chaves personalizados em sua conta e região. No entanto, você pode usar o parâmetro `CustomKeyStoreId` e `CustomKeyStoreName` (mas não ambos) para limitar a resposta para determinados armazenamentos de chaves personalizados. O valor `ConnectionState` `DISCONNECTED` indica que o armazenamento de chaves do AWS CloudHSM de exemplo não está conectado ao cluster do 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>"
   ],
}
```

Excluir um armazenamento de chaves do AWS CloudHSM

Ao excluir um armazenamento de chaves do AWS CloudHSM, o AWS KMS exclui do KMS todos os metadados sobre o armazenamento de chaves do AWS CloudHSM, inclusive informações sobre sua associação a um cluster do AWS CloudHSM. Essa operação não afeta o cluster do AWS CloudHSM, seus HSMs, nem seus usuários. Você pode criar um novo armazenamento de chaves do AWS CloudHSM associado ao cluster do AWS CloudHSM, mas não é possível desfazer a operação de exclusão.

Você pode excluir um armazenamento de chaves do AWS CloudHSM que esteja desconectado do cluster do AWS CloudHSM e que não contenha AWS KMS keys. Antes de excluir um armazenamento de chaves personalizado, faça o seguinte.

- Verifique se você ainda precisará usar qualquer uma das chaves do KMS no armazenamento de chaves para operações de criptografia. Em seguida, programe a exclusão de todas as chaves do KMS do armazenamento de chaves. Para obter ajuda para localizar as chaves do KMS em um armazenamento de chaves do AWS CloudHSM, consulte Localizar as chaves do KMS em um armazenamento de chaves do AWS CloudHSM.

- Confirme se todas as chaves do KMS foram excluídas. Para visualizar as chaves do KMS em um armazenamento de chaves do AWS CloudHSM, consulte Visualizar chaves do KMS em um armazenamento de chaves do AWS CloudHSM.
- Desconectar o armazenamento de chaves do AWS CloudHSM do cluster do AWS CloudHSM.

Em vez de excluir o armazenamento de chaves do AWS CloudHSM, considere desconectá-lo do cluster do AWS CloudHSM associado. Enquanto o armazenamento de chaves do AWS CloudHSM está desconectado, é possível gerenciar o armazenamento de chaves do AWS CloudHSM e suas AWS KMS keys. No entanto, não é possível criar nem usar chaves do KMS no armazenamento de chaves do AWS CloudHSM. Você pode reconectar o armazenamento de chaves do AWS CloudHSM a qualquer momento.

Tópicos

- Excluir um armazenamento de chaves do AWS CloudHSM (console)
- Excluir um armazenamento de chaves do AWS CloudHSM (API)

Excluir um armazenamento de chaves do AWS CloudHSM (console)

Para excluir um armazenamento de chaves do AWS CloudHSM do AWS Management Console, comece selecionando o armazenamento de chaves do AWS CloudHSM na página Custom key stores (Armazenamentos de chaves personalizados).

1. Faça login no AWS Management Console e abra o console do AWS Key Management Service (AWS KMS) em https://console.aws.amazon.com/kms.
2. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.
3. No painel de navegação, selecione Custom key stores (Repositórios de chaves personalizados), AWS CloudHSM key stores (Repositórios de chaves do).
4. Encontre a linha que representa o armazenamento de chaves do AWS CloudHSM que você deseja excluir. Se o Connection state (Estado de conexão) do armazenamento de chaves do AWS CloudHSM não for Disconnected (Desconectado), você deverá desconectar o armazenamento de chaves do AWS CloudHSM antes de excluí-lo.
5. No menu Key store actions (Ações de armazenamento de chaves), escolha Delete (Excluir).

Quando a operação for concluída, uma mensagem de êxito será exibida, e o armazenamento de chaves do AWS CloudHSM não será mais exibido na lista de armazenamentos de chaves. Se a

operação não for bem-sucedida, será exibida uma mensagem de erro descrevendo o problema e fornecendo ajuda para corrigi-lo. Se precisar de ajuda adicional, consulte Solucionar problemas de um armazenamento de chaves personalizado.

Excluir um armazenamento de chaves do AWS CloudHSM (API)

Para excluir um armazenamento de AWS CloudHSM chaves, use a DeleteCustomKeyStoreoperação. Se a operação tiver êxito, o AWS KMS retornará uma resposta HTTP 200 e um objeto JSON sem propriedades.

Para começar, verifique se o armazenamento de chaves do AWS CloudHSM não contém AWS KMS keys. Não é possível excluir um armazenamento de chaves personalizado que contém chaves do KMS. O primeiro exemplo de comando usa ListKeyse DescribeKeypara pesquisar AWS KMS keys no armazenamento de AWS CloudHSM chaves com o exemplo *cks-1234567890abcdef0*, ID de armazenamento de chaves personalizado. Nesse caso, o comando não retorna chaves do KMS. Se isso acontecer, use a ScheduleKeyDeletionoperação para programar a exclusão de cada uma das chaves do 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'
```

Em seguida, desconecte o armazenamento de chaves do AWS CloudHSM. Este exemplo de comando usa a DisconnectCustomKeyStoreoperação para desconectar um armazenamento de AWS CloudHSM chaves de seu AWS CloudHSM cluster. Antes de executar um comando como esse, substitua o ID de exemplo do armazenamento de chaves personalizado por um válido.

Bash

```
$ aws kms disconnect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

PowerShell

```
PS C:\> Disconnect-KMSCustomKeyStore -CustomKeyStoreId cks-1234567890abcdef0
```

Depois que o armazenamento de chaves personalizadas for desconectado, você poderá usar a DeleteCustomKeyStoreoperação para excluí-lo.

Bash

```
$ aws kms delete-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

PowerShell

```
PS C:\> Remove-KMSCustomKeyStore -CustomKeyStoreId cks-1234567890abcdef0
```

Gerenciar chaves do KMS em um armazenamento de chaves do CloudHSM

Você pode criar, visualizar, gerenciar, usar e programar a exclusão de AWS KMS keys em um armazenamento de chaves do AWS CloudHSM. Os procedimentos são muito semelhantes aos usados em outras chaves do KMS. A única diferença é que você especifica um armazenamento de chaves do AWS CloudHSM ao criar a chave do KMS. Em seguida, o AWS KMS cria o material de chave não extraível para a chave do KMS no cluster do AWS CloudHSM associado ao armazenamento de chaves do AWS CloudHSM. Ao usar uma chave do KMS em um armazenamento de chaves do AWS CloudHSM, as operações de criptografia são executadas nos HSMs no cluster.

Recursos compatíveis

Além dos procedimentos discutidos nesta seção, você pode fazer o seguinte com chaves do KMS em um armazenamento de chaves do AWS CloudHSM:

- Usar políticas de chaves, políticas do IAM e concessões para autorizar o acesso às chaves do KMS.
- Habilite e desabilite as chaves do KMS.
- Atribua etiquetas, crie aliases e use o controle de acesso por atributo (ABAC) para autorizar o acesso às chaves do KMS.
- Usar as chaves do KMS para operações de criptografia, incluindo criptografar, descriptografar, recriptografar e gerar chaves de dados.

- Use as chaves do KMS com serviços da AWS que se integram ao AWS KMS e oferecem suporte a chaves gerenciadas pelo cliente.
- Acompanhe o uso de suas chaves KMS nos AWS CloudTrailregistros e nas ferramentas de CloudWatch monitoramento da Amazon.

Recursos sem suporte

- Armazenamentos de chaves do AWS CloudHSM são compatíveis apenas com chaves do KMS de criptografia simétrica. Você não pode criar chaves do KMS de HMAC, chaves do KMS assimétricas nem pares de chaves de dados assimétricas em um armazenamento de chaves do AWS CloudHSM.
- Você não pode importar material de chave em uma chave do KMS em um armazenamento de chaves do AWS CloudHSM. O AWS KMS gera o material de chave para a chave do KMS no cluster do AWS CloudHSM.
- Você não pode habilitar ou desabilitar a alternância automática do material da chave para uma chave do KMS em um armazenamento de chaves do AWS CloudHSM.

Tópicos

- Criar chaves do KMS em um armazenamento de chaves do AWS CloudHSM
- Visualizar chaves do KMS em um armazenamento de chaves do AWS CloudHSM
- Usar chaves do KMS em um armazenamento de chaves do AWS CloudHSM
- Encontrar chaves do KMS e materiais de chave
- Agendar a exclusão de chaves do KMS de um armazenamento de chaves do AWS CloudHSM

Criar chaves do KMS em um armazenamento de chaves do AWS CloudHSM

Depois de criar um armazenamento de chaves do AWS CloudHSM, você pode criar AWS KMS keys nesse armazenamento de chaves. Elas devem ser chaves do KMS de criptografia simétrica com material de chave gerado pelo AWS KMS. Não é possível criar chaves do KMS assimétricas, chaves do KMS de Hash-based message authentication code (HMAC – Código de autenticação de mensagem por hash) ou chaves do KMS com material de chave importado em um armazenamento personalizado de chave. Além disso, não é possível usar chaves do KMS de criptografia simétrica em um armazenamento personalizado de chaves para gerar pares de chaves assimétricos de dados.

Para criar uma chave do KMS em um armazenamento de chaves do AWS CloudHSM, o armazenamento de chaves do AWS CloudHSM deve estar conectado ao cluster do AWS CloudHSM associado, e esse cluster deve conter pelo menos dois HSMs ativos em diferentes zonas de disponibilidade. Para localizar o estado da conexão e o número de HSMs, visualize a página de armazenamentos de chaves do AWS CloudHSM no AWS Management Console. Ao usar as operações da API, use a DescribeCustomKeyStoresoperação para verificar se o armazenamento de AWS CloudHSM chaves está conectado. Para verificar o número de HSMs ativos no cluster e suas zonas de disponibilidade, use a AWS CloudHSM DescribeClustersoperação.

Quando você cria uma chave do KMS no armazenamento de chaves do AWS CloudHSM, o AWS KMS cria essa chave do KMS no AWS KMS. No entanto, ele cria o material de chave para a chave do KMS no cluster do AWS CloudHSM associado. Especificamente, o AWS KMS faz login no cluster como o CU do `kmsuser` que você criou. Em seguida, ele cria uma chave simétrica persistente e não extraível de AES (Advanced Encryption Standard) de 256 bits no cluster. O AWS KMS define o valor do atributo de rótulo de chave, que é visível apenas no cluster, como o nome do recurso da Amazon (ARN) da chave do KMS.

Quando o comando é bem-sucedido, o estado de chave da nova chave do KMS é `Enabled` e sua origem é `AWS_CLOUDHSM`. Não é possível alterar a origem de uma chave do KMS após a sua criação. Ao visualizar uma chave KMS em um armazenamento de AWS CloudHSM chaves no AWS KMS console ou usando a DescribeKeyoperação, você pode ver propriedades típicas, como ID da chave, estado da chave e data de criação. No entanto, você também pode ver o ID do armazenamento de chaves personalizado e (opcionalmente) o ID do cluster do AWS CloudHSM. Para obter detalhes, consulte Visualizar chaves do KMS em um armazenamento de chaves do AWS CloudHSM.

Se ocorrer uma falha na tentativa de criar uma chave do KMS no armazenamento de chaves do AWS CloudHSM, use a mensagem de erro para ajudar a determinar a causa. Ela pode indicar que o armazenamento de chaves do AWS CloudHSM não está conectado (`CustomKeyStoreInvalidStateException`) ou que o cluster do AWS CloudHSM associado não tem os dois HSMs ativos obrigatórios para essa operação (`CloudHsmClusterInvalidConfigurationException`). Para obter ajuda, consulte Solucionar problemas de um armazenamento de chaves personalizado.

Para obter um exemplo do log do AWS CloudTrail da operação que cria uma chave do KMS em um armazenamento de chaves do AWS CloudHSM, consulte CreateKey.

Tópicos

- Criar uma chave do KMS em um armazenamento de chaves do AWS CloudHSM (console)
- Criar uma chave do KMS em um armazenamento de chaves do AWS CloudHSM (API)

Criar uma chave do KMS em um armazenamento de chaves do AWS CloudHSM (console)

Adote o procedimento a seguir para criar uma chave do KMS de criptografia simétrica em um armazenamento de chaves do AWS CloudHSM.

> **Note**
>
> Não inclua informações confidenciais ou sigilosas no alias, na descrição ou nas tags. Esses campos podem aparecer em texto simples em CloudTrail registros e outras saídas.

1. Faça login no AWS Management Console e abra o console do AWS Key Management Service (AWS KMS) em https://console.aws.amazon.com/kms.
2. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.
3. No painel de navegação, escolha Customer managed keys (Chaves gerenciadas pelo cliente).
4. Escolha Create key (Criar chave).
5. Selecione Symmetric (Simétrica).
6. Em Key usage (Uso da chave), a opção Encrypt and decrypt (Criptografar e descriptografar) é selecionada para você. Não altere essa opção.
7. Escolha Advanced options (Opções avançadas).
8. Em Key material origin (Origem do material de chave), escolha AWS CloudHSM key store (Armazenamento de chaves do).

   Você não pode criar uma chave multirregional em um armazenamento de chaves do AWS CloudHSM.
9. Escolha Próximo.
10. Selecione um armazenamento de chaves do AWS CloudHSM para a nova chave do KMS. Para criar um novo armazenamento de chaves do AWS CloudHSM, escolha Create custom key store (Criar armazenamento de chaves personalizado).

    O armazenamento de chaves do AWS CloudHSM que você selecionar deve ter o status Connected (Conectado). Seu cluster do AWS CloudHSM associado deve estar ativo e conter pelo menos dois HSMs ativos em diferentes zonas de disponibilidade.

Para obter ajuda com a conexão de um armazenamento de chaves do AWS CloudHSM, consulte Conectar e desconectar um armazenamento de chaves do AWS CloudHSM. Para obter ajuda sobre como adicionar HSMs, consulte Adicionar um HSM, no Manual do usuário do AWS CloudHSM.

11. Escolha Próximo.
12. Digite um alias e uma descrição opcional para a chave do KMS.
13. (Opcional). Na página Add Tags (Adicionar etiquetas), adicione etiquetas que identificam ou categorizam a chave do KMS.

    Ao adicionar tags aos recursos da AWS, a AWS gera um relatório de alocação de custos com utilização e custos agrupados por tags. Etiquetas também podem ser utilizadas para controlar o acesso a uma chave do KMS. Para informações sobre marcação de chaves do KMS, consulte Marcar chaves com tags e ABAC para AWS KMS.
14. Escolha Próximo.
15. Na seção Key Administrators (Administradores de chaves), selecione os usuários e as funções do IAM que podem gerenciar a chave do KMS. Para obter mais informações, consulte Permite que administradores de chaves administrem a chave do KMS.

    > **Note**
    >
    > As políticas do IAM podem conceder permissão para usar a chave do KMS a outros usuários e funções do IAM.
    > As práticas recomendadas do IAM não encorajam o uso de usuários do IAM com credenciais de longo prazo. Sempre que possível, use os perfis do IAM, por fornecerem credenciais temporárias. Para obter detalhes, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.
16. (Opcional) Para evitar que esses administradores de chaves excluam essa chave do KMS, desmarque a caixa na parte inferior da página para Permitir que os administradores de chaves excluam essa chave.
17. Escolha Próximo.
18. Na seção This account (Esta conta), selecione os usuários e as funções do IAM nessa Conta da AWS que podem usar a chave do KMS em operações de criptografia. Para obter mais informações, consulte Permite que os usuários de chaves usem a chave do KMS.

> **Note**
>
> As políticas do IAM podem conceder permissão para usar a chave do KMS a outros usuários e funções do IAM.
> As práticas recomendadas do IAM não encorajam o uso de usuários do IAM com credenciais de longo prazo. Sempre que possível, use os perfis do IAM, por fornecerem credenciais temporárias. Para obter detalhes, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

19. (Opcional) Você pode permitir que outras Contas da AWS usem essa chave do KMS para operações de criptografia. Para fazer isso, na seção Other Contas da AWS (Outras Conta da AWS) na parte inferior da página, escolha Add another Conta da AWS (Adicionar outra) e insira o ID da de uma conta externa. Para adicionar várias contas externas, repita essa etapa.

> **Note**
>
> Os administradores das outras Contas da AWS também devem permitir o acesso à chave do KMS criando políticas do IAM para seus usuários. Para ter mais informações, consulte Permitir que usuários de outras contas usem uma chave do KMS.

20. Escolha Próximo.
21. Revise as configurações que você escolheu. Ainda é possível voltar e alterar todas as configurações.
22. Quando terminar, escolha Finish (Terminar) para criar a chave.

Se o procedimento for bem-sucedido, a tela exibirá a nova chave do KMS no armazenamento de chaves do AWS CloudHSM que você escolheu. Ao escolher o nome ou alias para a nova chave do KMS, a guia Cryptographic configuration (Configuração criptográfica) da página de detalhes exibe a origem da chave do KMS (AWS CloudHSM), o ID e o tipo de armazenamento de chaves personalizado, e o ID do cluster do AWS CloudHSM. Se houver falha no procedimento, uma mensagem descrevendo a falha será exibida.

> **Tip**
>
> Para facilitar a identificação de chaves do KMS em um armazenamento de chaves personalizado, na página Customer managed keys (Chaves gerenciadas pelo cliente),

adicione a coluna Custom key store ID (ID de armazenamento de chaves personalizado) à exibição. Clique no ícone de engrenagem no canto superior direito e selecione Custom key store ID (ID de armazenamento de chaves personalizado). Para obter detalhes, consulte Personalizar suas tabelas de chaves do KMS.

Criar uma chave do KMS em um armazenamento de chaves do AWS CloudHSM (API)

Para criar uma nova AWS KMS key(chave KMS) em seu armazenamento de AWS CloudHSM chaves, use a CreateKeyoperação. Use o parâmetro `CustomKeyStoreId` para identificar o armazenamento de chaves personalizado e especificar um valor de `Origin` da `AWS_CLOUDHSM`.

Você também pode usar o parâmetro `Policy` para especificar uma política de chaves. Você pode alterar a política de chaves (PutKeyPolicy) e adicionar elementos opcionais, como uma descrição e tags, a qualquer momento.

Os exemplos nesta seção usam a AWS Command Line Interface (AWS CLI), mas você pode usar qualquer linguagem de programação compatível.

O exemplo a seguir começa com uma chamada para a DescribeCustomKeyStoresoperação para verificar se o armazenamento de AWS CloudHSM chaves está conectado ao AWS CloudHSM cluster associado. Por padrão, essa operação retorna todos os armazenamentos de chaves personalizados em sua conta e região. Para descrever apenas determinado armazenamento de chaves do AWS CloudHSM, use o parâmetro `CustomKeyStoreId` ou `CustomKeyStoreName` (mas não ambos).

Antes de executar um comando como esse, substitua o ID de exemplo do armazenamento de chaves personalizado por um ID válido.

Note

Não inclua informações confidenciais ou sigilosas nos campos `Description` ou `Tags`. Esses campos podem aparecer em texto simples em CloudTrail registros e outras saídas.

```
$ 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"
   ],
}
```

O próximo comando de exemplo usa a DescribeClustersoperação para verificar se o AWS CloudHSM cluster associado ao `ExampleKeyStore` (cluster-1a23b4cdefg) tem pelo menos dois HSMs ativos. Se o cluster tiver menos de dois HSMs, ocorrerá falha na operação `CreateKey`.

```
$ 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"
        }
    ]
}
```

Este exemplo de comando usa a CreateKeyoperação para criar uma chave KMS em um armazenamento de AWS CloudHSM chaves. Para criar uma chave do KMS em um armazenamento de chaves do AWS CloudHSM, você deve fornecer o ID do armazenamento de chaves do AWS CloudHSM e especificar um valor de `Origin` igual a `AWS_CLOUDHSM`.

A resposta inclui os IDs de armazenamento de chaves personalizado e o cluster do AWS CloudHSM.

Antes de executar um comando como esse, substitua o ID de exemplo do armazenamento de chaves personalizado por um ID válido.

```
$ 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"
    ]
  }
}
```

Visualizar chaves do KMS em um armazenamento de chaves do AWS CloudHSM

Para visualizar o AWS KMS keys em um armazenamento de chaves do AWS CloudHSM, use as mesmas técnicas que você usaria para visualizar qualquer chave gerenciada pelo cliente do AWS KMS. Para aprender os conceitos básicos, consulte Visualizar chaves. Para identificar as chaves no cluster do AWS CloudHSM que funcionam como material de chave para a sua chave do KMS, consulte Encontrar chaves do KMS e materiais de chave. Para obter informações sobre como visualizar os logs do AWS CloudTrail que registram todas as operações da API em um armazenamento de chaves personalizado, consulte Registrando chamadas de AWS KMS API com AWS CloudTrail.

No console do AWS KMS, as chaves do KMS do armazenamento de chaves personalizado são exibidas na página Customer managed keys (Chaves gerenciadas pelo cliente) juntamente com todas as outras chaves gerenciadas pelo cliente em sua Conta da AWS e região.

No entanto, os seguintes valores são específicos para chaves do KMS em um armazenamento de chaves do AWS CloudHSM.

- O nome e o ID do armazenamento de chaves do AWS CloudHSM que armazena a chave do KMS.
- O ID do cluster do AWS CloudHSM associado que contém seu material de chaves.
- Um valor `Origin` de `AWS CloudHSM` no console do AWS KMS ou `AWS_CLOUDHSM` em respostas de API.
- O valor do estado da chave pode estar `Unavailable`. Para obter ajuda para resolver o status, consulte Como corrigir chaves do KMS indisponíveis.

Para visualizar as chaves do KMS em um armazenamento de chaves do AWS CloudHSM (console)

1. Abra o console do AWS KMS em https://console.aws.amazon.com/kms.
2. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.
3. No painel de navegação, escolha Customer managed keys (Chaves gerenciadas pelo cliente).
4. No canto superior direito, selecione o ícone de engrenagem, escolha Custom key store ID (ID de armazenamento de chaves personalizado) e Origin (Origem) e escolha Confirm (Confirmar).

5. Para identificar chaves do KMS em qualquer armazenamento de chaves do AWS CloudHSM, procure chaves do KMS com um valor de Origin (Origem) do AWS CloudHSM. Para identificar chaves do KMS em um determinado armazenamento de chaves do AWS CloudHSM, visualize os valores na coluna Custom key store ID (ID de armazenamento de chaves personalizado).
6. Escolha o alias ou ID de chave de uma chave do KMS em um armazenamento de chaves do AWS CloudHSM.

   Essa página exibe informações detalhadas sobre a chave do KMS, incluindo seu Amazon Resource Name (ARN), sua política de chaves e suas etiquetas.
7. Selecione a guia Cryptographic configuration (Configuração criptográfica). As guias estão abaixo da seção General configuration (Configuração geral).

   Essa seção inclui informações sobre o armazenamento de chaves do AWS CloudHSM e o cluster do AWS CloudHSM associado às chaves do KMS.

Para visualizar as chaves do KMS em um armazenamento de chaves personalizado (API)

Você usa as mesmas operações de AWS KMS API para visualizar as chaves KMS em um armazenamento de AWS CloudHSM chaves que você usaria para qualquer chave KMS, incluindo ListKeysDescribeKey, e. GetKeyPolicy Por exemplo, a seguinte operação `describe-key` na AWS CLI mostra os campos especiais de uma chave do KMS em um armazenamento de chaves do AWS CloudHSM. Antes de executar um comando como esse, substitua o ID de exemplo por um valor válido.

```
$ 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"
    }
}
```

Para ajudar a encontrar as chaves do KMS em um armazenamento de chaves do AWS CloudHSM ou identificar as chaves no cluster do AWS CloudHSM que funcionam como material de chave para a sua chave do KMS, consulte Encontrar chaves do KMS e materiais de chave.

Usar chaves do KMS em um armazenamento de chaves do AWS CloudHSM

Após criar uma chave do KMS de criptografia simétrica em um armazenamento de chaves do AWS CloudHSM, é possível usá-la para as seguintes operações de criptografia:

- Encrypt
- Decrypt
- GenerateDataKey
- GenerateDataKeyWithoutPlaintext
- ReEncrypt

As operações que geram pares de chaves de dados assimétricos, GenerateDataKeyPaire GenerateDataKeyPairWithoutPlaintext, não são suportadas em armazenamentos de chaves personalizadas.

Ao usar sua chave do KMS em uma solicitação, identifique a chave do KMS pelo ID ou alias. Não é necessário especificar o armazenamento de chaves do AWS CloudHSM ou o cluster do AWS CloudHSM. A resposta inclui os mesmos campos que são retornados para qualquer chave do KMS de criptografia simétrica.

No entanto, quando você usa uma chave do KMS em um armazenamento de chaves do AWS CloudHSM, a operação de criptografia é executada inteiramente no cluster do AWS CloudHSM que está associado ao armazenamento de chaves do AWS CloudHSM. A operação usa o material de chave no cluster associado à chave do KMS escolhida.

Para tornar isso possível, as seguintes condições são necessárias.

- O estado de chave da chave do KMS deve ser `Enabled`. Para encontrar o estado da chave, use o campo Status no AWS KMSconsole ou o `KeyState` campo na DescribeKeyresposta.
- O armazenamento de chaves do AWS CloudHSM deve ser conectado ao cluster do AWS CloudHSM. Seu status no AWS KMSconsole ou `ConnectionState` na DescribeCustomKeyStoresresposta deve ser`CONNECTED`.
- O cluster do AWS CloudHSM associado ao armazenamento de chaves personalizado deve conter pelo menos um HSM ativo. Para encontrar o número de HSMs ativos no cluster, use o AWS KMSconsole, o AWS CloudHSM console ou a DescribeClustersoperação.
- O cluster do AWS CloudHSM deve conter o material de chave da chave do KMS. Se o material de chaves foi excluído do cluster ou um HSM foi criado de um backup que não incluía o material de chaves, haverá falha na operação de criptografia.

Se essas condições não forem atendidas, haverá falha na operação de criptografia, e o AWS KMS retornará uma exceção `KMSInvalidStateException`. Normalmente, você só precisará reconectar o armazenamento de chaves do AWS CloudHSM. Para obter ajuda adicional, consulte Como corrigir uma chave do KMS com falha.

Ao usar as chaves do KMS em um armazenamento de chaves do AWS CloudHSM, esteja ciente de que as chaves do KMS em cada armazenamento de chaves do AWS CloudHSM compartilha uma cota de solicitações de armazenamento de chaves personalizado para operações de criptografia. Se você exceder a cota, o AWS KMS retornará um `ThrottlingException`. Se o cluster do AWS CloudHSM associado ao armazenamento de chaves do AWS CloudHSM estiver processando vários comandos, incluindo aqueles não relacionados ao armazenamento de chaves do AWS CloudHSM, você poderá obter `ThrottlingException` a uma taxa ainda menor. Se você receber uma `ThrottlingException` para qualquer solicitação, diminua a sua taxa de solicitações e tente os comandos novamente. Para obter detalhes sobre a cota de solicitações do armazenamento de chaves personalizado, consulte Cotas de solicitação de armazenamento de chaves personalizadas.

Encontrar chaves do KMS e materiais de chave

Se você gerencia um armazenamento de chaves do AWS CloudHSM, pode ser necessário identificar as chaves do KMS em cada armazenamento de chaves do AWS CloudHSM. Por exemplo, pode ser necessário executar uma das seguintes tarefas.

- Acompanhe as chaves do KMS no armazenamento de chaves do AWS CloudHSM em logs do AWS CloudTrail.

- Preveja o efeito nas chaves do KMS de desconectar um armazenamento de chaves do AWS CloudHSM.
- Agende a exclusão de chaves do KMS antes de excluir um armazenamento de chaves do AWS CloudHSM.

Além disso, é recomendável identificar as chaves no cluster do AWS CloudHSM que funcionam como material de chave para as suas chaves do KMS. Embora o AWS KMS gerencie as chaves do KMS e seu material de chave, você ainda mantém o controle e a responsabilidade pelo gerenciamento do cluster do AWS CloudHSM, bem como dos seus HSMs e backups e as chaves nos HSMs. Talvez você precise identificar as chaves para auditar o material de chave, protegê-lo contra exclusão acidental ou excluí-lo de HSMs e backups de cluster após a exclusão da chave do KMS.

Todo o material de chave para as suas chaves do KMS no armazenamento de chaves do AWS CloudHSM pertence ao usuário de criptografia `kmsuser`. O AWS KMS define o atributo do rótulo de chave, que pode ser visualizado apenas no AWS CloudHSM, ao nome do recurso da Amazon (ARN) das chaves do KMS.

Para encontrar as chaves do KMS e o material de chave, use uma das técnicas a seguir.

- Localizar as chaves do KMS em um armazenamento de chaves do AWS CloudHSM: como identificar as chaves do KMS em um ou todos os seus armazenamentos de chaves do AWS CloudHSM.
- Localizar todas as chaves de um armazenamento de chaves do AWS CloudHSM: como encontrar todas as chaves no cluster que funcionam como material de chave para as chaves do KMS no armazenamento de chaves do AWS CloudHSM.
- Localizar a chave do AWS CloudHSM para uma chave do KMS: como encontrar a chave em seu cluster que funciona como material de chave para uma chave do KMS específica no armazenamento de chaves do AWS CloudHSM.
- Localizar a chave do KMS para uma chave do AWS CloudHSM: como encontrar a chave do KMS para uma determinada chave no seu cluster.

Localizar as chaves do KMS em um armazenamento de chaves do AWS CloudHSM

Se você gerencia um armazenamento de chaves do AWS CloudHSM, pode ser necessário identificar as chaves do KMS em cada armazenamento de chaves do AWS CloudHSM. Você pode usar essas

informações para rastrear as operações de chaves do KMS em logs do AWS CloudTrail, prever o efeito nas chaves do KMS ao desconectar um armazenamento de chaves personalizado ou agendar a exclusão de chaves do KMS antes de excluir um armazenamento de chaves do AWS CloudHSM.

Como encontrar as chaves do KMS em um armazenamento de chaves do AWS CloudHSM (console)

Para encontrar as chaves do KMS em um determinado armazenamento de chaves do AWS CloudHSM, na página Customer Managed Keys (Chaves gerenciadas pelo cliente), visualize os valores nos campos Custom Key Store Name (Nome do armazenamento de chaves personalizado) ou Custom Key Store ID (ID do armazenamento de chaves personalizado). Para identificar chaves do KMS em qualquer armazenamento de chaves do AWS CloudHSM, procure chaves do KMS com um valor de Origin (Origem) do AWS CloudHSM. Para adicionar colunas opcionais à exibição, selecione o ícone de engrenagem no canto superior direito da página.

Para encontrar as chaves do KMS em um armazenamento de chaves do AWS CloudHSM (API)

Para encontrar as chaves KMS em um armazenamento de AWS CloudHSM chaves, use as DescribeKeyoperações ListKeyse e depois filtre por `CustomKeyStoreId` valor. Antes de executar os exemplos, substitua os valores de ID fictícios do armazenamento de chaves personalizado por um valor válido.

Bash

Para encontrar chaves do KMS em determinado armazenamento de chaves do AWS CloudHSM, obtenha todas as chaves do KMS na conta e região. Filtre pelo ID do armazenamento de chaves personalizado.

```
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
```

Para obter chaves do KMS em qualquer armazenamento de chaves do AWS CloudHSM na conta e região, procure `CustomKeyStoreType` com o valor `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

Para encontrar chaves KMS em um determinado armazenamento de AWS CloudHSM chaves, use os KmsKey cmdlets Get- KmsKeyList e Get- para obter todas as suas chaves KMS na conta e na região. Filtre pelo ID do armazenamento de chaves personalizado.

```
PS C:\> Get-KMSKeyList | Get-KMSKey | where CustomKeyStoreId -eq
 'cks-1234567890abcdef0'
```

Para obter as chaves KMS em qualquer armazenamento de AWS CloudHSM chaves na conta e na região, filtre pelo CustomKeyStoreType valor de`AWS_CLOUDHSM`.

```
PS C:\> Get-KMSKeyList | Get-KMSKey | where CustomKeyStoreType -eq 'AWS_CLOUDHSM'
```

Localizar todas as chaves de um armazenamento de chaves do AWS CloudHSM

Você pode identificar as chaves no cluster do AWS CloudHSM que funcionam como material de chaves para o armazenamento de chaves do AWS CloudHSM. Para fazer isso, use o findAllKeyscomando em cloudhsm_mgmt_util para encontrar os identificadores de chave de todas as chaves que possuem ou compartilham. `kmsuser` A menos que você tenha se conectado como `kmsuser` e criado chaves fora do AWS KMS, todas as chaves que o `kmsuser` possui representam materiais de chave para chaves do KMS.

Qualquer responsável pela criptografia no cluster pode executar esse comando sem desconectar o armazenamento de chaves do AWS CloudHSM.

1. Inicie cloudhsm_mgmt_util usando o procedimento descrito no tópico Getting started with CloudHSM Management Utility (CMU) (Conceitos básicos do CloudHSM Management Utility [CMU]).
2. Faça login no cloudhsm_mgmt_util usando a conta de um responsável pela criptografia (CO).
3. Use o comando listUsers para encontrar o ID de usuário do usuário de criptografia `kmsuser`.

   Neste exemplo, o `kmsuser` possui ID de usuário 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. Use o findAllKeyscomando para encontrar os identificadores de teclas de todas as chaves que `kmsuser` possuem ou compartilham. Substitua o ID de usuário de exemplo (3) pelo o ID de usuário real do `kmsuser` no cluster.

   A saída de exemplo mostra que o `kmsuser` possui chaves com identificadores de chave 8, 9 e 262162 em ambos os HSMs no 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)
```

Localizar a chave do KMS para uma chave do AWS CloudHSM

Se você conhece o identificador de uma chave que o `kmsuser` possui no cluster, pode usar o rótulo da chaves para identificar a chave do KMS associada no armazenamento de chaves do AWS CloudHSM.

Quando o AWS KMS cria o material de chave para uma chave do KMS no seu cluster do AWS CloudHSM, ele grava o Amazon Resource Name (ARN) dessa chave do KMS no rótulo de chave. A menos que você tenha alterado o valor do rótulo, é possível usar o comando getAttribute ou cloudhsm_mgmt_util para associar essa chave à sua chave do KMS.

Para executar esse procedimento, você precisa desconectar temporariamente o armazenamento de chaves do AWS CloudHSM para poder fazer login como usuário de criptografia `kmsuser`.

> **Note**
>
> Enquanto um armazenamento de chaves personalizado estiver desconectado, todas as tentativas de criar chaves do KMS nele ou de usar chaves do KMS existentes em operações de criptografia falharão. Essa ação pode impedir que os usuários armazenem e acessem dados sigilosos.

1. Desconecte o armazenamento de chaves do AWS CloudHSM, caso ainda não tenha sido desconectado, e faça login no key_mgmt_util como `kmsuser`, conforme explicado em Como desconectar e fazer login.
2. Use o comando `getAttribute` em key_mgmt_util ou cloudhsm_mgmt_util para obter o atributo do rótulo (`OBJ_ATTR_LABEL`, atributo `3`) para um determinado identificador de chave.

   Por exemplo, esse comando usa `getAttribute` em cloudhsm_mgmt_util para obter o atributo do rótulo (atributo `3`) da chave com o identificador de chave `262162`. A saída mostra que a chave `262162` serve como material de chave para a chave do KMS com o ARN `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`. Antes de executar um comando como esse, substitua o identificador de chave de exemplo por um válido.

   Para obter uma lista de atributos de chave, use o comando listAttributes ou consulte a Referência de atributos de chave no Manual do usuário do 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. Encerre a sessão do key_mgmt_util ou cloudhsm_mgmt_util e reconecte o armazenamento de chaves do AWS CloudHSM, conforme descrito em Como fazer logout e se conectar novamente.

Localizar a chave do AWS CloudHSM para uma chave do KMS

Você pode usar o ID de uma chave do KMS em um armazenamento de chaves do AWS CloudHSM para identificar a chave no cluster do AWS CloudHSM que serve como material de chave. Você pode usar o identificador de chave para identificar a chave em comandos do cliente AWS CloudHSM.

Quando o AWS KMS cria o material de chave para uma chave do KMS no seu cluster do AWS CloudHSM, ele grava o Amazon Resource Name (ARN) dessa chave do KMS no rótulo de chave. A menos que você tenha alterado o valor do rótulo, pode usar o comando findKey em key_mgmt_util para obter o identificador de chaves do material de chave da chave do KMS. Para executar esse procedimento, você precisa desconectar temporariamente o armazenamento de chaves do AWS CloudHSM para poder fazer login como usuário de criptografia `kmsuser`.

> **Note**
>
> Enquanto um armazenamento de chaves personalizado estiver desconectado, todas as tentativas de criar chaves do KMS nele ou de usar chaves do KMS existentes em operações de criptografia falharão. Essa ação pode impedir que os usuários armazenem e acessem dados sigilosos.

1. Desconecte o armazenamento de chaves do AWS CloudHSM, caso ainda não tenha sido desconectado e faça login no key_mgmt_util como `kmsuser`, conforme explicado em Como desconectar e fazer login.
2. Use o comando findKey em key_mgmt_util para procurar uma chave com um rótulo que corresponda ao ARN de uma chave do KMS no armazenamento de chaves do AWS CloudHSM. Substitua o exemplo de ARN da chave do KMS no valor do parâmetro `-l` (L minúsculo de "label") por um ARN de chave do KMS válido.

   Por exemplo, esse comando encontra a chave com um rótulo que corresponde ao exemplo de ARN de chave do KMS, `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`. O exemplo de saída mostra que a chave com identificador 262162 tem o ARN de chave do KMS especificado em seu rótulo. Agora você pode usar esse identificador de chave em outros comandos 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. Encerre a sessão do key_mgmt_util e reconecte o armazenamento de chaves personalizado, conforme descrito em Como fazer logout e se conectar novamente.

Agendar a exclusão de chaves do KMS de um armazenamento de chaves do AWS CloudHSM

Quando tiver certeza de que não será necessário usar uma AWS KMS key para nenhuma operação criptográfica, você poderá programar a exclusão da chave do KMS. Use o mesmo procedimento que você usaria para programar a exclusão de qualquer chave do KMS do AWS KMS. Além disso, mantenha o armazenamento de chaves do AWS CloudHSM conectado para que o AWS KMS exclua o material de chave correspondente do cluster do AWS CloudHSM associado quando o período de espera expirar.

Você pode monitorar o agendamento, o cancelamento e a exclusão da chave do KMS em seus logs do AWS CloudTrail.

> **Warning**
>
> A exclusão de uma chave do KMS é uma operação destrutiva e potencialmente perigosa que evita a recuperação de todos os dados criptografados sob essa chave do KMS. Antes de programar a exclusão da chave KMS, examine o uso anterior da chave KMS e crie um CloudWatch alarme da Amazon que alerta você quando alguém tentar usar a chave KMS enquanto ela estiver pendente de exclusão. Sempre que possível, desabilite a chave do KMS em vez de excluí-la.

Se você agendar a exclusão de uma chave do KMS de um armazenamento de chaves do AWS CloudHSM, o estado da chave será alterado para Pending deletion (Exclusão pendente). A chave do KMS permanecerá no estado Pending deletion (Exclusão pendente) durante todo o período de espera, mesmo que ela fique indisponível porque você desconectou o armazenamento de chaves

personalizado. Isso permite que você cancele a exclusão da chave do KMS a qualquer momento durante o período de espera.

Quando o período de espera expirar, o AWS KMS excluirá a chave do KMS do AWS KMS. O AWS KMS faz o possível para excluir o material de chaves do cluster do AWS CloudHSM associado. Se o AWS KMS não puder excluir o material de chaves, como, por exemplo, quando o armazenamento de chaves é desconectado do AWS KMS, pode ser necessário excluir manualmente o material de chaves órfãs do cluster.

O AWS KMS não exclui o material de chaves de backups do cluster. Mesmo que você exclua a chave do KMS do AWS KMS e seu material de chave do cluster do AWS CloudHSM, os clusters criados a partir de backups podem conter o material de chave excluído. Para excluir permanentemente o material de chave, visualize a data de criação da chave do KMS. Em seguida, exclua todos os backups do cluster que podem conter o material de chaves.

Quando você agenda a exclusão de uma chave do KMS de um armazenamento de chaves do AWS CloudHSM, a chave do KMS torna-se inutilizável imediatamente (sujeita a consistência posterior). Contudo, os recursos criptografados com chaves de dados protegidas pela chave do KMS não serão afetados até que a chave do KMS seja usada novamente, por exemplo, para descriptografar a chave de dados. Esse problema afeta os Serviços da AWS, pois muitos deles usam chaves de dados para proteger recursos. Para obter mais detalhes, consulte Como as chaves do KMS inutilizáveis afetam as chaves de dados.

Solucionar problemas de um armazenamento de chaves personalizado

Os armazenamentos de chaves do AWS CloudHSM foram projetados para serem disponíveis e resilientes. No entanto, há algumas condições de erro que você pode ter de reparar para manter o armazenamento de chaves do AWS CloudHSM em operação.

Tópicos

- Como corrigir chaves do KMS indisponíveis
- Como corrigir uma chave do KMS com falha
- Como corrigir uma falha de conexão
- Como responder a uma falha de operação criptográfica
- Como corrigir credenciais kmsuser inválidas
- Como excluir material de chave órfã
- Como recuperar materiais de chave excluídos de uma chave do KMS

- Como fazer login como kmsuser

Como corrigir chaves do KMS indisponíveis

O estado da chave de AWS KMS keys em um armazenamento de chaves do AWS CloudHSM normalmente é `Enabled`. Como todas as chaves do KMS, o estado de chave é alterado quando você desabilita as chaves do KMS em um armazenamento de chaves do AWS CloudHSM ou agenda sua exclusão. No entanto, ao contrário de outras chaves do KMS, as chaves do KMS em um armazenamento de chaves personalizado também podem ter um estado de chave `Unavailable`.

Um estado de chave `Unavailable` indica que a chave do KMS está em um armazenamento de chaves personalizado que foi intencionalmente desconectado e que as tentativas de reconectá-lo, se houver, não foram bem-sucedidas. Enquanto uma chave do KMS está indisponível, é possível visualizá-la e gerenciá-la, mas não é possível usá-la para operações de criptografia.

Para encontrar o estado de chave de uma chave do KMS, na página Customer managed keys (Chaves gerenciadas pelo cliente), visualize o campo Status da chave do KMS. Ou use a DescribeKeyoperação e visualize o `KeyState` elemento na resposta. Para obter detalhes, consulte Visualizar chaves.

As chaves do KMS em um armazenamento de chaves personalizado desconectado terão o estado de chave `Unavailable` ou `PendingDeletion`. As chaves do KMS agendadas para exclusão de um armazenamento de chaves personalizado têm um estado de chave `Pending Deletion`, mesmo quando o armazenamento de chaves personalizado está desconectado. Isso permite que você cancele a programação da exclusão de chaves sem reconectar o armazenamento de chaves personalizado.

Para corrigir uma chave do KMS indisponível, reconecte o armazenamento de chaves personalizado. Após a reconexão do armazenamento de chaves personalizado, o estado de chave das chaves do KMS nesse armazenamento é automaticamente restaurado ao estado anterior, como `Enabled` ou `Disabled`. Chaves do KMS com exclusão pendente permanecem no estado `PendingDeletion`. No entanto, enquanto o problema persistir, habilitar ou desabilitar uma chave do KMS indisponível não altera seu estado de chave. A ação habilitar ou desabilitar entra em vigor somente quando a chave é disponibilizada.

Para obter ajuda com conexões com falha, consulte Como corrigir uma falha de conexão.

Como corrigir uma chave do KMS com falha

Problemas com a criação e o uso de chaves do KMS em armazenamentos de chaves do AWS CloudHSM podem ser causados por um problema no armazenamento de chaves do AWS CloudHSM, no cluster do AWS CloudHSM associado, na chave do KMS ou no material de chave.

Quando um armazenamento de chaves do AWS CloudHSM é desconectado do cluster do AWS CloudHSM, o estado de chave das chaves do KMS no armazenamento de chaves personalizado é `Unavailable`. Todas as solicitações para criar chaves do KMS em um armazenamento de chaves do AWS CloudHSM desconectado retornam uma exceção `CustomKeyStoreInvalidStateException`. Todas as solicitações para criptografar, descriptografar e criptografar novamente ou gerar chaves de dados retornam uma exceção `KMSInvalidStateException`. Para corrigir o problema, reconecte o armazenamento de chaves do AWS CloudHSM.

No entanto, suas tentativas de usar uma chave do KMS em um armazenamento de chaves do AWS CloudHSMpara operações de criptografia podem falhar mesmo quando o estado da chave é `Enabled` e o estado da conexão do armazenamento de chaves do AWS CloudHSM é `Connected`. Isso pode ser causado por uma das seguintes condições.

- O material de chave para a chave do KMS pode ter sido excluído do cluster do AWS CloudHSM associado. Para investigar, localize o identificador de chave do material de chave para uma chave do KMS e, se necessário, tente recuperar o material de chave.
- Todos os HSMs foram excluídos do cluster do AWS CloudHSM associado ao armazenamento de chaves do AWS CloudHSM. Para usar uma chave do KMS em um armazenamento de chaves do AWS CloudHSM em uma operação de criptografia, seu cluster do AWS CloudHSM deve conter pelo menos um HSM ativo. Para verificar o número e o estado dos HSMs em um AWS CloudHSM cluster, use o AWS CloudHSM console ou a DescribeClustersoperação. Para adicionar um HSM ao cluster, use o AWS CloudHSM console ou a CreateHsmoperação.
- O cluster do AWS CloudHSM associado ao armazenamento de chaves do AWS CloudHSM foi excluído. Para corrigir o problema, crie um cluster a partir de um backup relacionado ao cluster original, como um backup do cluster original, ou um backup que foi usado para criar o cluster original. Edite o ID do cluster nas configurações do armazenamento de chaves personalizado. Para obter instruções, consulte Como recuperar materiais de chave excluídos de uma chave do KMS.
- O cluster do AWS CloudHSM associado ao armazenamento de chaves personalizado não tinha sessões do PKCS #11 disponíveis. Isso geralmente ocorre durante períodos de alto tráfego de

intermitência quando sessões adicionais são necessárias para atender ao tráfego. Para responder a um `KMSInternalException` com uma mensagem de erro sobre as sessões do PKCS #11, volte e repita a solicitação.

Como corrigir uma falha de conexão

Se você tentar conectar um armazenamento de chaves do AWS CloudHSM ao cluster do AWS CloudHSM, mas a operação falhar, o estado da conexão do armazenamento de chaves do AWS CloudHSM será alterado para `FAILED`. Para encontrar o estado da conexão de um armazenamento de AWS CloudHSM chaves, use o AWS KMS console ou a DescribeCustomKeyStoresoperação.

Como alternativa, algumas tentativas de conexão falham rapidamente devido a erros de configuração de cluster facilmente detectados. Nesse caso, o estado da conexão ainda é `DISCONNECTED`. Essas falhas retornar uma mensagem de erro ou exceção que explica por que a tentativa falhou. Analise a descrição da exceção e os requisitos do cluster, corrija o problema, atualize o armazenamento de chaves do AWS CloudHSM, se necessário, e tente se conectar novamente.

Quando o estado da conexão estiver`FAILED`, execute a DescribeCustomKeyStoresoperação e veja o `ConnectionErrorCode` elemento na resposta.

> **Note**
>
> Quando o estado da conexão de um armazenamento de chaves do AWS CloudHSM for `FAILED`, você deverá desconectar o armazenamento de chaves do AWS CloudHSM antes de tentar reconectá-lo. Você não pode conectar um armazenamento de chaves do AWS CloudHSM com um estado de conexão `FAILED`.

- `CLUSTER_NOT_FOUND` indica que o AWS KMS não consegue encontrar o cluster do AWS CloudHSM com o ID do cluster especificado. Isso pode ocorrer quando o ID de cluster errado é fornecido para uma operação de API ou o cluster é excluído e não substituído. Para corrigir esse erro, verifique o ID do cluster, por exemplo, usando o AWS CloudHSM console ou a DescribeClustersoperação. Se o cluster foi excluído, crie um cluster a partir de um backup recente do original. Desconecte o armazenamento de chaves do AWS CloudHSM, edite o armazenamento de chaves do AWS CloudHSMna configuração de ID do cluster e reconecte o armazenamento de chaves do AWS CloudHSM ao cluster.
- `INSUFFICIENT_CLOUDHSM_HSMS` indica que o cluster do AWS CloudHSM associado não contém HSMs. Para se conectar, o cluster deve ter pelo menos um HSM. Para encontrar o número de

HSMs no cluster, use a DescribeClustersoperação. Para corrigir esse erro, adicione pelo menos um HSM ao cluster. Se você adicionar vários HSMs, é melhor criá-los em diferentes zonas de disponibilidade.

- `INSUFFICIENT_FREE_ADDRESSES_IN_SUBNET` indica que o AWS KMS não pôde conectar o armazenamento de chaves do AWS CloudHSM ao cluster do AWS CloudHSM porque pelo menos uma sub-rede privada associada ao cluster não tem um endereço IP disponível. Uma conexão de armazenamento de chaves do AWS CloudHSM requer um endereço IP livre em cada uma das sub-redes privadas associadas, embora dois endereços IP sejam preferíveis.

  Não é possível adicionar endereços IP (blocos CIDR) a uma sub-rede existente. Se possível, mova ou exclua outros recursos que estejam usando os endereços IP na sub-rede, como instâncias do EC2 não utilizadas ou interfaces elásticas de rede. Caso contrário, crie um cluster a partir de um backup recente do cluster AWS CloudHSM com sub-redes privadas novas ou existentes que tenham mais espaço de endereço livre. Depois, para associar o novo cluster ao armazenamento de chaves do AWS CloudHSM, desconecte o armazenamento de chaves personalizado, altere o ID do cluster do armazenamento de chaves do AWS CloudHSM para o ID do novo cluster e tente se conectar novamente.

  > **Tip**
  >
  > Para evitar redefinir a senha de `kmsuser`, use o backup mais recente do cluster do AWS CloudHSM.

- `INTERNAL_ERROR` indica que o AWS KMS não conseguiu concluir a solicitação devido a um erro interno. Repetir a solicitação . Para solicitações `ConnectCustomKeyStore`, desconecte o armazenamento de chaves do AWS CloudHSM antes de tentar se conectar novamente.
- `INVALID_CREDENTIALS` indica que o AWS KMS não pode fazer login no cluster do AWS CloudHSM associado, pois ele não tem a senha correta da conta `kmsuser`. Para obter ajuda com relação a esse erro, consulte Como corrigir credenciais `kmsuser` inválidas.
- `NETWORK_ERRORS` geralmente indica problemas de rede temporários. Desconecte o armazenamento de chaves do AWS CloudHSM, aguarde alguns minutos e tente se conectar novamente.
- `SUBNET_NOT_FOUND` indica que pelo menos uma sub-rede na configuração do cluster do AWS CloudHSM foi excluída. Se o AWS KMS não conseguir localizar todas as sub-redes na configuração do cluster, as tentativas de conectar o armazenamento de chaves do AWS CloudHSM ao cluster do AWS CloudHSM falharão.

Para corrigir esse erro, crie um cluster de um backup recente do mesmo cluster do AWS CloudHSM. (Esse processo cria uma configuração de cluster com uma VPC e sub-redes privadas.) Verifique se o novo cluster atende aos requisitos para um armazenamento de chaves personalizado e anote o novo ID do cluster. Depois, para associar o novo cluster ao armazenamento de chaves do AWS CloudHSM, desconecte o armazenamento de chaves personalizado, altere o ID do cluster do armazenamento de chaves do AWS CloudHSM para o ID do novo cluster e tente se conectar novamente.

> **Tip**
>
> Para evitar redefinir a senha de `kmsuser`, use o backup mais recente do cluster do AWS CloudHSM.

- `USER_LOCKED_OUT` indica que a conta do usuário de criptografia (CU) `kmsuser` está bloqueada do cluster do AWS CloudHSM associado devido ao excesso de tentativas de senha com falha. Para obter ajuda com relação a esse erro, consulte Como corrigir credenciais `kmsuser` inválidas.

  Para corrigir esse erro, desconecte o armazenamento de chaves do AWS CloudHSM e use o comando changePswd no cloudhsm_mgmt_util para alterar a senha da conta `kmsuser`. Edite as configurações de senha `kmsuser` do armazenamento de chaves personalizado e tente se conectar novamente. Para obter ajuda, use o procedimento descrito no tópico Como corrigir credenciais `kmsuser` inválidas.
- `USER_LOGGED_IN` indica que a conta do CU `kmsuser` está registrada no cluster do AWS CloudHSM associado. Isso impede que o AWS KMS faça a rotação da senha da conta `kmsuser` e faça login no cluster. Para corrigir esse erro, registre o CU `kmsuser` fora do cluster. Se tiver alterado a senha do `kmsuser` para fazer login no cluster, também será necessário atualizar o valor da senha do armazenamento de chaves do AWS CloudHSM. Para obter ajuda, consulte Como fazer logout e se conectar novamente.
- `USER_NOT_FOUND` indica que o AWS KMS não consegue localizar uma conta de CU `kmsuser` no cluster do AWS CloudHSM associado. Para corrigir esse erro, crie uma conta de usuário de criptografia `kmsuser` no cluster e atualize o valor da senha do armazenamento de chaves para o armazenamento de chaves do AWS CloudHSM. Para obter ajuda, consulte Como corrigir credenciais `kmsuser` inválidas.

Como responder a uma falha de operação criptográfica

Uma operação criptográfica que usa uma chave do KMS em um armazenamento de chaves personalizado pode falhar com um `KMSInvalidStateException`. As mensagens de erro a seguir podem acompanhar o `KMSInvalidStateException`.

O KMS não pode se comunicar com seu cluster CloudHSM. Pode ser um problema de rede transitório. Caso veja esse erro repetidamente, verifique se as ACLs de rede e as regras do grupo de segurança para a VPC do cluster do AWS CloudHSM estão corretas.

- Embora este seja um erro HTTPS 400, ele pode ser resultante de problemas de rede transitórios. Para responder, comece tentando novamente a solicitação. No entanto, se o erro persistir, examine a configuração dos seus componentes de rede. O erro é causado provavelmente pela configuração incorreta de um componente de rede, como uma regra de firewall ou uma regra de grupo de segurança de VPC que está bloqueando o tráfego de saída.

O KMS não pode se comunicar com o cluster do AWS CloudHSM porque o kmsuser está bloqueado. Caso veja esse erro repetidamente, desconecte o armazenamento de chaves do AWS CloudHSM e redefina a senha da conta kmsuser. Atualize a senha do kmsuser para o armazenam ento de chaves personalizado e tente fazer a solicitação novamente.

- Essa mensagem de erro indica que a conta do usuário de criptografia (CU) `kmsuser` está bloqueada do cluster do AWS CloudHSM correspondente devido ao excesso de tentativas de senha com falha. Para obter ajuda com relação a esse erro, consulte Como desconectar e fazer login.

Como corrigir credenciais **`kmsuser`** inválidas

Quando você conecta um armazenamento de chaves do AWS CloudHSM, o AWS KMS faz login no cluster do AWS CloudHSM associado como o usuário de criptografia `kmsuser`. Ele permanece conectado até que o armazenamento de chaves do AWS CloudHSM seja desconectado. A resposta DescribeCustomKeyStores mostra um `ConnectionState` com valor `FAILED` e `ConnectionErrorCode` de `INVALID_CREDENTIALS`, conforme mostrado no exemplo a seguir.

Se você desconectar o armazenamento de chaves do AWS CloudHSM e alterar a senha do `kmsuser`, o AWS KMS não poderá fazer login no cluster do AWS CloudHSM com as credenciais da conta de usuário de critografia `kmsuser`. Como resultado, haverá falha em todas as tentativas de conexão ao armazenamento de chaves do AWS CloudHSM. A resposta `DescribeCustomKeyStores` mostra um `ConnectionState` com valor `FAILED` e `ConnectionErrorCode` de `INVALID_CREDENTIALS`, conforme mostrado no exemplo a seguir.

```
$ 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"
   ],
}
```

Além disso, após cinco tentativas malsucedidas de efetuar login no cluster com uma senha incorreta, o AWS CloudHSM bloqueia a conta do usuário. Para efetuar login no cluster, você deve alterar a senha da conta.

Se o AWS KMS obtiver uma resposta de bloqueio ao tentar efetuar login no cluster como usuário de criptografia `kmsuser`, ocorrerá uma falha na solicitação para se conectar ao armazenamento de chaves do AWS CloudHSM. A DescribeCustomKeyStoresresposta inclui um `ConnectionState` de `FAILED` e um `ConnectionErrorCode` valor de`USER_LOCKED_OUT`, conforme mostrado no exemplo a seguir.

```
$ 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"
   ],
```

```
}
```

Para corrigir qualquer uma dessas condições, use o procedimento a seguir.

1. Desconecte o armazenamento de chaves do AWS CloudHSM.
2. Execute a DescribeCustomKeyStoresoperação e visualize o valor do `ConnectionErrorCode` elemento na resposta.

   - Se o valor `ConnectionErrorCode` for `INVALID_CREDENTIALS`, determine a senha atual para a conta `kmsuser`. Se necessário, use o comando changePswd no cloudhsm_mgmt_util para definir a senha como um valor conhecido.
   - Se o valor `ConnectionErrorCode` for `USER_LOCKED_OUT`, você deve usar o comando changePswd no cloudhsm_mgmt_util para alterar a senha `kmsuser`.
3. Edite a configuração de senha `kmsuser` para corresponder à senha `kmsuser` atual no cluster. Essa ação informa ao AWS KMS a senha a ser usada para fazer login no cluster. Ela não altera a senha `kmsuser` no cluster.
4. Conectar o armazenamento de chaves personalizado

Como excluir material de chave órfã

Depois de programar a exclusão de uma chave do KMS de um armazenamento de chaves do AWS CloudHSM, pode ser necessário excluir manualmente o material de chave correspondente do cluster do AWS CloudHSM associado.

Quando você cria uma chave do KMS em um armazenamento de chaves do AWS CloudHSM, o AWS KMS cria os metadados da chave do KMS no AWS KMS e gera o material de chave no cluster do AWS CloudHSM associado. Quando você programa a exclusão de uma chave do KMS em um armazenamento de chaves do AWS CloudHSM, após o período de espera, o AWS KMS exclui os metadados da chave do KMS. O AWS KMS faz o possível para excluir o material de chaves do cluster do AWS CloudHSM. A tentativa pode falhar se o AWS KMS não puder acessar o cluster, como quando ele é desconectado do armazenamento de chaves do AWS CloudHSM ou com alterações de senha do `kmsuser`. O AWS KMS não tenta excluir o material de chave dos backups do cluster.

AWS KMS informa os resultados de sua tentativa de excluir o material de chaves do cluster na entrada de eventos `DeleteKey` do seus logs do AWS CloudTrail. Ela aparece no elemento `backingKeysDeletionStatus` do elemento `additionalEventData`, conforme mostrado na

entrada de exemplo a seguir. A entrada também inclui o ARN da chave do KMS, o ID do cluster do AWS CloudHSM e o identificador de chave do material de chave (`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"
}
```

Para excluir o material de chaves do cluster do AWS CloudHSM associado, use um procedimento semelhante ao seguinte. Esse exemplo usa as ferramentas da linha de comando da AWS CLI e do AWS CloudHSM, mas você pode usar o AWS Management Console em vez da CLI.

1. Desconecte o armazenamento de chaves do AWS CloudHSM, caso ainda não tenha sido desconectado e faça login no key_mgmt_util, conforme explicado em Como desconectar e fazer login.
2. Use o comando deleteKey no key_mgmt_util para excluir a chave dos HSMs no cluster.

   Por exemplo, esse comando exclui a chave 262162 dos HSMs no cluster. O identificador da chave está listado na entrada do 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. Encerre a sessão do key_mgmt_util e reconecte o armazenamento de chaves do AWS CloudHSM, como descrito em Como fazer logout e se conectar novamente.

Como recuperar materiais de chave excluídos de uma chave do KMS

Se o material de chave para uma AWS KMS key for excluído, a chave do KMS ficará inutilizável, e o texto cifrado que foi criptografado com ela não poderá ser descriptografado. Isso poderá acontecer se o material de chaves para uma chave do KMS em um armazenamento de chaves do AWS CloudHSM for excluído do cluster do AWS CloudHSM associado. No entanto, há a possibilidade de recuperação do material de chaves.

Quando uma AWS KMS key (chave do KMS) é criada em um armazenamento de chaves do AWS CloudHSM, o AWS KMS faz login no cluster do AWS CloudHSM associado e cria o material de chave para a chave do KMS. Ele também altera a senha para um valor que apenas ele conhece e permanecerá conectado enquanto o armazenamento de chaves do AWS CloudHSM estiver conectado. Como apenas o proprietário da chave, ou seja, o CU que criou uma chave, pode excluir a chave, é improvável que a chave seja excluída dos HSMs acidentalmente.

No entanto, se o material de chave para uma chave do KMS for excluído dos HSMs em um cluster, o estado da chave do KMS será alterado para `UNAVAILABLE`. Se você tentar usar a chave do KMS para uma operação de criptografia, ocorrerá falha na operação com uma

exceção `KMSInvalidStateException`. E, o que é mais importante, os dados que tiverem sido criptografados com a chave do KMS não poderão ser descriptografados.

Em determinadas circunstâncias, é possível recuperar o material de chaves excluído, criando um cluster a partir de um backup que contenha o material de chaves. Essa estratégia funciona somente quando pelo menos um backup foi criado enquanto a chave existia e antes de ter sido excluída.

Use o processo a seguir para recuperar o material de chaves.

1. Encontre um backup de cluster que contém o material de chaves. O backup também deve conter todos os usuários e chaves de que você precisa para oferecer suporte ao cluster e seus dados criptografados.

   Use a DescribeBackupsoperação para listar os backups de um cluster. Use o timestamp do backup para ajudá-lo a selecionar um backup. Para limitar a saída para o cluster associado ao armazenamento de chaves do AWS CloudHSM, use o parâmetro `Filters`, conforme exibido no exemplo a seguir.

   ```
   $ aws cloudhsmv2 describe-backups --filters clusterIds=<cluster ID>
   {
       "Backups": [
           {
               "ClusterId": "cluster-1a23b4cdefg",
               "BackupId": "backup-9g87f6edcba",
               "CreateTimestamp": 1536667238.328,
               "BackupState": "READY"
           },
                ...
       ]
   }
   ```

2. Crie um cluster a partir de um backup selecionado. Verifique se o backup contém a chave excluída e outros usuários e chaves que o cluster requer.
3. Desconecte o armazenamento de chaves do AWS CloudHSM para que você possa editar suas propriedades.
4. Edite o ID do cluster do armazenamento de chaves do AWS CloudHSM. Insira o ID do cluster que você criou a partir do backup. Como o cluster compartilha um histórico de backup com o cluster original, o novo ID do cluster deve ser válido.
5. Reconecte o armazenamento de chaves do AWS CloudHSM.

Como fazer login como **kmsuser**

Para criar e gerenciar o material de chaves no cluster do AWS CloudHSM para o armazenamento de chaves do AWS CloudHSM, o AWS KMS usa a conta de usuário de criptografia kmsuser. Você cria a conta de usuário de criptografia kmsuser no cluster e fornece sua senha para o AWS KMS ao criar seu armazenamento de chaves do AWS CloudHSM.

Em geral, o AWS KMS gerencia a conta kmsuser. No entanto, para algumas tarefas, você precisa desconectar o armazenamento de chaves do AWS CloudHSM, fazer login no cluster como usuário de criptografia kmsuser e usar as ferramentas da linha de comando cloudhsm_mgmt_util e key_mgmt_util.

> **Note**
>
> Enquanto um armazenamento de chaves personalizado estiver desconectado, todas as tentativas de criar chaves do KMS nele ou de usar chaves do KMS existentes em operações de criptografia falharão. Essa ação pode impedir que os usuários armazenem e acessem dados sigilosos.

Este tópico explica como desconectar o armazenamento de chaves do AWS CloudHSM e fazer login como kmsuser, executar a ferramenta da linha de comando do AWS CloudHSM e desconectar e reconectar seu armazenamento de chaves do AWS CloudHSM.

Tópicos

- Como desconectar e fazer login
- Como fazer logout e se conectar novamente

Como desconectar e fazer login

Use o procedimento a seguir sempre que precisar fazer login em um cluster associado como CU kmsuser.

1. Desconecte o armazenamento de chaves do AWS CloudHSM, caso ele ainda não tenha sido desconectado. É possível usar o console do AWS KMS ou a API do AWS KMS.

   Enquanto a chave do AWS CloudHSM estiver conectada, o AWS KMS estará conectado como kmsuser. Isso evita que você faça login como kmsuser ou altere a senha kmsuser.

Por exemplo, esse comando é usado DisconnectCustomKeyStorepara desconectar um exemplo de armazenamento de chaves. Substitua o ID de exemplo do armazenamento de chaves do AWS CloudHSM por um ID válido.

```
$ aws kms disconnect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

2. Iniciar cloudhsm_mgmt_util. Use o procedimento descrito na seção Preparar para executar cloudhsm_mgmt_util do Manual do usuário do AWS CloudHSM.
3. Faça login no cloudhsm_mgmt_util no cluster do AWS CloudHSM como responsável pela criptografia (CO).

   Por exemplo, este comando efetua login como um CO chamado admin. Substitua o nome de usuário e a senha do CO de exemplo por valores válidos.

   ```
   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. Use o comando changePswd para alterar a senha da conta `kmsuser` para a senha de sua preferência. (O AWS KMS altera a senha quando você se conecta ao armazenamento de chaves do AWS CloudHSM.) A senha deve conter de 7 a 32 caracteres alfanuméricos. Ela diferencia maiúsculas de minúsculas e não pode conter caracteres especiais.

   Por exemplo, este comando altera a senha `kmsuser` para `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. Faça login no key_mgmt_util ou cloudhsm_mgmt_util como `kmsuser` usando a senha que você definir. Para obter instruções detalhadas, consulte Conceitos básicos cloudhsm_mgmt_util e Conceitos básicos key_mgmt_util. A ferramenta que você usa depende da sua tarefa.

   Por exemplo, este comando faz login em 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
```

Como fazer logout e se conectar novamente

1. Execute a tarefa e faça logout da ferramenta da linha de comando. Se você não fizer logout, ocorrerá falha nas tentativas de se reconectar ao armazenamento de chaves do AWS CloudHSM.

```
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. Edite a configuração de senha `kmsuser` para o armazenamento de chaves personalizado.

   Esse procedimento informa ao AWS KMS a senha atual do `kmsuser` no cluster. Se você pular essa etapa, o AWS KMS não poderá fazer login no cluster como `kmsuser`, e ocorrerá falha em todas as tentativas de reconectá-lo ao armazenamento de chaves personalizado. Você pode usar o AWS KMS console ou o `KeyStorePassword` parâmetro da UpdateCustomKeyStoreoperação.

   Por exemplo, este comando informa ao AWS KMS que a senha atual é `tempPassword`. Substitua a senha de exemplo pela real.

```
$ aws kms update-custom-key-store --custom-key-store-id cks-1234567890abcdef0 --
key-store-password tempPassword
```

3. Reconectar o armazenamento de chaves do AWS KMS ao cluster do AWS CloudHSM. Substitua o ID de exemplo do armazenamento de chaves do AWS CloudHSM por um ID válido. Durante o processo de conexão, o AWS KMS altera a senha `kmsuser` para um valor que apenas ele conhece.

   A ConnectCustomKeyStoreoperação retorna rapidamente, mas o processo de conexão pode levar um longo período de tempo. A resposta inicial não indica o sucesso do processo de conexão.

   ```
   $ aws kms connect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
   ```

4. Use a DescribeCustomKeyStoresoperação para verificar se o armazenamento de AWS CloudHSM chaves está conectado. Substitua o ID de exemplo do armazenamento de chaves do AWS CloudHSM por um ID válido.

   Neste exemplo, o campo de estado da conexão mostra que agora o armazenamento de chaves do AWS CloudHSM está conectado.

   ```
   $ 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"
      ],
   }
   ```

Armazenamentos de chaves externas

Os armazenamentos externos de chaves permitem que você proteja seus AWS recursos usando chaves criptográficas externas. AWS Esse recurso avançado foi criado para workloads regulamentadas que você precisa proteger com chaves de criptografia armazenadas em um sistema

de gerenciamento de chaves externas que você controla. Os armazenamentos externos de chaves apoiam o compromisso de soberania AWS digital de dar a você controle soberano sobre seus dados AWS, incluindo a capacidade de criptografar com material chave que você possui e controla externamente. AWS

Um armazenamento de chaves externo é um armazenamento de chaves personalizado apoiado por um gerenciador de chaves externo que você possui e gerencia fora dele AWS. Seu gerenciador de chaves externas pode ser um módulo de segurança de hardware (HSMs) físico ou virtual ou qualquer sistema baseado em hardware ou software capaz de gerar e usar chaves de criptografia. As operações de criptografia e descriptografia que usam uma chave do KMS em um armazenamento de chaves externas são realizadas pelo gerenciador de chaves externas usando seu material de chave de criptografia, um recurso conhecido como hold your own keys (HYOKs).

AWS KMS nunca interage diretamente com seu gerenciador de chaves externo e não pode criar, visualizar, gerenciar ou excluir suas chaves. Em vez disso, AWS KMS interage somente com o software proxy externo de armazenamento de chaves (proxy XKS) fornecido por você. Seu proxy externo de armazenamento de chaves medeia toda a comunicação entre AWS KMS e seu gerenciador de chaves externo. Ele transmite todas as solicitações AWS KMS para o seu gerenciador de chaves externo e transmite as respostas do seu gerenciador de chaves externo de volta para o. AWS KMS O proxy externo do armazenamento de chaves também traduz solicitações genéricas AWS KMS em um formato específico do fornecedor que seu gerente de chaves externo possa entender, permitindo que você use armazenamentos de chaves externos com gerenciadores de chaves de vários fornecedores.

Você pode usar chaves do KMS em um armazenamento de chaves externas para criptografia do lado do cliente, inclusive com o AWS Encryption SDK. Mas os armazenamentos externos de chaves são um recurso importante para a criptografia do lado do servidor, permitindo que você proteja seus AWS recursos de forma múltipla Serviços da AWS com suas chaves criptográficas externas. AWS Serviços da AWS que oferecem suporte a chaves gerenciadas pelo cliente para criptografia simétrica também oferecem suporte a chaves KMS em um armazenamento de chaves externo. Para obter detalhes sobre o suporte para serviços, consulte AWS Service Integration (Integração de produtos da).

Os armazenamentos externos de chaves permitem que você use AWS KMS para cargas de trabalho regulamentadas, nas quais as chaves de criptografia devem ser armazenadas e usadas fora do AWS. Mas eles são um grande desvio do modelo de responsabilidade compartilhada padrão e exigem o aumento dos encargos operacionais. O maior risco de disponibilidade e latência excederá,

para a maioria dos clientes, os benefícios de segurança percebidos pelos armazenamentos de chaves externas.

Os armazenamentos de chaves externas permitem controlar a raiz de confiança. Os dados criptografados sob chaves do KMS em seu armazenamento de chaves externas só podem ser descriptografados usando o gerenciador de chaves externas que você controla. Se você revogar temporariamente o acesso ao seu gerenciador de chaves externo, por exemplo, desconectando o armazenamento de chaves externo ou desconectando o gerenciador de chaves externo do proxy externo do armazenamento de chaves, AWS perderá todo o acesso às suas chaves criptográficas até que você as restaure. Durante esse intervalo, o texto cifrado criptografado sob suas chaves do KMS não poderá ser descriptografado. Se você revogar permanentemente o acesso ao seu gerenciador de chaves externas, todo o texto cifrado criptografado sob uma chave do KMS em seu armazenamento de chaves externas vai se tornar irrecuperável. As únicas exceções são AWS serviços que armazenam brevemente em cache as chaves de dados protegidas por suas chaves KMS. Essas chaves de dados continuarão funcionando até você desativar o recurso ou o cache expirar. Para obter detalhes, consulte Como as chaves do KMS inutilizáveis afetam as chaves de dados.

Os armazenamentos externos de chaves desbloqueiam os poucos casos de uso de cargas de trabalho regulamentadas em que as chaves de criptografia devem permanecer exclusivamente sob seu controle e inacessíveis. AWS Porém, esta é uma grande mudança na forma como você opera a infraestrutura baseada em nuvem e uma alteração significativa no modelo de responsabilidade compartilhada. Para a maioria das workloads, o aumento da carga operacional e os maiores riscos de disponibilidade e performance excederão os benefícios de segurança percebidos pelos armazenamentos de chaves externas.

Saiba mais:

- Announcing AWS KMS External Key Store (Anúncio do armazenamento de chaves externas do) no blog de notícias da AWS .

Preciso de armazenamento de chaves externas?

Para a maioria dos usuários, o armazenamento de AWS KMS chaves padrão, protegido pelos módulos de segurança de hardware validados pelo FIPS 140-2 Security Level 3, atende aos requisitos regulatórios, de controle e de segurança. Usuários do armazenamento de chaves externas

incorrem em custos consideráveis, sobrecarga de manutenção e solução de problemas, além de riscos de latência, disponibilidade e confiabilidade.

Ao considerar um armazenamento de chaves externas, dedique algum tempo para entender as alternativas, como um armazenamento de chaves do AWS CloudHSM baseado em um cluster do AWS CloudHSM que você possui e gerencia e chaves do KMS com material de chave importado que você gera em seus próprios HSMs e pode excluir das chaves do KMS sob demanda. Especificamente, importar material de chave com um intervalo de expiração muito curto pode fornecer um nível similar de controle sem riscos à performance ou à disponibilidade.

Um armazenamento de chaves externas pode ser a solução certa para sua organização, caso cumpra os seguintes requisitos:

- Você precisa usar chaves criptográficas em seu gerenciador de chaves local ou em um gerenciador de chaves fora do seu AWS controle.
- É necessário demonstrar que suas chaves de criptografia são retidas somente sob seu controle fora da nuvem.
- É necessário criptografar e descriptografar usando chaves de criptografia com autorização independente.
- O material de chaves deve estar sujeito a um caminho de auditoria secundário e independente.

Se escolher um armazenamento de chaves externas, limite o uso a workloads que necessitam de proteção com chaves de criptografia fora da AWS.

Modelo de responsabilidade compartilhada

As chaves KMS padrão usam material de chaves que é gerado e usado em HSMs que AWS KMS possuem e gerenciam. Você estabelece as políticas de controle de acesso em suas chaves KMS e configura Serviços da AWS que usem chaves KMS para proteger seus recursos. AWS KMS assume a responsabilidade pela segurança, disponibilidade, latência e durabilidade do material de chaves em suas chaves KMS.

As chaves do KMS em armazenamentos de chaves externas dependem do material e das operações do gerenciador de chaves externas. Assim, o equilíbrio de responsabilidades desloca-se em direção a você. Você é responsável pela segurança, confiabilidade, durabilidade e desempenho das chaves criptográficas em seu gerenciador de chaves externo. AWS KMS é responsável por responder prontamente às solicitações e se comunicar com seu proxy externo de armazenamento de chaves

e por manter nossos padrões de segurança. Para garantir que cada chave externa armazene texto cifrado pelo menos tão forte quanto o texto AWS KMS cifrado padrão, AWS KMS primeiro criptografa todo o texto sem formatação com material de chave específico da sua AWS KMS chave KMS e, em seguida, o envia ao seu gerenciador de chaves externo para criptografia com sua chave externa, um procedimento conhecido como criptografia dupla. Como resultado, nem o AWS KMS nem o proprietário do material de chave externa podem descriptografar somente o texto cifrado com criptografia dupla.

Você é responsável por manter um gerenciador de chaves externas que atenda aos seus padrões regulatórios e de performance, por fornecer e manter um proxy de armazenamento de chaves externas que esteja em conformidade com a AWS KMS External Key Store Proxy API Specification (Especificação da API do proxy de armazenamento de chaves externas do) e por garantir a disponibilidade e durabilidade do material de chave. Você também deve criar, configurar e manter um armazenamento de chaves externas. Quando surgem erros causados por componentes que você mantém, você deve estar preparado para identificar e resolver os erros para que os AWS serviços possam acessar seus recursos sem interrupções indevidas. AWS KMS fornece orientação de solução de problemas para ajudá-lo a determinar a causa dos problemas e as resoluções mais prováveis.

Analise as CloudWatch métricas e dimensões da Amazon que AWS KMS registram para lojas de chaves externas. AWS KMS recomenda fortemente que você crie CloudWatch alarmes para monitorar seu armazenamento externo de chaves para que você possa detectar os primeiros sinais de problemas operacionais e de desempenho antes que eles ocorram.

O que está mudando?

Armazenamentos de chaves externas são compatíveis apenas com chaves do KMS de criptografia simétrica. Dentro AWS KMS, você usa e gerencia as chaves KMS em um armazenamento de chaves externo da mesma forma que gerencia outras chaves gerenciadas pelo cliente, incluindo a definição de políticas de controle de acesso e o monitoramento do uso da chave. Utilize as mesmas APIs com os mesmos parâmetros para solicitar uma operação de criptografia com uma chave do KMS em um armazenamento de chaves externas que você usa para qualquer chave do KMS. O preço também é o mesmo das chaves do KMS padrão. Para obter mais detalhes, consulte Gerenciar chaves do KMS em um armazenamento de chaves externas, Usar chaves do KMS em um armazenamento de chaves externas e AWS Key Management Service Pricing (Preço do).

Porém, com os armazenamentos de chaves externas, os seguintes princípios mudam:

- Você é responsável pela disponibilidade, durabilidade e latência das operações de chaves.

- Você é responsável por todos os custos de desenvolvimento, compra, operação e licenciamento de seu sistema de gerenciamento de chaves externas.
- Você pode implementar a autorização independente de todas as solicitações AWS KMS de seu proxy externo de armazenamento de chaves.
- Você pode monitorar, auditar e registrar todas as operações do proxy externo do armazenamento de chaves e todas as operações do gerenciador de chaves externo relacionadas às AWS KMS solicitações.

Por onde começar?

Para criar e gerenciar um armazenamento de chaves externas, é necessário escolher sua opção de conectividade de proxy de armazenamento de chaves externas, organizar os pré-requisitos e criar e configurar o armazenamento de chaves externas. Para começar, consulte Planejar um armazenamento de chaves externas.

Cotas

AWS KMS permite até 10 armazenamentos de chaves personalizadas em cada Conta da AWS região, incluindo armazenamentos de AWS CloudHSM chaves e armazenamentos de chaves externos, independentemente do estado da conexão. Além disso, há cotas de solicitação do AWS KMS para o uso de chaves do KMS em um armazenamento de chaves externas.

Se você escolher a conectividade de proxy da VPC para seu proxy de armazenamento de chaves externas, também poderá haver cotas nos componentes obrigatórios, como VPCs, sub-redes e balanceadores de carga de rede. Para obter mais informações sobre essas cotas, use o console do Service Quotas.

Regiões

Para minimizar a latência da rede, crie seus componentes de armazenamento de chaves externas na Região da AWS mais próxima do gerenciador de chaves externas. Se possível, escolha uma região com um tempo de resposta (RTT) de 35 milissegundos ou menos.

Os armazenamentos de chaves externos são suportados Regiões da AWS em todas as regiões AWS KMS com suporte, exceto na China (Pequim) e na China (Ningxia).

Recursos sem suporte

AWS KMS não oferece suporte aos seguintes recursos em armazenamentos de chaves personalizadas.

- Chaves do KMS assimétricas
- Pares de chaves de dados assimétricas
- Chaves do KMS de HMAC
- Chaves do KMS com material de chave importado
- Alternância automática de chaves
- Chaves de várias regiões

Tópicos

- Conceitos de armazenamento de chaves externas
- Como funcionam os armazenamentos de chaves externas
- Controlar o acesso ao armazenamento de chaves externas
- Planejar um armazenamento de chaves externas
- Gerenciar um armazenamento de chaves externas
- Gerenciar chaves do KMS em um armazenamento de chaves externas
- Solução de problemas de armazenamentos de chaves externas

Conceitos de armazenamento de chaves externas

Este tópico explica alguns dos conceitos usados nos armazenamentos de chaves externas.

Tópicos

- Armazenamento de chaves externas
- Gerenciador de chaves externas
- Chave externa
- Proxy de armazenamento de chaves externas
- Conectividade de proxy de armazenamento de chaves externas
- Credencial de autenticação de proxy de armazenamento de chaves externas
- APIs de proxy
- Criptografia dupla

Armazenamento de chaves externas

Um armazenamento de chaves externo é um armazenamento de chaves AWS KMS personalizado apoiado por um gerenciador de chaves externo fora do AWS que você possui e gerencia. Cada chave do KMS em um armazenamento de chaves externas está associada a uma chave externa de seu gerenciador de chaves externas. Quando você usa uma chave do KMS em um armazenamento de chaves externas para criptografia ou descriptografia, a operação é executada pelo gerenciador de chaves externas usando sua chave externa, um mecanismo conhecido como mantenha sua própria chave (HYOK). Esse recurso foi desenvolvido para organizações que precisam manter chaves de criptografia em seu próprio gerenciador de chaves externas.

Os armazenamentos externos de chaves garantem que as chaves criptográficas e as operações que protegem seus AWS recursos permaneçam sob seu controle no gerenciador de chaves externo. AWS KMS envia solicitações ao seu gerenciador de chaves externo para criptografar e descriptografar dados, mas AWS KMS não pode criar, excluir ou gerenciar nenhuma chave externa. Todas as solicitações do AWS KMS seu gerenciador de chaves externo são mediadas por um componente de software proxy de armazenamento de chaves externo que você fornece, possui e gerencia.

AWS os serviços que oferecem suporte a chaves gerenciadas pelo AWS KMS cliente podem usar as chaves KMS em seu armazenamento de chaves externo para proteger seus dados. Como resultado, seus dados são, em última análise, protegidos por suas chaves usando suas operações de criptografia no gerenciador de chaves externas.

As chaves do KMS em um armazenamento de chaves externas têm modelos de confiança, acordos de responsabilidade compartilhada e expectativas de performance consideravelmente diferentes das chaves do KMS padrão. Com armazenamentos de chaves externas, você é responsável pela segurança e integridade do material de chave e pelas operações de criptografia. A disponibilidade e a latência das chaves do KMS em um armazenamento de chaves externas são afetadas pelo hardware, software, componentes de redes e pela distância entre o AWS KMS e o gerenciador de chaves externas. Também é provável que você incorra em custos adicionais com seu gerenciador de chaves externo e com a infraestrutura de rede e balanceamento de carga com a qual seu gerenciador de chaves externo se comunique. AWS KMS

Você pode usar seu armazenamento de chaves externas como parte de sua estratégia geral de proteção de dados. Para cada AWS recurso que você protege, você pode decidir qual requer uma chave KMS em um armazenamento de chaves externo e qual pode ser protegido por uma chave KMS padrão. Isso lhe dá a flexibilidade para escolher chaves do KMS para classificações de dados, aplicações ou projetos específicos.

Gerenciador de chaves externas

Um gerenciador de chaves externas é um componente fora da AWS que pode gerar chaves simétricas AES de 256 bits e realizar criptografia e descriptografia simétricas. O gerenciador de chaves externas para um armazenamento de chaves externas pode ser um módulo de segurança de hardware (HSM) físico, um HSM virtual ou um gerenciador de chaves de software com ou sem um componente HSM. Ele pode estar localizado em qualquer lugar externo AWS, inclusive em suas instalações, em um data center local ou remoto ou em qualquer nuvem. O armazenamento de chaves externas pode basear-se em um único gerenciador de chaves externas ou em várias instâncias de gerenciador de chaves relacionadas que compartilham chaves de criptografia, como um cluster do HSM. Os armazenamentos de chaves externas são criados para oferecer suporte a uma variedade de gerenciadores externos de diferentes fornecedores. Para obter detalhes sobre os requisitos do seu gerenciador de chaves externas, consulte Planejar um armazenamento de chaves externas.

Chave externa

Cada chave do KMS em um armazenamento de chaves externas está associada a uma chave de criptografia do gerenciador de chaves externas conhecida como chave externa. Ao criptografar ou descriptografar com uma chave do KMS no armazenamento de chaves externas, a operação de criptografia é executada pelo gerenciador de chaves externas usando suas chaves externas.

> **Warning**
>
> A chave externa é essencial para a operação da chave do KMS. Se a chave externa for perdida ou excluída, o texto cifrado criptografado sob a chave do KMS associada vai se tornar irrecuperável.

Para armazenamentos de chaves externas, a chave externa deve ser uma chave AES de 256 bits que esteja habilitada e possa executar criptografia e descriptografia. Para obter requisitos detalhados de chaves externas, consulte Requisitos para uma chave do KMS em um armazenamento de chaves externas.

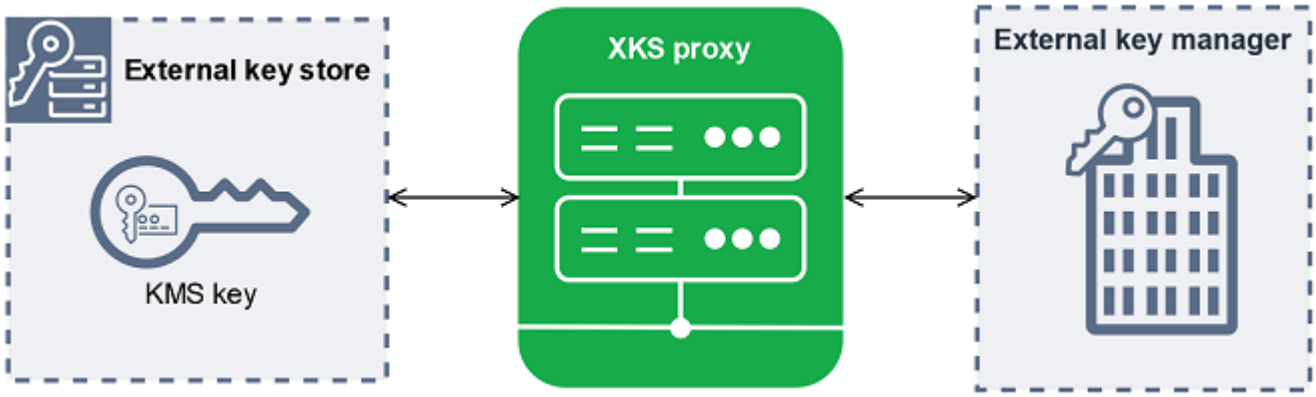
AWS KMS não pode criar, excluir ou gerenciar nenhuma chave externa. O material de chave de criptografia nunca sai do gerenciador de chaves externas. Ao criar uma chave do KMS em um armazenamento de chaves externas, você fornece o ID de uma chave externa (`XksKeyId`). Você não pode alterar o ID da chave externa associada a uma chave do KMS, embora seu gerenciador de chaves externas possa alternar o material de chave associado ao ID da chave externa.

Além da chave externa, uma chave do KMS em um armazenamento de chaves externas também tem material de chave do AWS KMS . Os dados protegidos pela chave KMS são criptografados primeiro AWS KMS usando o material de AWS KMS chaves e, em seguida, pelo gerenciador de chaves externo usando sua chave externa. Esse processo de criptografia dupla garante que o texto cifrado protegido pela chave do KMS seja sempre pelo menos tão forte quanto o texto cifrado protegido somente pelo AWS KMS.

Muitas chaves de criptografia têm diferentes tipos de identificadores. Ao criar uma chave do KMS em um armazenamento de chaves externas, forneça o ID da chave externa que o proxy de armazenamento de chaves externas usa para se referir à chave externa. Se você usar o identificador errado, haverá falha na tentativa de criar uma chave do KMS em seu armazenamento de chaves externas.

Proxy de armazenamento de chaves externas

O proxy externo de armazenamento de chaves (“proxy XKS”) é um aplicativo de software de propriedade e gerenciamento do cliente que medeia toda a comunicação entre AWS KMS e seu gerenciador de chaves externo. Ele também traduz AWS KMS solicitações genéricas em um formato que seu gerente de chaves externo específico do fornecedor entenda. É necessário um proxy de armazenamento de chaves externas para um armazenamento de chaves externas. Cada armazenamento de chaves externas é associado a um proxy de armazenamento de chaves externas.



AWS KMS não pode criar, excluir ou gerenciar nenhuma chave externa. O material de chave de criptografia nunca sai do gerenciador de chaves externas. Toda a comunicação entre AWS KMS e seu gerenciador de chaves externo é mediada pelo proxy externo do armazenamento de chaves. AWS KMS envia solicitações para o proxy externo do armazenamento de chaves e recebe respostas do proxy externo do armazenamento de chaves. O proxy externo do armazenamento de chaves é

responsável por transmitir solicitações de AWS KMS seu gerenciador de chaves externo e transmitir respostas de seu gerenciador de chaves externo de volta para AWS KMS

Você possui e gerencia o proxy de armazenamento de chaves externas para seu armazenamento de chaves externas e é responsável por sua manutenção e operação. Você pode desenvolver seu proxy de armazenamento de chaves externo com base na especificação da API de proxy de armazenamento de chaves externo de código aberto que AWS KMS publica ou compra um aplicativo proxy de um fornecedor. Seu proxy de armazenamento de chaves externas pode estar incluído em seu gerenciador de chaves externas. Para oferecer suporte ao desenvolvimento de proxy, AWS KMS também fornece um exemplo de proxy de armazenamento de chaves externo (aws-kms-xks-proxy) e um cliente de teste (xks-kms-xksproxy-test-client) que verifica se o proxy do armazenamento de chaves externo está em conformidade com a especificação.

Para se autenticar AWS KMS, o proxy usa certificados TLS do lado do servidor. Para se autenticar em seu proxy, AWS KMS assina todas as solicitações em seu proxy externo de armazenamento de chaves com uma credencial de autenticação de proxy SigV4. Opcionalmente, seu proxy pode habilitar o TLS mútuo (mTLS) para garantir que ele só aceita solicitações de. AWS KMS

O proxy externo de armazenamento de chaves deve oferecer suporte a HTTP/1.1 ou posterior e TLS 1.2 ou posterior com pelo menos um dos seguintes conjuntos de criptografia:

- TLS_AES_256_GCM_SHA384 (TLS 1.3)
- TLS_CHACHA20_POLY1305_SHA256 (TLS 1.3)

> **Note**
>
> O AWS GovCloud (US) Region não suporta 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)

Para criar e usar as chaves do KMS em seu armazenamento de chaves externas, você deve primeiro conectar o armazenamento de chaves externas ao proxy de armazenamento de chaves externas. Você também pode desconectar o armazenamento de chaves externas do proxy sob demanda. Quando você faz isso, todas as chaves do KMS no armazenamento de chaves externas ficam indisponíveis e não podem ser usadas em nenhuma operação de criptografia.

Conectividade de proxy de armazenamento de chaves externas

A conectividade de proxy de armazenamento de chaves externo (“conectividade de proxy XKS”) descreve o método AWS KMS usado para se comunicar com seu proxy de armazenamento de chaves externo.

Você especifica sua opção de conectividade de proxy ao criar o armazenamento de chaves externas, e ela se torna uma propriedade do armazenamento de chaves externas. Você pode alterar sua opção de conectividade de proxy atualizando a propriedade do armazenamento de chaves personalizado, mas você deve ter certeza de que o proxy de armazenamento de chaves externas ainda pode acessar as mesmas chaves externas.

AWS KMS suporta as seguintes opções de conectividade:

- Conectividade de endpoint público — AWS KMS envia solicitações para seu proxy externo de armazenamento de chaves pela Internet para um endpoint público que você controla. Essa opção é simples de criar e manter, mas talvez não atenda aos requisitos de segurança de todas as instalações.
- Conectividade do serviço de endpoint VPC — AWS KMS envia solicitações para um serviço de endpoint da Amazon Virtual Private Cloud (Amazon VPC) que você cria e mantém. Você pode hospedar seu proxy externo de armazenamento de chaves dentro de sua Amazon VPC ou hospedar seu proxy externo de armazenamento de chaves fora AWS e usar a Amazon VPC somente para comunicação.

Para obter detalhes sobre as opções de conectividade de proxy de armazenamento de chaves externas, consulte Escolher uma opção de conectividade do proxy.

Credencial de autenticação de proxy de armazenamento de chaves externas

Para se autenticar no proxy externo do armazenamento de chaves, AWS KMS assine todas as solicitações no proxy externo do armazenamento de chaves com uma credencial de autenticação Signature V4 (SigV4). Você estabelece e mantém a credencial de autenticação em seu proxy e, em seguida, fornece essa credencial AWS KMS ao criar seu armazenamento externo.

> **Note**
>
> A credencial SigV4 AWS KMS usada para assinar solicitações ao proxy XKS não está relacionada a nenhuma credencial SigV4 associada aos diretores em seu. AWS Identity and

Access Management Contas da AWS Não reutilize nenhuma credencial SigV4 do IAM para seu proxy de armazenamento de chaves externas.

Toda credencial de autenticação do proxy tem duas partes. É necessário fornecer as duas partes ao criar um armazenamento de chaves externas ou atualizar a credencial de autenticação do armazenamento de chaves externas.

- ID da chave de acesso: identifica a chave de acesso secreta. Você pode fornecer esse ID em texto não criptografado.
- Chave de acesso secreta: a parte secreta da credencial. AWS KMS criptografa a chave de acesso secreta na credencial antes de armazená-la.

Você pode editar a configuração da credencial a qualquer momento, como ao inserir valores incorretos, ao alterar a credencial no proxy ou quando seu proxy alterna a credencial. Para obter detalhes técnicos sobre a AWS KMS autenticação no proxy externo do armazenamento de chaves, consulte Autenticação na Especificação da API AWS KMS External Key Store Proxy.

Para permitir que você alterne sua credencial sem interromper o Serviços da AWS uso de chaves KMS em seu armazenamento de chaves externo, recomendamos que o proxy do armazenamento de chaves externo suporte pelo menos duas credenciais de autenticação válidas para. AWS KMS Isso garante que sua credencial anterior continue funcionando enquanto você fornece sua nova credencial para o AWS KMS.

Para ajudá-lo a rastrear a idade da sua credencial de autenticação de proxy, AWS KMS define uma CloudWatch métrica da Amazon, XksProxyCredentialAge. Você pode usar essa métrica para criar um CloudWatch alarme que o notifique quando a idade da sua credencial atingir um limite estabelecido por você.

Para fornecer uma garantia adicional de que seu proxy de armazenamento de chaves externas responde somente ao AWS KMS, alguns proxies de chaves externas oferecem suporte à Transport Layer Security mútua (mTLS). Para obter detalhes, consulte Autenticação mTLS (opcional).

APIs de proxy

Para oferecer suporte a um armazenamento de chaves AWS KMS externo, um proxy externo de armazenamento de chaves deve implementar as APIs de proxy necessárias, conforme descrito na Especificação da API de proxy de armazenamento de chaves AWS KMS externo. Essas solicitações de API de proxy são as únicas solicitações AWS KMS enviadas ao proxy. Embora você nunca envie

essas solicitações diretamente, conhecê-las pode ajudar a corrigir problemas que possam surgir no armazenamento de chaves externas ou no proxy. Por exemplo, AWS KMS inclui informações sobre a latência e as taxas de sucesso dessas chamadas de API em suas CloudWatch métricas da Amazon para lojas de chaves externas. Para obter detalhes, consulte Monitorar um armazenamento de chaves externas.

A tabela a seguir lista e descreve cada API de proxy. Também inclui as AWS KMS operações que acionam uma chamada para a API proxy e quaisquer exceções de AWS KMS operação relacionadas à API proxy.

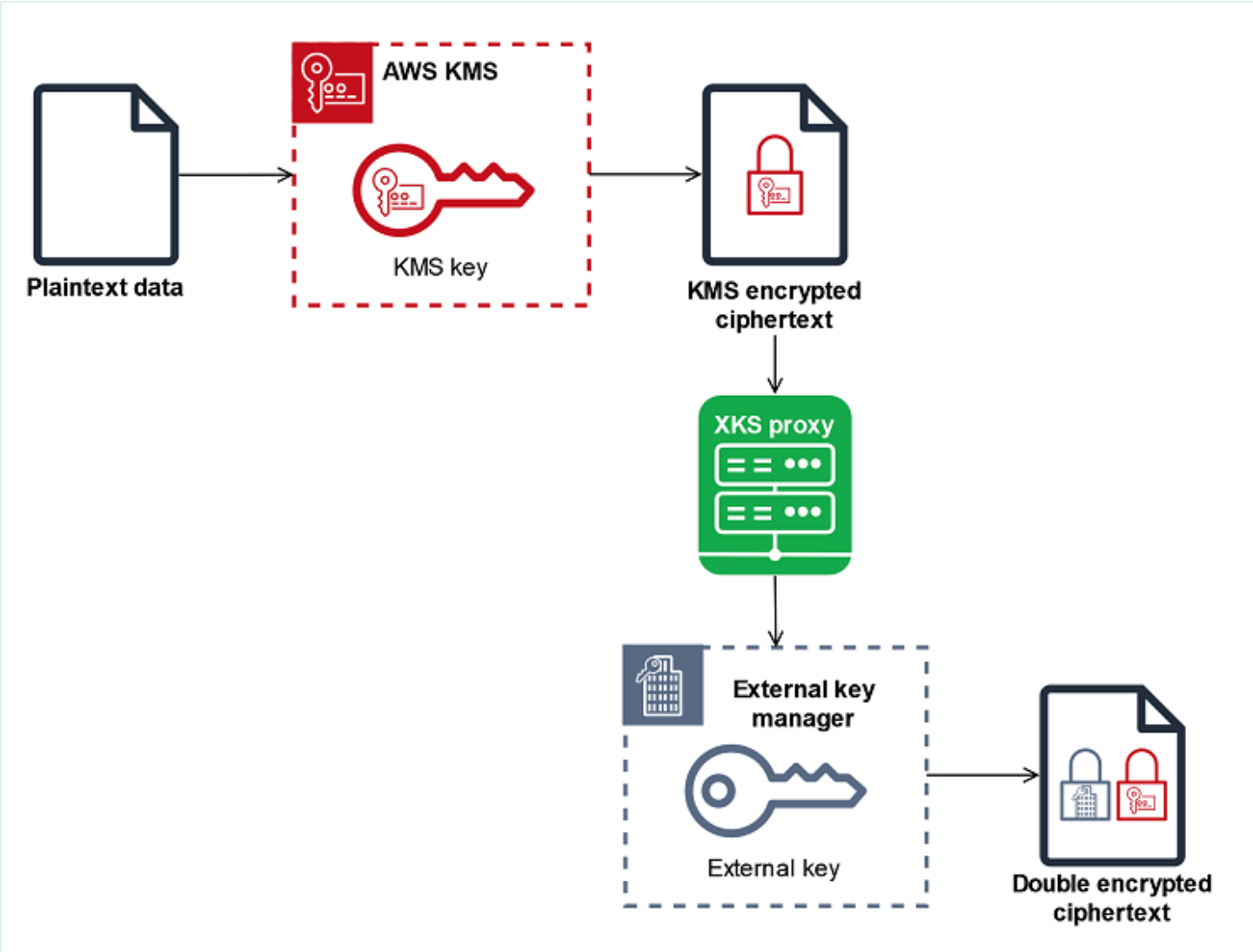
API de proxy	Descrição	AWS KMS Operações relacionadas
Decrypt	AWS KMS envia o texto cifrado a ser descriptografado e o ID da chave externa a ser usada. O algoritmo de criptografia obrigatório é AES_GCM.	Descriptografar, ReEncrypt
Encrypt	AWS KMS envia dados para serem criptografados e o ID da chave externa a ser usada. O algoritmo de criptografia obrigatório é AES_GCM.	Criptografar,, GenerateDataKey, GenerateDataKeyWithoutPlaintextReEncrypt
GetHealthStatus	AWS KMS solicita informações sobre o status do proxy e do seu gerenciador de chaves externo. Cada gerenciador de chaves externas pode ter um dos status a seguir. • `Active`: íntegro; pode atender ao tráfego • `Degraded`: não íntegro, mas pode atender ao tráfego • `Unavailable` : não íntegro; não pode atender ao tráfego	CreateCustomKeyStore(para conectividade de endpoint público), ConnectCustomKeyStore(para conectividade de serviço de endpoint VPC) Se todas as instâncias do gerenciador de chaves externas tiverem o status `Unavailable` , as tentativas de criar ou conectar o armazenamento de chaves falharão com `XksProxyUriUnreachableException` .
GetKeyMetadata	AWS KMS solicita informações sobre a chave externa associada a uma	CreateKey

API de proxy	Descrição	AWS KMS Operações relacionadas
	chave KMS em seu armazenamento de chaves externo. A resposta inclui a especificação da chave (`AES_256`), o uso da chave (`[ENCRYPT, DECRYPT]`) e se a chave externa está `ENABLED` ou `DISABLED`.	Se a especificação da chave não for `AES_256`, se o uso da chave não for `[ENCRYPT, DECRYPT]` ou se o status for `DISABLED`, a operação `CreateKey` falhará com `XksKeyInvalidConfigurationException` .

Criptografia dupla

Os dados criptografados por uma chave do KMS em um armazenamento de chaves externas são criptografados duas vezes. Primeiro, AWS KMS criptografa os dados com material de AWS KMS chave específico da chave KMS. Em seguida, o texto cifrado criptografado pelo AWS KMSé criptografado pelo gerenciador de chaves externas usando sua chave externa. O processo é conhecido como criptografia dupla.

A criptografia dupla garante que os dados criptografados por uma chave do KMS em um armazenamento de chaves externas sejam pelo menos tão fortes quanto o texto cifrado criptografado por uma chave do KMS padrão. Ele também protege o texto simples em trânsito do proxy externo do AWS KMS armazenamento de chaves. Com a criptografia dupla, você mantém o controle total de seus textos cifrados. Se você revogar permanentemente o acesso da AWS à sua chave externa por meio do proxy externo, todo texto cifrado da AWS restante será efetivamente destruído por criptografia.



Para habilitar a criptografia dupla, cada chave do KMS em um armazenamento de chaves externas tem duas chaves de reserva de criptografia:

- Um material de AWS KMS chave exclusivo da chave KMS. Esse material de chave é gerado e usado somente em módulos de segurança de hardware (HSMs) certificados pelo AWS KMS FIPS 140-2 Security Level 3.
- Uma chave externa em seu gerenciador de chaves externas.

A criptografia dupla tem os seguintes efeitos:

- AWS KMS não pode descriptografar nenhum texto cifrado criptografado por uma chave KMS em um armazenamento de chaves externo sem acessar suas chaves externas por meio do proxy externo do armazenamento de chaves.

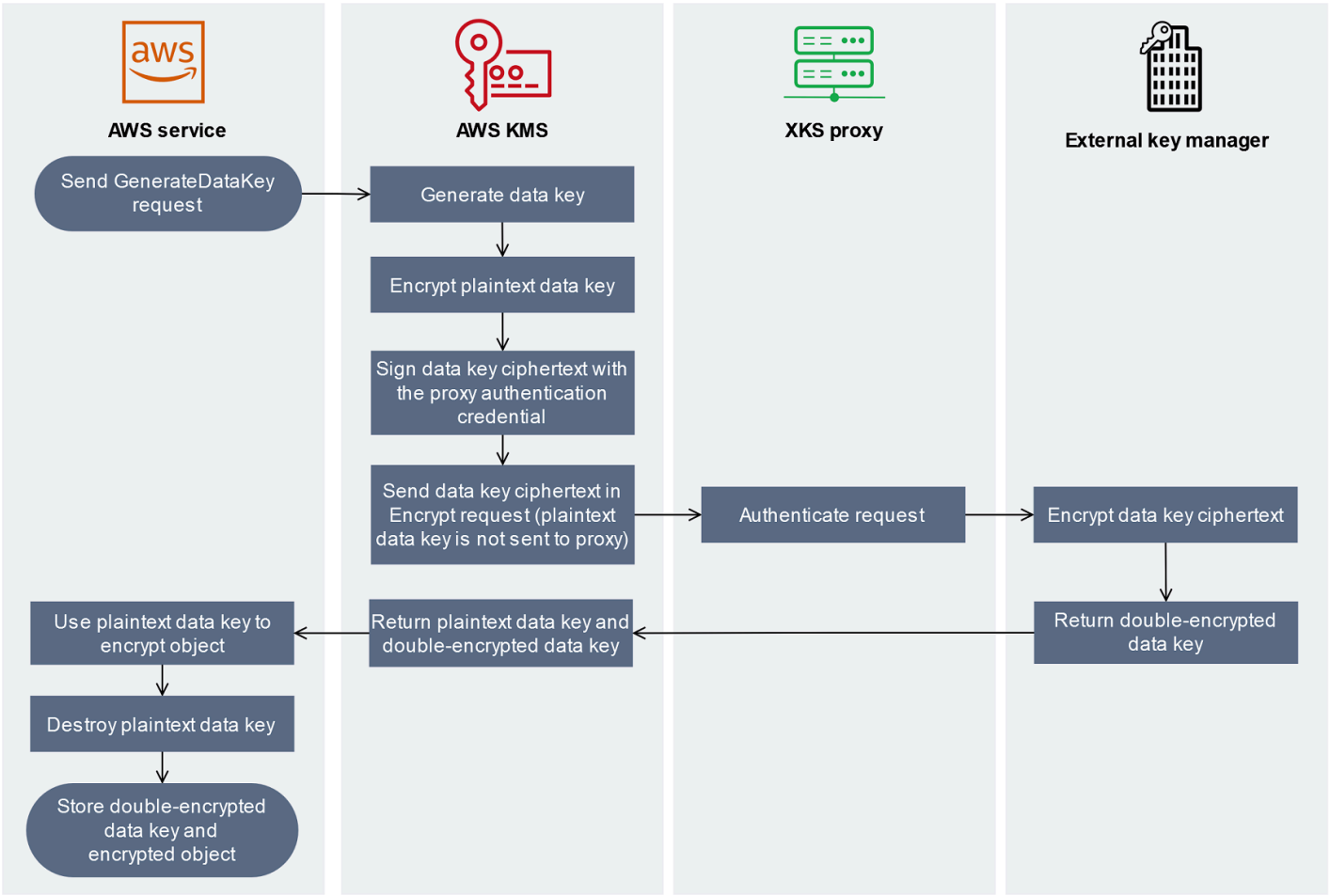
- Você não pode descriptografar nenhum texto cifrado criptografado por uma chave KMS em um armazenamento externo de chaves externo AWS, mesmo que você tenha o material de chave externo.
- Você não pode recriar uma chave do KMS que foi excluída de um armazenamento de chaves externas, mesmo que você tenha o material de chave externa. Cada chave do KMS tem metadados exclusivos que ela inclui no texto cifrado simétrico. Uma nova chave do KMS não seria capaz de descriptografar o texto cifrado criptografado pela chave original, ainda que usasse o mesmo material de chave externa.

Para obter um exemplo de criptografia dupla na prática, consulte Como funcionam os armazenamentos de chaves externas.

Como funcionam os armazenamentos de chaves externas

O armazenamento de chaves externas, o proxy de armazenamento de chaves externas e o gerenciador de chaves externas trabalham juntos para proteger seus recursos da AWS . O procedimento a seguir descreve o fluxo de trabalho de criptografia de um AWS service (Serviço da AWS) comum que criptografa cada objeto em uma chave de dados exclusiva protegida por uma chave do KMS. Nesse caso, você escolheu uma chave do KMS em um armazenamento de chaves externas para proteger o objeto. O exemplo mostra como AWS KMS usa criptografia dupla para proteger a chave de dados em trânsito e garantir que o texto cifrado gerado por uma chave KMS em um armazenamento de chaves externo seja sempre pelo menos tão forte quanto o texto cifrado criptografado por uma chave KMS simétrica padrão com material de chave inserido. AWS KMS

Os métodos de criptografia usados por cada unidade real AWS service (Serviço da AWS) que se integra AWS KMS variam. Para obter detalhes, consulte o tópico “Proteção dos dados” no capítulo Segurança da documentação do AWS service (Serviço da AWS) .



1. Você adiciona um novo objeto ao seu AWS service (Serviço da AWS) recurso. Para criptografar o objeto, AWS service (Serviço da AWS) ele envia uma GenerateDataKeysolicitação para AWS KMS usar uma chave KMS em seu armazenamento de chaves externo.
2. AWS KMS gera uma chave de dados simétrica de 256 bits e se prepara para enviar uma cópia da chave de dados em texto simples para o gerenciador de chaves externo por meio do proxy externo do armazenamento de chaves. AWS KMS inicia o processo de criptografia dupla criptografando a chave de dados em texto simples com o material de AWS KMS chave associado à chave KMS no armazenamento de chaves externo.
3. AWS KMS envia uma solicitação de criptografia para o proxy externo do armazenamento de chaves associado ao armazenamento de chaves externo. A solicitação inclui o texto cifrado da chave de dados a ser criptografado e a ID da chave externa associada à chave KMS. AWS KMS assina a solicitação usando a credencial de autenticação de proxy para seu proxy externo de armazenamento de chaves.

A cópia em texto simples da chave de dados não é enviada para o proxy de armazenamento de chaves externas.

4. O proxy de armazenamento de chaves externas autentica a solicitação e passa a solicitação de criptografia para o gerenciador de chaves externas.

   Alguns proxies de armazenamento de chaves externas também implementam uma política de autorização opcional que permite que somente entidades principais selecionadas realizem operações sob condições específicas.

5. O gerenciador de chaves externas criptografa o texto cifrado da chave de dados usando a chave externa especificada. O gerenciador de chaves externas retorna a chave de dados com criptografia dupla para o proxy de armazenamento de chaves externas, que a retorna para o AWS KMS.
6. AWS KMS retorna a chave de dados em texto simples e a cópia criptografada dupla dessa chave de dados para o. AWS service (Serviço da AWS)
7. O AWS service (Serviço da AWS) usa a chave de dados de texto simples para criptografar o objeto de recurso, destrói a chave de dados de texto sem formatação e armazena a chave de dados criptografada com o objeto criptografado.

   Alguns Serviços da AWS podem armazenar em cache a chave de dados de texto simples para usar em vários objetos ou reutilizá-la enquanto o recurso estiver em uso. Para obter detalhes, consulte Como as chaves do KMS inutilizáveis afetam as chaves de dados.

Para descriptografar o objeto criptografado, é AWS service (Serviço da AWS) necessário enviar a chave de dados criptografada de volta AWS KMS em uma solicitação de descriptografia.
Para descriptografar a chave de dados criptografada, AWS KMS deve enviar a chave de dados criptografada de volta ao proxy externo do armazenamento de chaves com o ID da chave externa. Se a solicitação de descriptografia para o proxy externo do armazenamento de chaves falhar por algum motivo, não será AWS KMS possível descriptografar a chave de dados criptografada e não será possível descriptografar o AWS service (Serviço da AWS) objeto criptografado.

Controlar o acesso ao armazenamento de chaves externas

Todos os recursos de controle de acesso do AWS KMS (políticas de chave, políticas do IAM e concessões) que você usa com chaves do KMS padrão funcionam da mesma forma para chaves do KMS em um armazenamento de chaves externas. Você pode usar políticas do IAM para controlar o acesso às operações de API que criam e gerenciam armazenamentos de chaves externas. Use

políticas do IAM e políticas de chaves para controlar o acesso às AWS KMS keys no armazenamento de chaves externas. Você também pode usar políticas de controle de serviço para sua organização da AWS e políticas de endpoint da VPC para controlar o acesso às chaves do KMS em seu armazenamento de chaves externas.

Recomendamos que você forneça aos usuários e perfis apenas as permissões necessárias para as tarefas que possivelmente executarão.

Tópicos

- Autorizar gerenciadores de armazenamento de chaves externas
- Autorizar usuários de chaves do KMS em armazenamentos de chaves externas
- Autorizar o AWS KMS a se comunicar com o proxy de armazenamento de chaves externas
- Autorização de proxy de armazenamento de chaves externas (opcional)
- Autenticação mTLS (opcional)

Autorizar gerenciadores de armazenamento de chaves externas

As entidades principais que criam e gerenciam um armazenamento de chaves externas precisam de permissões para as operações de armazenamento de chaves personalizado. A lista a seguir descreve as permissões mínimas necessárias para os gerenciadores de armazenamento de chaves externas. Como um armazenamento de chaves personalizado não é um recurso da AWS, você não pode fornecer permissão a um armazenamento de chaves externas para entidades principais de outras Contas da AWS.

- `kms:CreateCustomKeyStore`
- `kms:DescribeCustomKeyStores`
- `kms:ConnectCustomKeyStore`
- `kms:DisconnectCustomKeyStore`
- `kms:UpdateCustomKeyStore`
- `kms:DeleteCustomKeyStore`

As entidades principais que criam um armazenamento de chaves externas precisam de permissão para criar e configurar os componentes do armazenamento de chaves externas. Elas podem criar armazenamentos de chaves externas somente em suas próprias contas. Para criar um

armazenamento de chaves externas com conectividade de serviço de endpoint da VPC, as entidades principais devem ter permissão para criar os seguintes componentes:

- Uma Amazon VPC
- Sub-redes públicas e privadas
- Um balanceador de carga de rede e grupo de destino
- Um serviço de endpoint da Amazon VPC

Para obter detalhes, consulte Identity and Access Management para a Amazon VPC, Gerenciamento de identidade e acesso para endpoints da VPC e serviços de endpoint da VPC e Elastic Load Balancing API permissions (Permissões de API do Elastic Load Balancing).

Autorizar usuários de chaves do KMS em armazenamentos de chaves externas

As entidades principais que criam e gerenciam AWS KMS keys no armazenamento de chaves externas exigem as mesmas permissões que as que criam e gerenciam qualquer chave do KMS no AWS KMS. A política de chaves padrão para a chave do KMS em um armazenamento de chaves externas é idêntica à política de chaves padrão para chaves do KMS no AWS KMS. O controle de acesso por atributo (ABAC), que usa etiquetas e aliases para controlar o acesso a chaves do KMS, também é eficaz em chaves do KMS em armazenamentos de chaves externas.

As entidades principais que usam as chaves do KMS no seu armazenamento de chaves personalizado para operações de criptografia precisam de permissão para executar a operação criptográfica com a chaves do KMS, como kms:Decrypt. Você pode fornecer essas permissões em uma política do IAM ou em uma política de chaves. No entanto, elas não precisam de permissões adicionais para usar uma chave do KMS em um armazenamento de chaves personalizado.

Para definir uma permissão que se aplique somente às chaves do KMS em um armazenamento de chaves externas, use a condição de política `kms:KeyOrigin` com um valor de `EXTERNAL_KEY_STORE`. Você pode usar essa condição para limitar a CreateKey permissão kms: ou qualquer permissão específica de um recurso de chave KMS. Por exemplo, a política do IAM a seguir permite que a identidade à qual está anexada chame as operações especificadas em todas as chaves do KMS da conta, desde que as chaves do KMS estejam em um armazenamento de chaves externas. É possível limitar a permissão às chaves do KMS em um armazenamento de chaves externas e às chaves do KMS em uma Conta da AWS, mas não a qualquer armazenamento de chaves externas específico na conta.

```
{
```

```
  "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"
    }
  }
}
```

Autorizar o AWS KMS a se comunicar com o proxy de armazenamento de chaves externas

O AWS KMS se comunica com seu gerenciador de chaves externas somente por meio do proxy de armazenamento de chaves externas que você fornece. O AWS KMS autentica o proxy assinando suas solicitações usando o processo Signature Version 4 (SigV4) com a credencial de autenticação de proxy de armazenamento de chaves externas que você especifica. Se você estiver usando conectividade de endpoint público para seu proxy de armazenamento de chaves externas, o AWS KMS não precisará de outras permissões.

No entanto, se você estiver usando a conectividade do serviço de endpoint da VPC, deverá conceder permissão para o AWS KMS criar um endpoint de interface para seu serviço de endpoint da Amazon VPC. Essa permissão é necessária, independentemente se o proxy de armazenamento de chaves externas está em sua VPC ou se o proxy de armazenamento de chaves externas está localizado em outro lugar, mas usa o serviço de endpoint da VPC para se comunicar com o AWS KMS.

Para permitir AWS KMS a criação de um endpoint de interface, use o console Amazon VPC ou ModifyVpcEndpointServicePermissionsa operação. Conceda permissões para a seguinte entidade principal: `cks.kms.<region>.amazonaws.com`.

Por exemplo, o comando da AWS CLI a seguir permite que o AWS KMS se conecte ao serviço de endpoint da VPC na região Oeste dos EUA (Oregon) (us-west-2). Antes de usar esse comando, substitua o ID do serviço da Amazon VPC e a Região da AWS por valores válidos para sua configuração.

```
modify-vpc-endpoint-service-permissions
--service-id vpce-svc-12abc34567def0987
--add-allowed-principals '["cks.kms.us-west-2.amazonaws.com"]'
```

Para remover essa permissão, use o console da Amazon VPC ou o ModifyVpcEndpointServicePermissionscom o `RemoveAllowedPrincipals` parâmetro.

Autorização de proxy de armazenamento de chaves externas (opcional)

Alguns proxies de armazenamento de chaves externas implementam requisitos de autorização para o uso de suas chaves externas. O proxy de armazenamento de chaves externas é permitido, mas não obrigatório, para criar e implementar um esquema de autorização que permita que usuários específicos solicitem operações específicas somente sob certas condições. Por exemplo, o proxy pode ser configurado para dar ao usuário A permissão para criptografar com uma chave externa específica, mas não para descriptografar com ela.

A autorização de proxy é independente da autenticação de proxy baseada em SIGv4 que o AWS KMS exige para todos os proxies de armazenamento de chaves externas. Também é independente das políticas de chave, políticas do IAM e concessões que autorizam o acesso a operações que afetam o armazenamento de chaves externas ou suas chaves do KMS.

Para habilitar a autorização pelo proxy de armazenamento de chaves externas, o AWS KMS inclui metadados em cada solicitação da API de proxy, incluindo o autor da chamada, a chave do KMS, a operação do AWS KMS e o AWS service (Serviço da AWS) (se houver). Veja a seguir os metadados da solicitação para a versão 1 (v1) da API de proxy de chave externa.

```
"requestMetadata": {
    "awsPrincipalArn": string,
    "awsSourceVpc": string, // optional
    "awsSourceVpce": string, // optional
    "kmsKeyArn": string,
    "kmsOperation": string,
    "kmsRequestId": string,
    "kmsViaService": string // optional
}
```

Por exemplo, você pode configurar o proxy para permitir solicitações de uma entidade principal específica (`awsPrincipalArn`), mas somente quando a solicitação é feita em nome da entidade principal por um AWS service (Serviço da AWS) específico (`kmsViaService`).

Se a autorização do proxy falhar, a operação do AWS KMS relacionada falhará com uma mensagem que explica o erro. Para obter mais detalhes, consulte Problemas de autorização de proxy.

Autenticação mTLS (opcional)

Para habilitar o proxy de armazenamento de chaves externas para autenticar solicitações do AWS KMS, o AWS KMS assina todas as solicitações para seu proxy de armazenamento de chaves externas com uma credencial de autenticação Signature V4 (SigV4) para o armazenamento de chaves externas.

Para assegurar que o proxy de armazenamento de chaves externas responda somente às solicitações do AWS KMS, alguns proxies de chave externa oferecem suporte à Transport Layer Security mútua (mTLS), na qual as duas partes da transação usam certificados para se autenticar. O mTLS adiciona a autenticação do lado do cliente (em que o servidor de proxy do armazenamento de chaves externas autentica o cliente do AWS KMS) à autenticação do lado do servidor fornecida pelo TLS padrão. Caso a credencial de autenticação de proxy esteja comprometida, o que raramente acontece, o mTLS impede que terceiros façam solicitações de API bem-sucedidas ao proxy do armazenamento de chaves externas.

Para implementar o mTLS, configure seu proxy de armazenamento de chaves externas para aceitar somente certificados TLS do lado do cliente com as seguintes propriedades:

- O nome comum da entidade no certificado TLS deve ser `cks.kms.<Region>.amazonaws.com`, por exemplo, `cks.kms.eu-west-3.amazonaws.com`.
- O certificado deve estar vinculado a uma autoridade de certificação associada ao Amazon Trust Services.

Planejar um armazenamento de chaves externas

Antes de criar seu armazenamento de chaves externas, escolha a opção de conectividade que determina como o AWS KMS se comunicará com os componentes do armazenamento de chaves externas. A opção de conectividade escolhida determinará o restante do processo de planejamento.

Saiba mais:

- Analise o processo de criação de um armazenamento de chaves externas, incluindo a montagem dos pré-requisitos. Isso ajudará a garantir que você tenha todos os componentes obrigatórios para criar seu armazenamento de chaves externas.

- Saiba como controlar o acesso ao armazenamento de chaves externas, inclusive as permissões que os administradores e usuários do armazenamento de chaves externas exigem.
- Saiba mais sobre as CloudWatch métricas e dimensões da Amazon que AWS KMS registram para lojas de chaves externas. É altamente recomendável criar alarmes para monitorar o armazenamento de chaves externas para poder detectar os primeiros sinais de problemas operacionais e de performance.

Escolher uma opção de conectividade do proxy

Se você estiver criando um armazenamento de chaves externas, precisará determinar como o AWS KMS se comunica com o proxy de armazenamento de chaves externas. Essa escolha determinará quais componentes são necessários e como configurá-los. O AWS KMS oferece suporte às opções de conectividade a seguir. Escolha a opção que atenda aos seus objetivos de performance e segurança.

Antes de começar, confirme se você precisa de um armazenamento de chaves externas. A maioria dos clientes pode usar chaves do KMS baseadas em material de chave do AWS KMS.

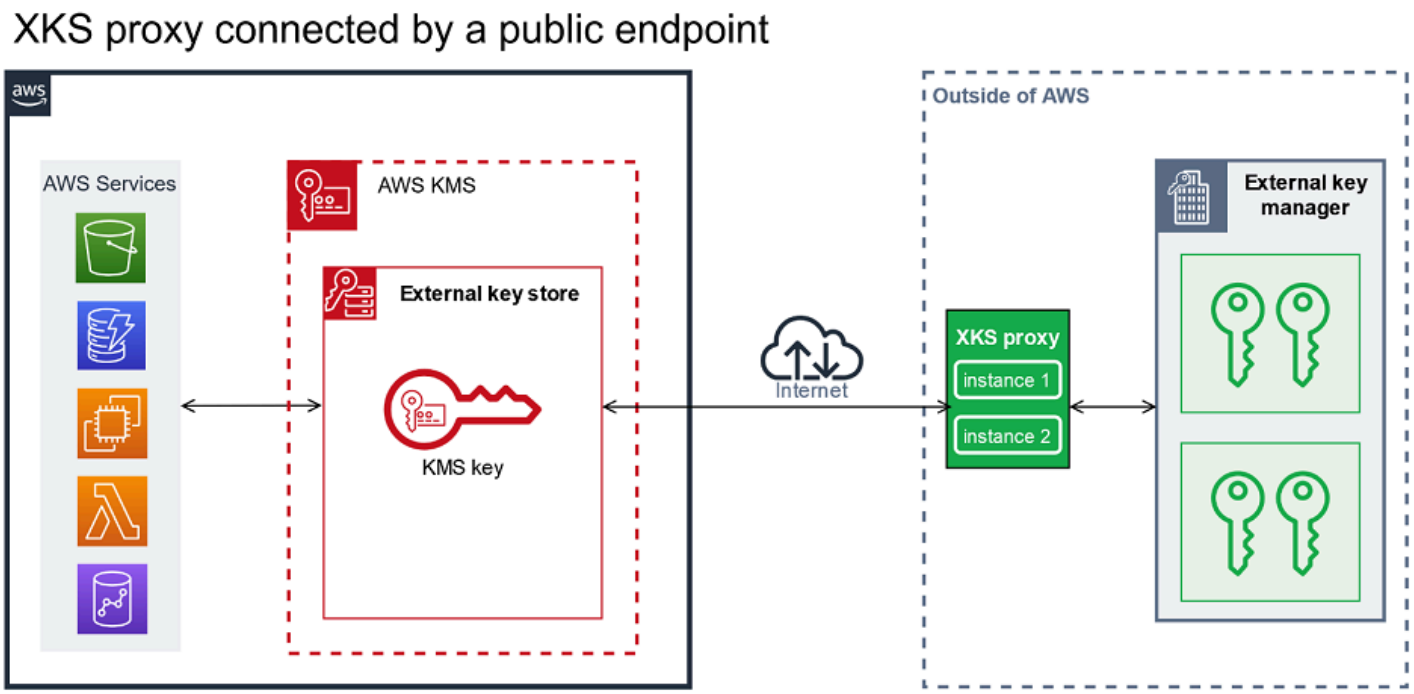
> **Note**
>
> Se seu proxy de armazenamento de chaves externas estiver incorporado ao gerenciador de chaves externas, a conectividade poderá ser predeterminada. Para obter orientações, consulte a documentação do gerenciador de chaves externas ou do proxy de armazenamento de chaves externas.

Você pode alterar a opção de conectividade de proxy de armazenamento de chaves externas mesmo em um armazenamento de chaves externas operacional. Contudo, o processo deve ser planejado e executado com atenção para minimizar interrupções, evitar erros e garantir acesso contínuo às chaves de criptografia que criptografam seus dados.

Conectividade de endpoints públicos

O AWS KMS se conecta ao proxy de armazenamento de chaves externas (proxy XKS) pela Internet usando um endpoint público.

Essa opção de conectividade é mais fácil de configurar e de manter e se alinha bem com alguns modelos de gerenciamento de chaves. No entanto, pode não atender aos requisitos de segurança de algumas organizações.



Requisitos

Se você escolher a conectividade de endpoint público, será necessário realizar as ações a seguir.

- Seu proxy de armazenamento de chaves externas deve estar acessível em um endpoint roteável publicamente.
- Você pode usar o mesmo endpoint público para vários armazenamentos de chaves externas, desde que eles usem valores de caminho do URI do proxy diferentes.
- Você pode usar o mesmo endpoint para um armazenamento de chaves externas com conectividade de endpoint público e qualquer armazenamento de chaves externas com conectividade de serviços de endpoint da VPC na mesma Região da AWS, mesmo que os armazenamentos de chaves estejam em Contas da AWS diferentes.
- É necessário obter um certificado TLS emitido por uma autoridade de certificação pública com suporte para armazenamentos de chaves externas. Para obter uma lista, consulte Trusted Certificate Authorities (Autoridades de certificação confiáveis).

  O nome comum (CN) da entidade no certificado TLS deve corresponder ao nome do domínio no endpoint do URI do proxy do armazenamento de chaves externas. Por exemplo, se o endpoint público for `https://myproxy.xks.example.com`, o TLS, o CN no certificado TLS deverá ser `myproxy.xks.example.com` ou `*.xks.example.com`.

- Certifique-se de que qualquer firewall entre o AWS KMS e o proxy de armazenamento de chaves externas permita tráfego de entrada e saída pela porta 443 no proxy. O AWS KMS se comunica na porta 443. Esse valor não é configurável.

Para todos os requisitos de um armazenamento de chaves externas, consulte Organizar os pré-requisitos.

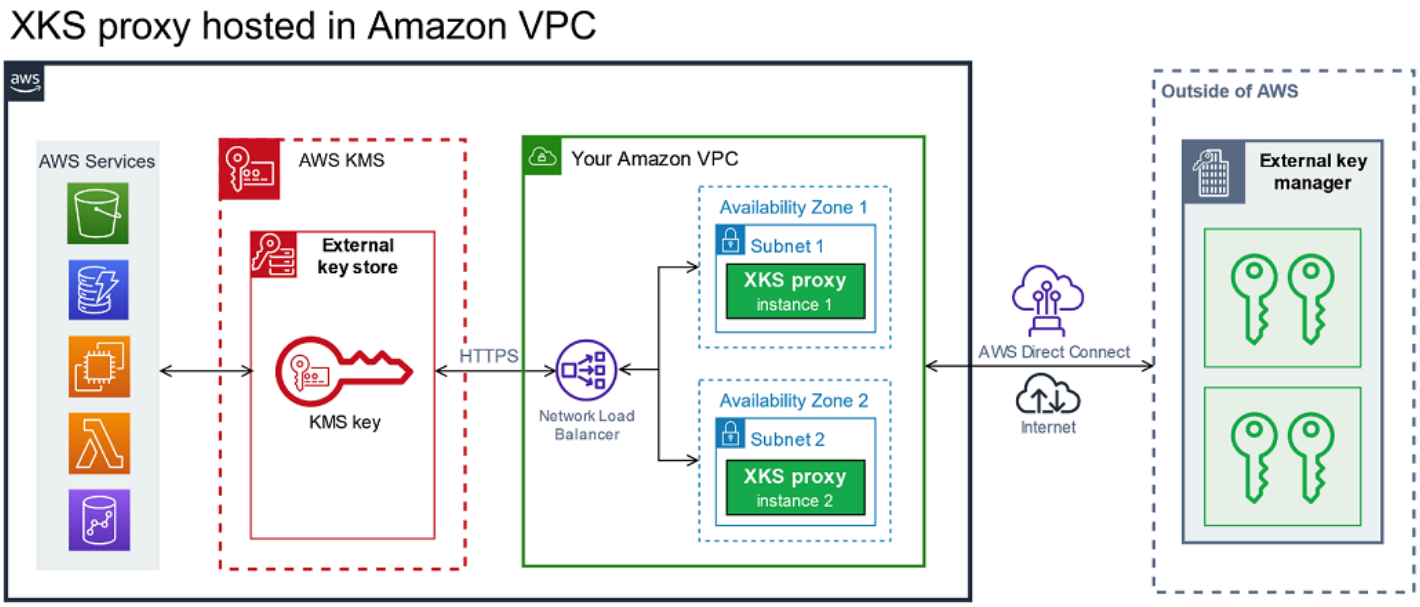
Conectividade do serviço de endpoint da VPC

O AWS KMS se conecta ao proxy de armazenamento de chaves externas (proxy XKS) criando um endpoint de interface para um serviço de endpoint da Amazon VPC que você cria e configura. Você é responsável por criar o serviço de endpoint da VPC e por conectar sua VPC ao gerenciador de chaves externas.

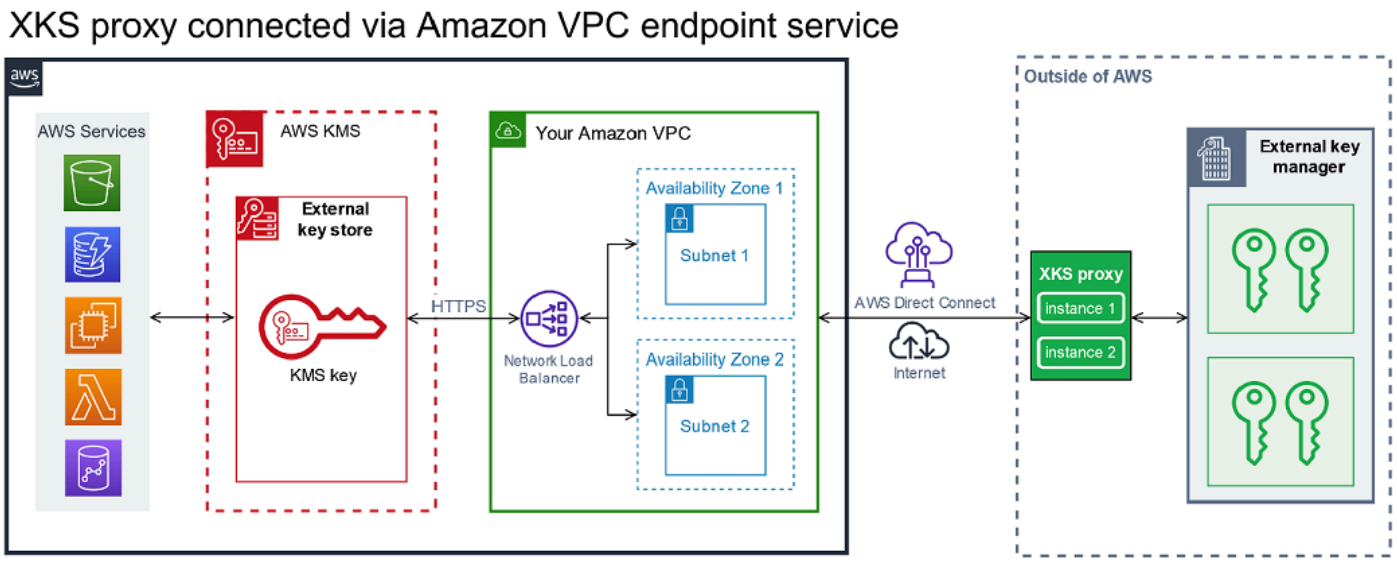
Seu serviço de endpoint pode usar qualquer uma das opções com suporte de rede para a Amazon VPC para comunicações, inclusive AWS Direct Connect.

Essa opção de conectividade é mais complicada de configurar e manter. Mas usa o AWS PrivateLink, permitindo que o AWS KMS se conecte de forma privada à sua Amazon VPC e ao proxy de armazenamento de chaves externas sem usar a Internet pública.

Você pode localizar o proxy de armazenamento de chaves externas na Amazon VPC.



Ou localize seu proxy de armazenamento de chaves externas fora da AWS e use seu serviço de endpoint da Amazon VPC somente para comunicação segura com o AWS KMS.



Configurar a conectividade do serviço de endpoint da VPC

Use as orientações desta seção para criar e configurar os recursos da AWS e componentes relacionados obrigatórios para um armazenamento de chaves externas que usa a conectividade do serviço de endpoint da VPC. Os recursos listados para essa opção de conectividade são um complemento aos recursos obrigatórios para todos os armazenamentos de chaves externas. Depois de criar e configurar os recursos obrigatórios, você pode criar seu armazenamento de chaves externas.

Você pode localizar seu proxy de armazenamento de chaves externas na Amazon VPC ou localizar o proxy fora da AWS e usar seu serviço de endpoint da VPC para comunicação.

Antes de começar, confirme se você precisa de um armazenamento de chaves externas. A maioria dos clientes pode usar chaves do KMS baseadas em material de chave do AWS KMS.

> **Note**
>
> Alguns dos elementos obrigatórios para a conectividade do serviço de endpoint da VPC podem estar incluídos no gerenciador de chaves externas. Além disso, seu software pode ter outros requisitos de configuração. Antes de criar e configurar os recursos da AWS desta seção, consulte a documentação do proxy e do gerenciador de chaves.

Tópicos

- Requisitos para conectividade do serviço de endpoint da VPC

- Criar uma Amazon VPC e sub-redes
- Criar um grupo de destino
- Criar um balanceador de carga de rede
- Criar um serviço de endpoint da VPC
- Verificar o domínio do DNS privado
- Autorizar o AWS KMS para se conectar ao serviço de endpoint da VPC

Requisitos para conectividade do serviço de endpoint da VPC

Se você escolher a conectividade do serviço de endpoint da VPC para seu armazenamento de chaves externas, serão necessários os recursos a seguir.

Para minimizar a latência da rede, crie seus componentes da AWS na Região da AWS com suporte que esteja mais próxima do gerenciador de chaves externas. Se possível, escolha uma região com um tempo de resposta (RTT) de 35 milissegundos ou menos.

- Uma Amazon VPC conectada ao gerenciador de chaves externas. Deve ter pelo menos duas sub-redes privadas em duas zonas de disponibilidade diferentes.

  Você pode usar uma Amazon VPC existente para seu armazenamento de chaves externas, desde que ela atenda aos requisitos de uso do armazenamento de chaves externas. Vários armazenamentos de chaves externas podem compartilhar uma Amazon VPC, mas cada armazenamento de chaves externas deve ter seu próprio serviço de endpoint da VPC e nome DNS privado.
- Um serviço de endpoint da Amazon VPC desenvolvido pelo AWS PrivateLink com um balanceador de carga de rede e um grupo de destino.

  O serviço de endpoint não pode exigir aceitação. Além disso, você deve adicionar o AWS KMS como entidade principal autorizada. Isso permite que o AWS KMS crie endpoints de interface para que ele possa se comunicar com seu proxy de armazenamento de chaves externas.
- Um nome DNS privado para o serviço de endpoint da VPC exclusivo em sua Região da AWS.

  O nome DNS privado deve ser o subdomínio de um domínio público de nível superior. Por exemplo, se o nome DNS privado for `myproxy-private.xks.example.com`, ele deverá ser o subdomínio de um domínio público, como `xks.example.com` ou `example.com`.

  É necessário verificar a propriedade do domínio DNS para o nome DNS privado.

- Um certificado TLS emitido por uma autoridade de certificação pública com suporte para o proxy de armazenamento de chaves externas.

  O nome comum (CN) da entidade no certificado TLS deve corresponder ao nome DNS privado. Por exemplo, se o nome DNS privado for `myproxy-private.xks.example.com`, o CN no certificado TLS deverá ser `myproxy-private.xks.example.com` ou `*.xks.example.com`.

Para todos os requisitos de um armazenamento de chaves externas, consulte Organizar os pré-requisitos.

Criar uma Amazon VPC e sub-redes

A conectividade do serviço de endpoint da VPC exige uma Amazon VPC conectada ao gerenciador de chaves externas com pelo menos duas sub-redes privadas. Você pode criar uma Amazon VPC ou usar uma Amazon VPC existente que atenda aos requisitos para armazenamentos de chaves externas. Para obter ajuda sobre como criar uma nova Amazon VPC, consulte Criar uma VPC no Guia do usuário da Amazon Virtual Private Cloud.

Requisitos para sua Amazon VPC

Para trabalhar com armazenamentos de chaves externas usando a conectividade do serviço de endpoint da VPC, a Amazon VPC deve ter as seguintes propriedades:

- Deve estar na mesma Conta da AWS e região com suporte do armazenamento de chaves externas.
- Requer pelo menos duas sub-redes privadas, cada uma em uma zona de disponibilidade diferente.
- O intervalo de endereços IP privados de sua Amazon VPC não deve se sobrepor ao intervalo de endereços IP privados do datacenter que hospeda seu gerenciador de chaves externas.
- Todos os componentes devem usar IPv4.

Você tem muitas opções para conectar a Amazon VPC ao seu proxy de armazenamento de chaves externas. Escolha uma opção que atenda a suas necessidades de performance e segurança. Para obter uma lista, consulte Conectar sua VPC a outras redes e Network-to-Amazon VPC connectivity options (Opções de conectividade entre a rede e a Amazon VPC). Para obter mais detalhes, consulte AWS Direct Connect e o Guia do usuário do AWS Site-to-Site VPN.

Criar uma Amazon VPC para seu armazenamento de chaves externas

Use as instruções a seguir para criar a Amazon VPC para o armazenamento de chaves externas. Uma Amazon VPC será necessária somente se você escolher a opção de conectividade do serviço de endpoint da VPC. Você pode criar uma Amazon VPC existente que atenda aos requisitos de um armazenamento de chaves externas.

Siga as instruções no tópico Criar uma VPC, sub-redes e outros recursos de VPC usando os valores obrigatórios abaixo. Para outros campos, aceite os valores padrão e forneça os nomes conforme solicitado.

Campo	Valor
IPv4 CIDR block (Bloco CIDR IPv4)	Insira os endereços IP da VPC. O intervalo de endereços IP privados de sua Amazon VPC não deve se sobrepor ao intervalo de endereços IP privados do datacenter que hospeda seu gerenciador de chaves externas.
Número de zonas de disponibilidade (AZs)	2 ou mais
Número de sub-redes públicas	Nenhum é obrigatório (0)
Número de sub-redes privadas	Um para cada AZ
Gateways NAT	Nenhum é obrigatório.
Endpoints da VPC	Nenhum é obrigatório.
Enable DNS hostnames	Sim
Habilitar a resolução de DNS	Sim

Não se esqueça de testar a comunicação da VPC. Por exemplo, se o proxy de armazenamento de chaves externas não estiver localizado na Amazon VPC, crie uma instância do Amazon EC2 em sua Amazon VPC e verifique se a Amazon VPC pode se comunicar com seu proxy de armazenamento de chaves externas.

Conectar a VPC ao gerenciador de chaves externas

Conecte a VPC ao datacenter em que o gerenciador de chaves externas está hospedado usando uma das opções de conectividade de rede compatíveis com a Amazon VPC. Certifique-se de que a instância do Amazon EC2 na VPC (ou o proxy de armazenamento de chaves externas, se estiver na VPC) possa se comunicar com o datacenter e o gerenciador de chaves externas.

Criar um grupo de destino

Antes de criar o serviço de endpoint da VPC obrigatório, crie seus componentes obrigatórios, um balanceador de carga de rede (NLB) e um grupo de destino. O balanceador de carga de rede (NLB) distribui solicitações entre vários destinos íntegros, e qualquer um deles pode atender à solicitação. Nesta etapa, você cria um grupo de destino com pelo menos dois hosts para seu proxy de armazenamento de chaves externas e registra seus endereços IP com o grupo de destino.

Siga as instruções no tópico Configure a target group (Configurar um grupo de destino) usando os valores obrigatórios a seguir. Para outros campos, aceite os valores padrão e forneça os nomes conforme solicitado.

Campo	Valor
Target type	Endereços IP
Protocolo	TCP
Porta	443
Tipo de endereço IP	IPv4
VPC	Escolha a VPC em que você criará o serviço de endpoint da VPC para seu armazenamento de chaves externas.
Protocolo e caminho de	O protocolo e o caminho de verificação de integridade serão diferentes da configuração de proxy de armazenamento de chaves externas. Consulte a

Campo	Valor
verificação de integridade	documentação do gerenciador de chaves externas ou do proxy de armazenamento de chaves externas. Para obter informações gerais sobre como configurar verificações de integridade para grupos de destino, consulte Health checks for your target groups (Verificações de integridade de grupos de destino) no Guia do usuário do Elastic Load Balancing para Network Load Balancers.
Rede	Outro endereço IP privado
Endereço IPv4	Os endereços privados do proxy de armazenamento de chaves externas
Portas	443

Criar um balanceador de carga de rede

O balanceador de carga de rede distribui o tráfego da rede, incluindo solicitações do AWS KMS para seu proxy de armazenamento de chaves externas, aos destinos configurados.

Siga as instruções no tópico Configure a load balancer and a listener (Configurar um balanceador de carga e um receptor) para configurar e adicionar um receptor e criar um balanceador de carga usando os valores obrigatórios a seguir. Para outros campos, aceite os valores padrão e forneça os nomes conforme solicitado.

Campo	Valor
Scheme	Interno
Tipo de endereço IP	IPv4
Mapeamento de rede	Escolha a VPC em que você criará o serviço de endpoint da VPC para seu armazenamento de chaves externas.
Mapeamento	Escolha as duas zonas de disponibilidade (pelo menos duas) que você configurou para as sub-redes da VPC. Verifique os nomes das sub-redes e o endereço IP privado.

Campo	Valor
Protocolo	TCP
Porta	443
Ação padrão: encaminhar para	Escolha o grupo de destino para seu balanceador de carga de rede.

Criar um serviço de endpoint da VPC

Normalmente, você cria um endpoint para um serviço. No entanto, ao criar um serviço de endpoint da VPC, você é o provedor, e o AWS KMS cria um endpoint para seu serviço. Para um armazenamento de chaves externas, crie um serviço de endpoint da VPC com o balanceador de carga de rede criado na etapa anterior. O serviço de endpoint da VPC deve estar na mesma Conta da AWS e região compatível que o armazenamento de chaves externas.

Vários armazenamentos de chaves externas podem compartilhar uma Amazon VPC, mas cada armazenamento de chaves externas deve ter seu próprio serviço de endpoint da VPC e nome DNS privado.

Siga as instruções no tópico Create an endpoint service (Criar um serviço de endpoint) para criar seu serviço de endpoint da VPC com os valores obrigatórios a seguir. Para outros campos, aceite os valores padrão e forneça os nomes conforme solicitado.

Campo	Valor
Tipo de load balancer	Rede
Balanceadores de carga disponíveis	Escolha o balanceador de carga de rede criado na etapa anterior. Se o novo balanceador de carga não for exibido na lista, verifique se o estado está ativo. Pode demorar alguns minutos para que o estado do balanceador de carga seja alterado de em provisionamento para ativo.
Aceitação obrigatória	Falso. Desmarque a caixa de seleção.

Campo	Valor
	Não requer aceitação. O AWS KMS não consegue se conectar ao serviço de endpoint da VPC sem uma aceitação manual. Se a aceitação for obrigatória, as tentativas de criar o armazenamento de chaves externas falharão com uma exceção `XksProxyInvalidConfigurationException` .
Habilitar nome DNS privado	Associar um nome DNS privado ao serviço
Nome DNS privado	Insira um nome DNS privado que seja exclusivo na Região da AWS. O nome DNS privado deve ser o subdomínio de um domínio público de nível superior. Por exemplo, se o nome DNS privado for `myproxy-private.xks.example.com` , ele deverá ser o subdomínio de um domínio público, como `xks.example.com` ou `example.com` . Esse nome DNS privado deve corresponder ao nome comum (CN) da entidade no certificado TLS configurado em seu proxy de armazenamento de chaves externas. Por exemplo, se o nome DNS privado for `myproxy-private.xks.example.com` , o CN no certificado TLS deverá ser `myproxy-private.xks.example.com` ou `*.xks.example.com` . Se o certificado e o nome DNS privado não coincidirem, as tentativas de conectar um armazenamento de chaves externas ao proxy de armazenamento de chaves externas falharão com um código de erro de conexão de `XKS_PROXY_INVALID_TLS_CONFIGURATION` . Para obter detalhes, consulte Erros gerais de configuração.
Tipos de endereço IP compatíveis	IPv4

Verificar o domínio do DNS privado

Quando você cria o serviço de endpoint da VPC, seu status de verificação de domínio é `pendingVerification`. Antes de usar o serviço de endpoint da VPC para criar um armazenamento de chaves externas, esse status deve ser `verified`. Para verificar se você é o

proprietário do domínio associado ao nome DNS privado, é necessário criar um registro TXT em um servidor DNS público.

Por exemplo, se o nome DNS privado do serviço de endpoint da VPC for `myproxy-private.xks.example.com`, você deverá criar um registro TXT em um domínio público, como `xks.example.com` ou `example.com`, o que for público. O AWS PrivateLink procura o registro TXT primeiro em `xks.example.com` e depois em `example.com`.

> **Tip**
>
> Depois que você adicionar um registro TXT, poderá levar alguns minutos para que o valor do status da verificação do domínio seja alterado de `pendingVerification` para `verify`.

Para começar, encontre o status de verificação do domínio usando um dos métodos a seguir. Os valores válidos são `verified`, `pendingVerification` e `failed`.

- No console da Amazon VPC, escolha Endpoint services (Serviços de endpoint) e escolha o serviço de endpoint. No painel de detalhes, consulte Domain verification status (Status da verificação do domínio).
- Use a DescribeVpcEndpointServiceConfigurationsoperação. O valor de `State` está no campo `ServiceConfigurations.PrivateDnsNameConfiguration.State`.

Se o status da verificação não for `verified`, siga as instruções no tópico Domain ownership verification (Verificação de propriedade do domínio) para adicionar um registro TXT ao servidor DNS do domínio e verificar se o registro TXT foi publicado. Em seguida, verifique o status de verificação novamente.

Não é necessário criar um registro A para o nome de domínio DNS privado. Quando o AWS KMS cria um endpoint de interface para seu serviço de endpoint da VPC, o AWS PrivateLink cria automaticamente uma zona hospedada com o registro A obrigatório para o nome de domínio privado na VPC do AWS KMS. Para armazenamentos de chaves externas com conectividade de serviço de endpoint da VPC, isso acontece quando você conecta seu armazenamento de chaves externas ao proxy de armazenamento de chaves externas.

Autorizar o AWS KMS para se conectar ao serviço de endpoint da VPC

Você deve adicionar o AWS KMS à lista de entidades principais autorizadas para seu serviço de endpoint da VPC. Isso permite que o AWS KMS crie endpoints de interface para seu

serviço de endpoint da VPC. Se o AWS KMS não for uma entidade principal autorizada, as tentativas de criar um armazenamento de chaves externas falharão, com a exceção `XksProxyVpcEndpointServiceNotFoundException`.

Siga as instruções no tópico Manage permissions (Gerenciar permissões) no Guia do AWS PrivateLink. Use o valor obrigatório a seguir.

Campo	Valor
ARN	`cks.kms.<region>.amazonaws.com` Por exemplo, `cks.kms.us-east-1.amazonaws.com` .

Próximo: Criar um armazenamento de chaves externas

Gerenciar um armazenamento de chaves externas

Você pode gerenciar um armazenamento de chaves externas usando o console do AWS KMS ou a API do AWS KMS. Você pode criar um armazenamento de chaves externas, visualizar e editar as propriedades, monitorar a performance e conectá-lo e desconectá-lo do proxy do armazenamento de chaves externas e excluir o armazenamento de chaves externas.

Tópicos

- Criar um armazenamento de chaves externas
- Editar propriedades do armazenamento de chaves externas
- Visualizar um armazenamento de chaves externas
- Monitorar um armazenamento de chaves externas
- Conectar e desconectar um armazenamento de chaves externas
- Excluir um armazenamento de chaves externas

Criar um armazenamento de chaves externas

Você pode criar um ou vários armazenamentos de chaves externas em cada região da Conta da AWS. Cada armazenamento de chaves externas deve estar associado a um gerenciador de chaves externas fora da AWS e a um proxy de armazenamento de chaves externas (proxy XKS) que é intermediário na comunicação entre o AWS KMS e o gerenciador de chaves externas. Para obter detalhes, consulte Planejar um armazenamento de chaves externas. Antes de começar, confirme se

você precisa de um armazenamento de chaves externas. A maioria dos clientes pode usar chaves do KMS baseadas em material de chave do AWS KMS.

> **Tip**
>
> Alguns gerenciadores de chaves externas fornecem um método mais simples de criar um armazenamento de chaves externas. Para obter detalhes, consulte a documentação do gerenciador de chaves externas.

Antes de criar o armazenamento de chaves externas, você precisa organizar os pré-requisitos. Durante o processo de criação, especifique as propriedades do armazenamento de chaves externas. Mais importante ainda, indique se o armazenamento de chaves externas no AWS KMS usa um endpoint público ou um serviço de endpoint da VPC para se conectar ao proxy de armazenamento de chaves externas. Especifique também os detalhes da conexão, inclusive o endpoint de URI do proxy e o caminho dentro desse endpoint de proxy em que o AWS KMS envia solicitações de API ao proxy.

- Se você usa conectividade de endpoint público, verifique se o AWS KMS pode se comunicar com o proxy pela Internet usando uma conexão HTTPS. Isso inclui configurar o TLS no proxy de armazenamento de chaves externas e garantir que os firewalls entre o AWS KMS e o proxy permitam tráfego de entrada e saída para a porta 443 no proxy. Ao criar um armazenamento de chaves externas com conectividade de endpoint público, o AWS KMS testa a conexão enviando uma solicitação de status ao proxy do armazenamento de chaves externas. Esse teste verifica se o endpoint está acessível e se o proxy de armazenamento de chaves externas aceitará uma solicitação assinada com sua credencial de autenticação de proxy de armazenamento de chaves externas. Se essa solicitação de teste falhar, a operação para criar o armazenamento de chaves externas falhará.
- Se você usa a conectividade do serviço de endpoint da VPC, verifique se o balanceador de carga de rede, o nome DNS privado e o serviço de endpoint da VPC estão configurados corretamente e em operação. Se o proxy do armazenamento de chaves externas não estiver na VPC, você precisará verificar se o serviço de endpoint da VPC pode se comunicar com o proxy de armazenamento de chaves externas. (O AWS KMS testa a conectividade do serviço de endpoint da VPC quando você conecta o armazenamento de chaves externas ao proxy de armazenamento de chaves externas.)

Considerações adicionais:

- AWS KMSregistra CloudWatch métricas e dimensões da Amazon, especialmente para lojas de chaves externas. Grafos de monitoramento baseados em algumas dessas métricas são exibidos no console do AWS KMS para cada armazenamento de chaves externas. É altamente recomendável usar essas métricas para criar alarmes que monitorem seu armazenamento de chaves externas. Esses alarmes alertam sobre os primeiros sinais de problemas operacionais e de performance antes que eles ocorram. Para obter instruções, consulte Monitorar um armazenamento de chaves externas.
- Os armazenamentos de chaves externas estão sujeitos a cotas de recursos. O uso de chaves do KMS em um armazenamento de chaves externas está sujeito às cotas de solicitação. Analise essas cotas antes de projetar sua implementação de armazenamento de chaves externas.

> **Note**
>
> Revise sua configuração para ver se há dependências circulares que possam impedi-lo de funcionar.
> Por exemplo, se você criar o proxy de armazenamento de chaves externo usando recursos do AWS, certifique-se de que a operação do proxy não exija a disponibilidade de uma chave do KMS em um armazenamento de chaves externo que seja acessado por meio desse proxy.

Todos os novos armazenamentos de chaves externas são criados no estado desconectado. Antes de criar chaves do KMS em seu armazenamento de chaves externas, é necessário conectá-lo ao proxy de armazenamento de chaves externas. Para alterar as propriedades do armazenamento de chaves externas, edite as configurações de armazenamento de chaves externas.

Tópicos

- Organizar os pré-requisitos
- Arquivo de configuração do proxy
- Criar um armazenamento de chaves externas (console)
- Criar um armazenamento de chaves externas (API)

Organizar os pré-requisitos

Antes de criar um armazenamento de chaves externas, é necessário organizar os componentes obrigatórios, incluindo o gerenciador de chaves externas que você usará para dar suporte ao

armazenamento de chaves externas e o proxy do armazenamento de chaves externas que converte as solicitações do AWS KMS para um formato que o gerenciador de chaves externas entenda.

Os componentes a seguir são obrigatórios para todos os armazenamentos de chaves externas. Além desses componentes, é necessário fornecer os componentes que ofereçam suporte à opção de conectividade do proxy de armazenamento de chaves externas que você escolher.

> **Tip**
>
> O gerenciador de chaves externas pode incluir alguns desses componentes ou eles poderão ser configurados para você. Para obter detalhes, consulte a documentação do gerenciador de chaves externas.
> Se você estiver criando seu armazenamento de chaves externas no console do AWS KMS, você tem a opção de carregar um arquivo de configuração de proxy baseado em JSON que especifica o caminho do URI do proxy e a credencial de autenticação do proxy. Alguns proxies de armazenamento de chaves externas geram esse arquivo para você. Para obter detalhes, consulte a documentação do proxy de armazenamento de chaves externas ou do gerenciador de chaves externas.

Gerenciador de chaves externas

Cada armazenamento de chaves externas requer pelo menos uma instância do gerenciador de chaves externas. Pode ser um módulo de segurança de hardware (HSM) físico ou virtual ou um software de gerenciamento de chaves.

Você pode usar um único gerenciador de chaves, mas recomendamos pelo menos duas instâncias de gerenciador de chaves relacionadas que compartilhem chaves de criptografia para redundância. O armazenamento de chaves externas não exige o uso exclusivo do gerenciador de chaves externas. Porém, o gerenciador de chaves externas deve ter a capacidade de lidar com a frequência esperada de solicitações de criptografia e descriptografia dos serviços da AWS que usam chaves do KMS no armazenamento de chaves externas para proteger seus recursos. O gerenciador de chaves externas deve ser configurado para lidar com até 1.800 solicitações por segundo e responder dentro do tempo limite de 250 milissegundos para cada solicitação. Recomendamos localizar o gerenciador de chaves externas próximo a uma Região da AWS para que o tempo de resposta (RTT) da rede seja de 35 milissegundos ou menos.

Se o proxy de armazenamento de chaves externas permitir, será possível alterar o gerenciador de chaves externas que você associa ao proxy de armazenamento de chaves externas, mas o novo

gerenciador de chaves externas deve ser um backup ou snapshot com o mesmo material de chave. Se a chave externa que você associa a uma chave do KMS não estiver mais disponível para seu proxy de armazenamento de chaves externas, o AWS KMS não poderá descriptografar o texto cifrado criptografado com a chave do KMS.

O gerenciador de chaves externas deve estar acessível ao proxy de armazenamento de chaves externas. Se a GetHealthStatusresposta do proxy informar que todas as instâncias externas do gerenciador de chaves sãoUnavailable, todas as tentativas de criar um armazenamento de chaves externo falharão com um XksProxyUriUnreachableException.

Proxy de armazenamento de chaves externas

É necessário especificar um proxy de armazenamento de chaves externas (proxy XKS) que esteja em conformidade com os requisitos de design em AWS KMS External Key Store Proxy API Specification (Especificação da API de proxy de armazenamento de chaves externas do). Você pode desenvolver ou comprar um proxy de armazenamento de chaves externas ou usar um proxy de armazenamento de chaves externas fornecido ou incorporado ao gerenciador de chaves externas. O AWS KMS recomenda que o proxy de armazenamento de chaves externas seja configurado para lidar com até 1.800 solicitações por segundo e responder dentro do tempo limite de 250 milissegundos para cada solicitação. Recomendamos localizar o gerenciador de chaves externas próximo a uma Região da AWS para que o tempo de resposta (RTT) da rede seja de 35 milissegundos ou menos.

Você pode usar um proxy de armazenamento de chaves externas para mais de um armazenamento de chaves externas, mas cada armazenamento de chaves externas deve ter um endpoint de URI e um caminho exclusivo dentro do proxy de armazenamento de chaves externas para as solicitações.

Se você estiver usando a conectividade do serviço de endpoint da VPC, poderá localizar o proxy de armazenamento de chaves externas na Amazon VPC, mas isso não é necessário. Você pode localizar seu proxy fora da AWS, como em seu datacenter privado, e usar o serviço de endpoint da VPC somente para se comunicar com o proxy.

Credencial de autenticação de proxy

Para criar um armazenamento de chaves externas, é necessário especificar sua credencial de autenticação de proxy de armazenamento de chaves externas (XksProxyAuthenticationCredential).

É necessário estabelecer uma credencial de autenticação (XksProxyAuthenticationCredential) para o AWS KMS em seu proxy de armazenamento de

chaves externas. O AWS KMS autentica seu proxy assinando suas solicitações usando o processo Signature Version 4 (SigV4) com a credencial de autenticação de proxy do armazenamento de chaves externas. Você especifica a credencial de autenticação ao criar seu armazenamento de chaves externas e pode alterá-la a qualquer momento. Se o proxy alternar sua credencial, certifique-se de atualizar os valores da credencial para seu armazenamento de chaves externas.

A credencial de autenticação do proxy tem duas partes. É necessário fornecer as duas partes para o armazenamento de chaves externas.

- ID da chave de acesso: identifica a chave de acesso secreta. Você pode fornecer o ID em texto não criptografado.
- Chave de acesso secreta: a parte secreta da credencial. O AWS KMS criptografa a chave de acesso secreta na credencial antes de armazená-la.

A credencial SigV4 que o AWS KMS usa para assinar solicitações ao proxy de armazenamento de chaves externas não está relacionada a credenciais SigV4 associadas às entidades principais do AWS Identity and Access Management de suas contas da AWS. Não reutilize nenhuma credencial SigV4 do IAM para seu proxy de armazenamento de chaves externas.

Conectividade do proxy

Para criar um armazenamento de chaves externas, é necessário especificar sua opção de conectividade do proxy de armazenamento de chaves externas (`XksProxyConnectivity`).

O AWS KMS pode se comunicar com seu proxy de armazenamento de chaves externas usando um endpoint público ou um serviço de endpoint da Amazon Virtual Private Cloud (Amazon VPC). Embora seja mais simples de configurar e manter, um endpoint público pode não atender aos requisitos de segurança de todas as instalações. Se você escolher a opção de conectividade do serviço de endpoint da Amazon VPC, deverá criar e manter os componentes obrigatórios, inclusive uma Amazon VPC com pelo menos duas sub-redes em duas zonas de disponibilidade diferentes, um serviço de endpoint da VPC com um balanceador de carga de rede e grupo de destino e um nome DNS privado para o serviço de endpoint da VPC.

Você pode alterar a opção de conectividade de proxy para seu armazenamento de chaves externas. No entanto, você deve garantir a disponibilidade contínua do material de chave associado às chaves do KMS em seu armazenamento de chaves externas. Caso contrário, o AWS KMS não conseguirá descriptografar nenhum texto cifrado criptografado com essas chaves do KMS.

Para obter ajuda para decidir qual opção de conectividade de proxy é melhor para seu armazenamento de chaves externas, consulte Escolher uma opção de conectividade do proxy. Para obter ajuda para criar uma configuração da conectividade do serviço de endpoint da VPC, consulte Configurar a conectividade do serviço de endpoint da VPC.

Endpoint de URI do proxy

Para criar um armazenamento de chaves externas, você deve especificar o endpoint (`XksProxyUriEndpoint`) que o AWS KMS usa para enviar solicitações ao proxy de armazenamento de chaves externas.

O protocolo deve ser o HTTPS. O AWS KMS se comunica na porta 443. Não especifique a porta no valor do endpoint do URI do proxy.

- Conectividade de endpoint público: especifique o endpoint disponível publicamente para seu proxy de armazenamento de chaves externas. Esse endpoint deve estar acessível antes de você criar o armazenamento de chaves externas.
- Conectividade do serviço de endpoint da VPC: especifique `https://` seguido pelo nome DNS privado do serviço de endpoint da VPC.

O certificado do servidor TLS configurado no proxy do armazenamento de chaves externas deve corresponder ao nome do domínio no endpoint de URI do proxy de armazenamento de chaves externas e ser emitido por uma autoridade de certificação com suporte para armazenamentos de chaves externas. Para obter uma lista, consulte Trusted Certificate Authorities (Autoridades de certificação confiáveis). A autoridade de certificação exigirá prova de propriedade do domínio antes de emitir o certificado TLS.

O nome comum (CN) da entidade no certificado TLS deve corresponder ao nome DNS privado. Por exemplo, se o nome DNS privado for `myproxy-private.xks.example.com`, o CN no certificado TLS deverá ser `myproxy-private.xks.example.com` ou `*.xks.example.com`.

Você pode alterar seu endpoint do URI do proxy, mas certifique-se de que o proxy do armazenamento de chaves externas tenha acesso ao material de chave associado às chaves do KMS de seu armazenamento de chaves externas. Caso contrário, o AWS KMS não conseguirá descriptografar nenhum texto cifrado criptografado com essas chaves do KMS.

Requisitos de exclusividade

- O valor combinado do endpoint (`XksProxyUriEndpoint`) do URI do proxy e do caminho do URI do proxy (`XksProxyUriPath`) deve ser exclusivo na região e Conta da AWS.
- Armazenamentos de chaves externas com conectividade de endpoint público podem compartilhar o mesmo endpoint do URI do proxy, desde que tenham valores do caminho do URI do proxy diferentes.
- Um armazenamento de chaves externas com conectividade de endpoint público não pode usar o mesmo valor de endpoint do URI do proxy que qualquer armazenamento de chaves externas com conectividade de serviços de endpoint da VPC na mesma Região da AWS, mesmo que os armazenamentos de chaves estejam em Contas da AWS diferentes.
- Cada armazenamento de chaves externas com conectividade de endpoint da VPC deve ter seu próprio nome DNS privado. O endpoint do URI do proxy (nome DNS privado) deve ser exclusivo na região e Conta da AWS.

Caminho do URI do proxy

Para criar um armazenamento de chaves externas, é necessário especificar o caminho base em seu proxy de armazenamento de chaves externas para as APIs de proxy necessárias. O valor deve começar com `/` e terminar com /kms/xks/v1, em que `v1` representa a versão da API do AWS KMS para o proxy de armazenamento de chaves externas. Esse caminho pode incluir um prefixo opcional entre os elementos obrigatórios, como `/example-prefix/kms/xks/v1`. Para encontrar esse valor, consulte a documentação do proxy de armazenamento de chaves externas.

O AWS KMS envia solicitações de proxy ao endereço especificado pela concatenação do endpoint do URI do proxy e do caminho do URI do proxy. Por exemplo, se o endpoint do URI do proxy for `https://myproxy.xks.example.com` e o caminho do URI do proxy for `/kms/xks/v1`, o AWS KMS enviará suas solicitações de API de proxy para `https://myproxy.xks.example.com/kms/xks/v1`.

Você pode alterar o caminho do URI do proxy, mas certifique-se de que o proxy do armazenamento de chaves externas tenha acesso ao material de chave associado às chaves do KMS de seu armazenamento de chaves externas. Caso contrário, o AWS KMS não conseguirá descriptografar nenhum texto cifrado criptografado com essas chaves do KMS.

Requisitos de exclusividade

- O valor combinado do endpoint (`XksProxyUriEndpoint`) do URI do proxy e do caminho do URI do proxy (`XksProxyUriPath`) deve ser exclusivo na região e Conta da AWS.

Serviço de VPC endpoint

Especifica o nome do serviço de endpoint da Amazon VPC usado para se comunicar com o proxy de armazenamento de chaves externas. Esse componente é obrigatório somente para armazenamentos de chaves externas que usam conectividade de serviços de endpoint da VPC. Para obter ajuda para instalar e configurar seu serviço de endpoint da VPC para um armazenamento de chaves externas, consulte Configurar a conectividade do serviço de endpoint da VPC.

O serviço de endpoint da VPC deve ter as seguintes propriedades:

- O serviço de endpoint da VPC deve estar na mesma região e Conta da AWS que o armazenamento de chaves externas.
- Deve ter um balanceador de carga de rede (NLB) conectado a pelo menos duas sub-redes, cada uma em uma zona de disponibilidade diferente.
- A lista de entidades principais autorizadas para o serviço de endpoint da VPC deve incluir a entidade principal do serviço do AWS KMS da região: `cks.kms.<region>.amazonaws.com`, como `cks.kms.us-east-1.amazonaws.com`.
- Não deve exigir a aceitação de solicitações de conexão.
- Deve ter um nome DNS privado dentro de um domínio público de nível superior. Por exemplo, você pode ter o nome DNS privado myproxy-private.xks.example.com no domínio público `xks.example.com`.

  O nome DNS privado de um armazenamento de chaves externas com conectividade do serviço de endpoint da VPC deve ser exclusivo na Região da AWS.
- O status da verificação do domínio do nome DNS privado deverá ser `verified`.
- O certificado do servidor TLS configurado no proxy do armazenamento de chaves externas deve especificar o nome de host DNS privado no qual o endpoint pode ser acessado.

Requisitos de exclusividade

- Armazenamentos de chaves externas com conectividade de endpoint da VPC podem compartilhar uma `Amazon VPC`, mas cada armazenamento de chaves externas deve ter seu próprio serviço de endpoint da VPC e nome DNS privado.

Arquivo de configuração do proxy

Um arquivo de configuração de proxy é um arquivo opcional baseado em JSON que contém valores para o caminho do URI do proxy e as propriedades da credencial de autenticação do proxy do armazenamento de chaves externas. Ao criar ou editar um armazenamento de chaves externas no console do AWS KMS, é possível carregar um arquivo de configuração de proxy para fornecer valores de configuração para o armazenamento de chaves externas. Usar esse arquivo evita erros de digitação e colagem e garante que os valores do armazenamento de chaves externas correspondam aos valores do proxy de armazenamento de chaves externas.

Os arquivos de configuração do proxy são gerados pelo proxy de armazenamento de chaves externas. Para saber se o proxy de armazenamento de chaves externas oferece um arquivo de configuração de proxy, consulte a documentação do proxy de armazenamento de chaves externas.

Veja a seguir o exemplo de um arquivo de configuração de proxy bem formado com valores fictícios.

```
{
  "XksProxyUriPath": "/example-prefix/kms/xks/v1",
  "XksProxyAuthenticationCredential": {
    "AccessKeyId": "ABCDE12345670EXAMPLE",
    "RawSecretAccessKey": "0000EXAMPLEFA5FT0mCc3DrGUe2sti527BitkQ0Zr9MO9+vE="
  }
}
```

Você pode carregar um arquivo de configuração de proxy somente ao criar ou editar um armazenamento de chaves externas no console do AWS KMS. Você não pode usá-lo com as UpdateCustomKeyStoreoperações CreateCustomKeyStoreou, mas pode usar os valores no arquivo de configuração do proxy para garantir que os valores dos parâmetros estejam corretos.

Criar um armazenamento de chaves externas (console)

Antes de criar um armazenamento de chaves externas, analise Planejar um armazenamento de chaves externas, escolha o tipo de conectividade de proxy e verifique se você criou e configurou todos os componentes obrigatórios. Se precisar de ajuda para encontrar algum dos valores obrigatórios, consulte a documentação do proxy de armazenamento de chaves externas ou do software de gerenciamento de chaves.

> **Note**
>
> Ao criar um armazenamento de chaves externas no AWS Management Console, você pode carregar um arquivo de configuração de proxy baseado em JSON com valores para

o caminho do URI do proxy e a credencial de autenticação do proxy. Alguns proxies geram esse arquivo para você. Não é obrigatório.

1. Faça login no AWS Management Console e abra o console do AWS Key Management Service (AWS KMS) em https://console.aws.amazon.com/kms.
2. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.
3. No painel de navegação, selecione Custom key stores (Armazenamentos de chaves personalizados), External key stores (Armazenamentos de chaves externas).
4. Escolha Create external key store (Criar armazenamento de chaves externas).
5. Digite um nome amigável para o armazenamento de chaves externas. O nome deve ser exclusivo entre todos os outros armazenamentos de chaves externas da conta.

   > **Important**
   >
   > Não inclua informações confidenciais ou sigilosas nesse campo. Esse campo pode ser exibido em texto simples em CloudTrail registros e outras saídas.

6. Escolha o tipo de conectividade de proxy.

   A escolha de conectividade de proxy determina os componentes obrigatórios para o proxy de armazenamento de chaves externas. Para obter ajuda para fazer essa escolha, consulte Escolher uma opção de conectividade do proxy.
7. Escolha ou insira o nome do serviço de endpoint da VPC para esse armazenamento de chaves externas. Essa etapa é exibida somente quando o tipo de conectividade de proxy de armazenamento de chaves externas é o serviço de endpoint da VPC.

   O serviço de endpoint da VPC e suas VPCs devem atender aos requisitos de um armazenamento de chaves externas. Para obter detalhes, consulte the section called “Organizar os pré-requisitos”.
8. Insira o endpoint do URI do proxy. O protocolo deve ser o HTTPS. O AWS KMS se comunica na porta 443. Não especifique a porta no valor do endpoint do URI do proxy.

   Se o AWS KMS reconhecer o serviço de endpoint da VPC que você especificou na etapa anterior, ele preencherá este campo para você.

Para obter conectividade de endpoint público, insira um URI de endpoint disponível publicamente. Para obter conectividade do endpoint da VPC: insira `https://` seguido pelo nome DNS privado do serviço de endpoint da VPC.

9. Para inserir os valores do prefixo do caminho do URI do proxy e da credencial de autenticação do proxy, carregue um arquivo de configuração do proxy ou insira os valores manualmente.

   - Se você tiver um arquivo de configuração de proxy opcional que contenha valores para o caminho do URI do proxy e a credencial de autenticação do proxy, escolha Upload configuration file (Carregar arquivo de configuração). Siga as etapas para carregar o arquivo.

     Quando o arquivo for carregado, o console exibirá os valores do arquivo em campos editáveis. Você pode alterar os valores agora ou editar esses valores depois que o armazenamento de chaves externas for criado.

     Para exibir o valor da chave de acesso secreta, escolha Show secret access key (Exibir chave de acesso secreta).

   - Caso não tenha um arquivo de configuração de proxy, você poderá inserir o caminho do URI do proxy e os valores da credencial de autenticação do proxy manualmente.

     a. Caso não tenha um arquivo de configuração de proxy, insira o URI do proxy manualmente. O console fornece o valor obrigatório de /kms/xks/v1.

        Se o caminho do URI do proxy incluir um prefixo opcional, como `example-prefix` em `/example-prefix/kms/xks/v1`, insira o prefixo no campo Proxy URI path prefix (Prefixo do caminho do URI do proxy). Senão, deixe o campo vazio.

     b. Caso não tenha um arquivo de configuração de proxy, insira a credencial de autenticação do proxy manualmente. Tanto o ID da chave de acesso como a chave de acesso secreta são obrigatórios.

        - Em Proxy credential: Access key ID (Credencial do proxy: ID da chave de acesso), insira o ID da chave de acesso da credencial de autenticação do proxy. O ID da chave de acesso identifica a chave de acesso secreta.
        - Em Proxy credential: Secret acces key (Credencial do proxy: chave de acesso secreta), insira a chave de acesso secreta da credencial de autenticação do proxy.

Para exibir o valor da chave de acesso secreta, escolha Show secret access key (Exibir chave de acesso secreta).

Esse procedimento não define nem altera a credencial de autenticação que você estabeleceu no proxy de armazenamento de chaves externas. Ele apenas associa esses valores ao armazenamento de chaves externas. Para obter informações sobre como configurar, alterar e alternar sua credencial de autenticação de proxy, consulte a documentação do proxy de armazenamento de chaves externas ou do software de gerenciamento de chaves.

Se a credencial de autenticação de proxy for alterada, edite a configuração de credencial para seu armazenamento de chaves externas.

10. Escolha Create external key store (Criar armazenamento de chaves externas).

Se o procedimento for bem-sucedido, o novo armazenamento de chaves externas será exibido na lista de armazenamentos de chaves externas na conta e região. Se ele for malsucedido, será exibida uma mensagem de erro descrevendo o problema e fornecendo ajuda para corrigi-lo. Se precisar de ajuda adicional, consulte CreateKey erros na chave externa.

Próximo: os novos armazenamentos de chaves externas não são conectados automaticamente. Antes de criar AWS KMS keys em seu armazenamento de chaves externas, é necessário conectar o armazenamento de chaves externas ao proxy de armazenamento de chaves externas.

Criar um armazenamento de chaves externas (API)

Você pode usar a CreateCustomKeyStoreoperação para criar um novo armazenamento de chaves externo. Para obter ajuda para encontrar os valores dos parâmetros obrigatórios, consulte a documentação do proxy de armazenamento de chaves externas ou do software de gerenciamento de chaves.

> **Tip**
>
> Você não pode carregar um arquivo de configuração de proxy ao usar a operação `CreateCustomKeyStore`. Porém, você pode usar os valores no arquivo de configuração do proxy para garantir que os valores dos parâmetros estejam corretos.

Para criar um armazenamento de chaves externas, a operação `CreateCustomKeyStore` exige os valores de parâmetros a seguir.

- `CustomKeyStoreName`: um nome amigável para o armazenamento de chaves externas que é exclusivo na conta.

  > **Important**
  >
  > Não inclua informações confidenciais ou sigilosas nesse campo. Esse campo pode ser exibido em texto simples em CloudTrail registros e outras saídas.

- `CustomKeyStoreType`: especifique `EXTERNAL_KEY_STORE`.
- `XksProxyConnectivity`: especifique `PUBLIC_ENDPOINT` ou `VPC_ENDPOINT_SERVICE`.
- `XksProxyAuthenticationCredential`: especifique o ID da chave de acesso e a chave de acesso secreta.
- `XksProxyUriEndpoint`: o endpoint que o AWS KMS usa para se comunicar com o proxy de armazenamento de chaves externas.
- `XksProxyUriPath`: o caminho dentro do proxy para as APIs de proxy.
- `XksProxyVpcEndpointServiceName`: exigido somente quando o valor de `XksProxyConnectivity` é `VPC_ENDPOINT_SERVICE`.

> **Note**
>
> Se você usa a versão 1.0 da AWS CLI, execute o comando a seguir antes de especificar um parâmetro com um valor HTTP ou HTTPS, como o parâmetro `XksProxyUriEndpoint`.
>
> ```
> aws configure set cli_follow_urlparam false
> ```
>
> Caso contrário, a versão 1.0 da AWS CLI substitui o valor do parâmetro pelo conteúdo encontrado nesse endereço de URI, causando o seguinte erro:
>
> ```
> Error parsing parameter '--xks-proxy-uri-endpoint': Unable to retrieve
> https:// : received non 200 status code of 404
> ```

Os exemplos a seguir usam valores fictícios. Antes de executar o comando, substitua-os por valores válidos para seu armazenamento de chaves externas.

Crie um armazenamento de chaves externas com conectividade pública de endpoints.

```
$ 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>
```

Crie um armazenamento de chaves externas com conectividade de serviço de endpoint da 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>
```

Quando a operação é bem-sucedida, `CreateCustomKeyStore` retorna o ID do armazenamento de chaves personalizado, conforme exibido na resposta de exemplo a seguir.

```
{
    "CustomKeyStoreId": cks-1234567890abcdef0
}
```

Se a operação falhar, corrija o erro indicado pela exceção e tente novamente. Para obter ajuda adicional, consulte Solução de problemas de armazenamentos de chaves externas.

Próximo: para usar o armazenamento de chaves externas, conecte-o ao proxy do armazenamento de chaves externas.

Editar propriedades do armazenamento de chaves externas

Você pode editar as propriedades selecionadas de um armazenamento de chaves externas existente.

Você pode editar algumas propriedades enquanto o armazenamento de chaves externas está conectado ou desconectado. Para outras propriedades, é necessário primeiro desconectar o armazenamento de chaves externas do proxy de armazenamento de chaves externas. O estado da conexão do armazenamento de chaves externas deve ser `DISCONNECTED`. Enquanto seu armazenamento de chaves externas está desconectado, é possível gerenciar o armazenamento de chaves e suas chaves do KMS, mas não é possível criar nem usar chaves do KMS no armazenamento de chaves externas. Para encontrar o estado da conexão do seu armazenamento de chaves externo, use a DescribeCustomKeyStoresoperação ou consulte a seção Configuração geral na página de detalhes do armazenamento de chaves externo.

Antes de atualizar as propriedades do seu armazenamento de chaves externo, AWS KMS envia uma GetHealthStatussolicitação ao proxy do armazenamento de chaves externo usando os novos valores. Se a solicitação for bem-sucedida, isso indicará que você pode se conectar e se autenticar em um proxy de armazenamento de chaves externas com os valores de propriedade atualizados. Em caso de falha na solicitação, a operação de edição falhará com uma exceção que identifica o erro.

Quando a operação de edição for concluída, os valores atualizados das propriedades do armazenamento de chaves externas serão exibidos no console do AWS KMS e na resposta de `DescribeCustomKeyStores`. No entanto, pode levar até cinco minutos para as alterações entrarem em vigor totalmente.

Ao editar seu armazenamento de chaves externas no console do AWS KMS, você tem a opção de carregar um arquivo de configuração de proxy baseado em JSON que especifica o caminho do URI do proxy e a credencial de autenticação do proxy. Alguns proxies de armazenamento de chaves externas geram esse arquivo para você. Para obter detalhes, consulte a documentação do proxy de armazenamento de chaves externas ou do gerenciador de chaves externas.

> **Warning**
>
> Os valores de propriedade atualizados devem conectar seu armazenamento de chaves externas a um proxy para o mesmo gerenciador de chaves externas dos valores anteriores ou para um backup ou snapshot do gerenciador de chaves externas com as mesmas chaves de criptografia. Se o armazenamento de chaves externas perder o acesso às chaves externas associadas às chaves do KMS permanentemente, o texto cifrado criptografado sob

essas chaves externas será irrecuperável. Especificamente, alterar a conectividade de proxy de um armazenamento de chaves externas pode impedir que o AWS KMS acesse suas chaves externas.

Tip

Alguns gerenciadores de chaves externas fornecem um método mais simples de editar propriedades de armazenamento de chaves externas. Para obter detalhes, consulte a documentação do gerenciador de chaves externas.

Você pode alterar as seguintes propriedades de um armazenamento de chaves externas.

Propriedades editáveis do armazenamento de chaves externas	Qualquer estado da conexão	Exigir estado Disconnected (Desconectado)
Nome do armazenamento de chaves personalizado Um nome amigável obrigatório para um armazenamento de chaves personalizado. **Important** Não inclua informações confidenciais ou sigilosas nesse campo. Esse campo pode ser exibido em texto simples em CloudTrail registros e outras saídas.	✓	
Credencial de autenticação de proxy () XksProxyAuthenticationCredential (É necessário especificar o ID da chave de acesso e a chave de acesso secreta, mesmo que você esteja alterando apenas um elemento.)	✓	

Propriedades editáveis do armazenamento de chaves externas	Qualquer estado da conexão	Exigir estado Disconnected (Desconectado)
Caminho do URI do proxy (XksProxyUriPath)	✓	
Conectividade de proxy (XksProxyConnectivity) (Também é necessário atualizar o endpoint do URI do proxy. Se estiver alterando para a conectividade do serviço de endpoint da VPC, você deverá especificar um nome de serviço de endpoint da VPC do proxy.)		✓
Ponto final do URI do proxy () XksProxyUriEndpoint Se você alterar o URI do endpoint do proxy, talvez também seja necessário alterar o certificado TLS.		✓
Nome do serviço de endpoint VPC proxy () XksProxyVpcEndpointServiceName (Este campo é obrigatório para a conectividade do serviço de endpoint da VPC)		✓

Tópicos

- Editar um armazenamento de chaves externas (console)
- Editar um armazenamento de chaves externas (API)

Editar um armazenamento de chaves externas (console)

Ao editar um armazenamento de chaves, é possível alterar qualquer valor editável. Algumas alterações exigem que o armazenamento de chaves externas seja desconectado do proxy de armazenamento de chaves externas.

Se você estiver editando o caminho do URI do proxy ou a credencial de autenticação do proxy, poderá inserir os novos valores ou carregar um arquivo de configuração de proxy de armazenamento de chaves externas que contenha os novos valores.

1. Faça login no AWS Management Console e abra o console do AWS Key Management Service (AWS KMS) em https://console.aws.amazon.com/kms.
2. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.
3. No painel de navegação, selecione Custom key stores (Armazenamentos de chaves personalizados), External key stores (Armazenamentos de chaves externas).
4. Escolha a linha do armazenamento de chaves externas que deseja editar.
5. Se necessário, desconecte o armazenamento de chaves externas do proxy de armazenamento de chaves externas. No menu Key store actions (Ações do armazenamento de chaves), escolha Disconnect (Desconectar).
6. No menu Key store actions (Ações do armazenamento de chaves), escolha Edit (Editar).
7. Alterar uma ou mais das propriedades editáveis de armazenamento de chaves externas. Você também pode carregar um arquivo de configuração de proxy de armazenamento de chaves externas com valores para o caminho do URI do proxy e a credencial de autenticação do proxy. Você pode usar um arquivo de configuração de proxy mesmo que alguns valores especificados no arquivo não tenham sido alterados.
8. Escolha Update external key store (Atualizar armazenamento de chaves externas).
9. Revise o aviso e, se decidir continuar, confirme o aviso e escolha Update external key store (Atualizar armazenamento de chaves externas).

   Se o procedimento for bem-sucedido, uma mensagem descreverá as propriedades que você editou. Se for malsucedido, será exibida uma mensagem de erro descrevendo o problema e fornecendo ajuda para corrigi-lo.
10. Se necessário, reconecte o armazenamento de chaves externas. No menu Key store actions (Ações do armazenamento de chaves), escolha Connect (Conectar).

    Você pode deixar o armazenamento de chaves externas desconectado. Porém, enquanto estiver desconectado, não será possível criar as chaves do KMS no armazenamento de chaves externas nem usá-las no armazenamento de chaves externas em operações de criptografia.

Editar um armazenamento de chaves externas (API)

Para alterar as propriedades de um armazenamento de chaves externo, use a UpdateCustomKeyStoreoperação. Você pode alterar várias propriedades de um armazenamento de chaves externas na mesma operação. Se a operação tiver êxito, o AWS KMS retornará uma resposta HTTP 200 e um objeto JSON sem propriedades.

Use o parâmetro `CustomKeyStoreId` para identificar o armazenamento de chaves externas. Utilize os outros parâmetros para alterar as propriedades. Você não pode usar um arquivo de configuração de proxy com a operação `UpdateCustomKeyStore`. O arquivo de configuração do proxy é compatível somente com o console do AWS KMS. Contudo, é possível usar o arquivo de configuração do proxy para ajudar você a determinar os valores corretos dos parâmetros para o proxy de armazenamento de chaves externas.

Os exemplos nesta seção usam a AWS Command Line Interface (AWS CLI), mas você pode usar qualquer linguagem de programação compatível.

Antes de começar, se necessário, desconecte o armazenamento de chaves externas do proxy de armazenamento de chaves externas. Após a atualização, se necessário, você pode reconectar o armazenamento de chaves externas ao proxy do armazenamento de chaves externas. Você pode deixar o armazenamento de chaves externas no estado desconectado, mas é necessário reconectá-lo para que seja possível criar novas chaves do KMS no armazenamento de chaves ou usar as chaves do KMS existentes no armazenamento de chaves para operações de criptografia.

> **Note**
>
> Se você usa a versão 1.0 da AWS CLI, execute o comando a seguir antes de especificar um parâmetro com um valor HTTP ou HTTPS, como o parâmetro `XksProxyUriEndpoint`.
>
> ```
> aws configure set cli_follow_urlparam false
> ```
>
> Caso contrário, a versão 1.0 da AWS CLI substitui o valor do parâmetro pelo conteúdo encontrado nesse endereço de URI, causando o seguinte erro:
>
> ```
> Error parsing parameter '--xks-proxy-uri-endpoint': Unable to retrieve
> https:// : received non 200 status code of 404
> ```

Alterar o nome do armazenamento de chaves externas

O primeiro exemplo usa a UpdateCustomKeyStoreoperação para alterar o nome amigável do armazenamento externo de chaves paraXksKeyStore. O comando usa o parâmetro CustomKeyStoreId para identificar o armazenamento de chaves personalizado e CustomKeyStoreName para especificar o novo nome para o armazenamento de chaves personalizado. Substitua todos os valores de exemplo por valores reais para o armazenamento de chaves externas.

```
$ aws kms update-custom-key-store --custom-key-store-id cks-1234567890abcdef0 --new-
custom-key-store-name XksKeyStore
```

Alterar a credencial de autenticação de proxy

O exemplo a seguir atualiza a credencial de autenticação de proxy que o AWS KMS usa para se autenticar no proxy de armazenamento de chaves externas. Você pode usar um comando como este para atualizar a credencial, caso ela seja alternada em seu proxy.

Atualize primeiro a credencial no proxy de armazenamento de chaves externas. Em seguida, use esse recurso para relatar a alteração no AWS KMS. (Seu proxy oferecerá suporte brevemente à credencial antiga e à nova para que você tenha tempo de atualizar a credencial no AWS KMS.)

É necessário sempre especificar o ID da chave de acesso e a chave de acesso secreta na credencial, mesmo que apenas um valor seja alterado.

Os dois primeiros comandos definem as variáveis para manter os valores das credenciais. As operações UpdateCustomKeyStore usam o parâmetro CustomKeyStoreId para identificar o armazenamento de chaves externas. Utiliza o parâmetro XksProxyAuthenticationCredential com os campos AccessKeyId e RawSecretAccessKey para especificar a nova credencial. Substitua todos os valores de exemplo por valores reais para o armazenamento de chaves externas.

```
$ 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
```

Alterar o caminho do URI do proxy

O exemplo a seguir atualiza o caminho do URI do proxy (`XksProxyUriPath`). A combinação do endpoint do URI do proxy e do caminho do URI do proxy deve ser exclusivo na Conta da AWS e na região. Substitua todos os valores de exemplo por valores reais para o armazenamento de chaves externas.

```
$ aws kms update-custom-key-store --custom-key-store-id cks-1234567890abcdef0 \
            --xks-proxy-uri-path /kms/xks/v1
```

Alterar a conectividade do serviço de endpoint da VPC

O exemplo a seguir usa a UpdateCustomKeyStoreoperação para alterar o tipo de conectividade proxy do armazenamento de chaves externo para`VPC_ENDPOINT_SERVICE`. Para fazer essa alteração, é necessário especificar os valores obrigatórios para a conectividade do serviço de endpoint da VPC, inclusive o nome do serviço de endpoint da VPC (`XksProxyVpcEndpointServiceName`) e um valor de endpoint do URI do proxy (`XksProxyUriEndpoint`) que inclua o nome DNS privado do serviço de endpoint da VPC. Substitua todos os valores de exemplo por valores reais para o armazenamento de chaves externas.

```
$ 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
```

Alteração na conectividade de endpoints públicos

O exemplo a seguir altera o tipo de conectividade de proxy de armazenamento de chaves externas para `PUBLIC_ENDPOINT`. Ao fazer essa alteração, é necessário atualizar o valor do endpoint do URI do proxy (`XksProxyUriEndpoint`). Substitua todos os valores de exemplo por valores reais para o armazenamento de chaves externas.

> **Note**
>
> A conectividade de endpoint da VPC oferece maior segurança do que a conectividade de endpoint público. Antes de mudar para a conectividade de endpoint público, considere outras opções, como localizar seu proxy de armazenamento de chaves externas on-premises e usar a VPC somente para comunicação.

```
$ 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
```

Visualizar um armazenamento de chaves externas

Você pode visualizar os armazenamentos externos de chaves em cada conta e região usando o AWS KMS console ou usando a DescribeCustomKeyStoresoperação.

Ao visualizar um armazenamento de chaves externas, você pode ver o seguinte:

- Informações básicas sobre o armazenamento de chaves, inclusive seu nome amigável, ID, tipo de armazenamento de chaves e data de criação.
- Informações de configuração para o proxy de armazenamento de chaves externa, inclusive o tipo de conectividade, o endpoint e o caminho do URI do proxy e o ID da chave de acesso da credencial de autenticação de proxy atual.
- Se o proxy de armazenamento de chaves externas usar a conectividade do serviço de endpoint da VPC, o console exibirá o nome do serviço de endpoint da VPC.
- O estado da conexão atual.

> **Note**
>
> Um valor do estado da conexão Disconnected (Desconectado) indica que o armazenamento de chaves externas nunca foi conectado ou que foi desconectado do proxy do armazenamento de chaves externas intencionalmente. No entanto, se as tentativas de usar uma chave do KMS em um armazenamento de chaves externas conectado falharem, pode ser indício de um problema com o armazenamento de chaves externas ou o proxy. Para obter ajuda, consulte Erros de conexão do armazenamento de chaves externas.

- Uma seção de monitoramento com gráficos das CloudWatch métricas da Amazon projetada para ajudar você a detectar e resolver problemas com seu armazenamento externo de chaves. Para obter ajuda na interpretação dos gráficos, no uso deles no planejamento e na solução de problemas e na criação de CloudWatch alarmes com base nas métricas dos gráficos, consulte. Monitorar um armazenamento de chaves externas

Consulte também:

- Visualizar chaves do KMS em um armazenamento de chaves externas
- Registrando chamadas de AWS KMS API com AWS CloudTrail

Tópicos

- Propriedades do armazenamento de chaves externas
- Visualizar um armazenamento de chaves externas (console)
- Visualizar um armazenamento de chaves externas (API)

Propriedades do armazenamento de chaves externas

As seguintes propriedades de um armazenamento de chaves externo são visíveis no AWS KMS console e na DescribeCustomKeyStoresresposta.

Propriedades do armazenamento de chaves personalizado

Os valores a seguir aparecem na seção General configuration (Configuração geral) da página de detalhes de cada armazenamento de chaves personalizado. Essas propriedades se aplicam a todos os armazenamentos de chaves personalizados, inclusive armazenamentos de chaves do AWS CloudHSM e armazenamentos de chaves externas.

ID do armazenamento de chaves personalizado

Um ID exclusivo que o AWS KMS atribui ao armazenamento de chaves personalizado.

Nome do armazenamento de chaves personalizado

Um nome amigável que você atribui ao armazenamento de chaves personalizado ao criá-lo. Você pode alterar esse valor a qualquer momento.

Tipo do armazenamento de chaves personalizado

O tipo do armazenamento de chaves personalizado. Os valores válidos são AWS CloudHSM (`AWS_CLOUDHSM`) ou External key store (Armazenamento de chaves externas) (`EXTERNAL_KEY_STORE`). Você não pode alterar o tipo depois de criar o armazenamento de chaves personalizado.

Data de Criação

A data em que o armazenamento de chaves personalizado foi criado. Essa data é exibida na hora local da Região da AWS.

Estado da conexão

Indica se o armazenamento de chaves personalizado está conectado a seu armazenamento de chaves de reserva. O estado da conexão será `DISCONNECTED` somente se o armazenamento de chaves personalizado nunca tiver sido conectado ao armazenamento de chaves de reserva ou se tiver sido desconectado intencionalmente. Para obter detalhes, consulte the section called “Estado da conexão”.

Propriedades de configuração do armazenamento de chaves externas

Os valores a seguir aparecem na seção Configuração de proxy do armazenamento de chaves externo da página de detalhes de cada armazenamento de chaves externo e no `XksProxyConfiguration` elemento da DescribeCustomKeyStoresresposta. Para obter uma descrição detalhada de cada campo, inclusive requisitos de exclusividade e ajuda para determinar o valor correto para cada campo, consulte the section called “Organizar os pré-requisitos” no tópico Criar um armazenamento de chaves externas.

Conectividade do proxy

Indica se o armazenamento de chaves externas usa conectividade de endpoint público ou conectividade de serviço de endpoint da VPC.

Endpoint de URI do proxy

O endpoint que o AWS KMS usa para se comunicar com o proxy de armazenamento de chaves externas.

Caminho do URI do proxy

O caminho do endpoint do URI do proxy para o qual o AWS KMS envia as solicitações da API de proxy.

Credencial de proxy: ID da chave de acesso

Parte da credencial de autenticação de proxy que você estabelece em seu proxy de armazenamento de chaves externas. O ID da chave de acesso identifica a chave de acesso secreta na credencial.

O AWS KMS usa o processo de assinatura SigV4 e a credencial de autenticação de proxy para assinar suas solicitações no proxy de armazenamento de chaves externas. A credencial na assinatura permite que o proxy de armazenamento de chaves externas autentique solicitações do AWS KMS em seu nome.

Nome do serviço de endpoint da VPC

O nome do serviço de endpoint da Amazon VPC que oferece suporte ao armazenamento de chaves externas. Esse valor é exibido somente quando o armazenamento de chaves externas usa a conectividade de serviço de endpoint da VPC. Você pode localizar o proxy de armazenamento de chaves externas na VPC ou usar o serviço de endpoint da VPC para se comunicar de forma segura com o proxy de armazenamento de chaves externas.

Visualizar um armazenamento de chaves externas (console)

Para visualizar armazenamentos de chaves externas em uma determinada conta e região, use o procedimento a seguir.

1. Faça login no AWS Management Console e abra o console do AWS Key Management Service (AWS KMS) em https://console.aws.amazon.com/kms.
2. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.
3. No painel de navegação, selecione Custom key stores (Armazenamentos de chaves personalizados), External key stores (Armazenamentos de chaves externas).
4. Para exibir informações detalhadas sobre um armazenamento de chaves externas, escolha o nome do armazenamento de chaves.

Visualizar um armazenamento de chaves externas (API)

Para visualizar seus armazenamentos externos de chaves, use a DescribeCustomKeyStoresoperação. Por padrão, essa operação retorna todos os armazenamentos de chaves personalizados na conta e região. No entanto, você pode usar o parâmetro `CustomKeyStoreId` ou `CustomKeyStoreName` (mas não ambos) para limitar o resultado para um determinado armazenamento de chaves personalizado.

Para armazenamentos de chaves personalizados, a saída consiste no ID, nome e tipo do armazenamento de chaves personalizado e no estado da conexão do armazenamento de chaves. Se o estado da conexão é `FAILED`, o resultado também inclui um `ConnectionErrorCode` que descreve o motivo do erro. Para obter ajuda para interpretar `ConnectionErrorCode` para um armazenamento de chaves externas, consulte Códigos de erro de conexão para armazenamentos de chaves externas.

Para armazenamentos de chaves externas, a saída também inclui o elemento `XksProxyConfiguration`. Esse elemento inclui o tipo de conectividade, o endpoint do URI do

proxy, o caminho do URI do proxy e o ID da chave de acesso da credencial de autenticação do proxy.

Os exemplos nesta seção usam a AWS Command Line Interface (AWS CLI), mas você pode usar qualquer linguagem de programação compatível.

Por exemplo, o comando a seguir retorna todos os armazenamentos de chaves personalizados na conta e região. Você pode usar os parâmetros `Marker` e `Limit` para percorrer os armazenamentos de chaves personalizados do resultado.

```
$ aws kms describe-custom-key-stores
```

O comando a seguir usa o parâmetro `CustomKeyStoreName` para obter apenas o armazenamento de chaves externas de exemplo com o nome amigável `ExampleXksPublic`. Este exemplo de armazenamento de chaves usa conectividade pública de endpoint. Está conectado ao proxy de armazenamento de chaves externas.

```
$ 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"
      }
    }
  ]
}
```

O comando a seguir obtém um exemplo de armazenamento de chaves externas com conectividade de serviço de endpoint da VPC. Neste exemplo, o armazenamento de chaves externas está conectado ao proxy de armazenamento de chaves externas.

```
$ 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"
      }
    }
  ]
}
```

O `ConnectionState` `Disconnected` indica que um armazenamento de chaves externas nunca foi conectado ou foi intencionalmente desconectado do proxy de armazenamento de chaves externas. No entanto, se as tentativas de usar uma chave do KMS em um armazenamento de chaves externas conectado falharem, pode ser indício de um problema com o proxy de armazenamento de chaves externas ou outros componentes externos.

Quando o `ConnectionState` do armazenamento de chaves externas `FAILED`, a resposta `DescribeCustomKeyStores` inclui um elemento `ConnectionErrorCode` que explica o motivo desse erro.

Por exemplo, na saída a seguir, o valor `XKS_PROXY_TIMED_OUT` indica que o AWS KMS pode se conectar ao proxy de armazenamento de chaves externas, mas a conexão falhou porque o proxy de armazenamento de chaves externas não respondeu ao AWS KMS no tempo estipulado. Caso veja esse código de erro de conexão repetidamente, notifique seu fornecedor de proxy de armazenamento de chaves externas. Para obter ajuda com relação a esta e outras falhas de erro de conexão, consulte Solução de problemas de armazenamentos de chaves externas.

```
$ 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"
      }
    }
  ]
}
```

Monitorar um armazenamento de chaves externas

AWS KMScoleta métricas para cada interação com um armazenamento de chaves externo e as publica em sua CloudWatch conta. Essas métricas são usadas para gerar os grafos na seção de monitoramento da página de detalhes de cada armazenamento de chaves externas. O tópico a seguir detalha como usar os grafos para identificar e solucionar problemas operacionais e de configuração que afetam o armazenamento de chaves externas. Recomendamos usar as CloudWatch métricas para definir alarmes que notifiquem você quando seu armazenamento externo de chaves não estiver funcionando conforme o esperado. Para obter mais informações, consulte Monitoramento com a Amazon CloudWatch.

Tópicos

- Visualizar os grafos
- Interpretar os grafos
- Definir alarmes

Visualizar os grafos

Você pode visualizar os grafos em diferentes níveis de detalhes. Por padrão, cada grafo usa um intervalo de três horas e um período de agregação de cinco minutos. Você pode ajustar a visualização do grafo no console, mas suas alterações serão revertidas para as configurações padrão quando a página de detalhes do armazenamento de chaves externas for fechada ou quando

o navegador for atualizado. Para obter ajuda com a CloudWatch terminologia da Amazon, consulte os CloudWatch conceitos da Amazon.

Visualizar detalhes do ponto de dados

Os dados de cada grafo são coletados por métricas do AWS KMS. Para visualizar mais informações sobre um ponto de dados específico, pause o mouse sobre o ponto de dados no grafo linha. Isso exibirá um pop-up com mais informações sobre a métrica da qual o grafo foi derivado. Cada item da lista exibe o valor de dimensão registrado no ponto de dados. O pop-up exibirá um valor nulo (–) se não houver dados métricos disponíveis para o valor da dimensão no ponto de dados. Alguns grafos registram várias dimensões e valores para um único ponto de dados. Outros grafos, como o grafo de confiabilidade, usam os dados coletados pela métrica para calcular um valor exclusivo. Cada item da lista é associado a uma cor de grafo linha diferente.

Modificar o intervalo de tempo

Para alterar o intervalo de tempo, selecione um dos intervalos de tempo predefinidos no canto superior direito da seção de monitoramento. Os intervalos de tempo predefinidos variam de uma hora a uma semana (1h, 3h, 12h, 1d, 3d ou 1w). Isso ajusta o intervalo de tempo para todos os grafos. Se você quiser visualizar um gráfico específico em um intervalo de tempo diferente, ou se quiser definir um intervalo de tempo personalizado, amplie o gráfico ou visualize-o no CloudWatch console da Amazon.

Ampliar grafos

Você pode usar o recurso de zoom de minimapa para focar em seções de grafos linhas e grafos de área empilhada sem alterações entre as visualizações com zoom aumentado e zoom diminuído. Por exemplo, é possível usar o recurso de zoom de minimapa para focar em um pico em um grafo linha para comparar o pico com outras métricas no painel usando a mesma linha do tempo.

1. Escolha e arraste a área do gráfico em que deseja focar e, em seguida, solte-a.
2. Para redefinir o zoom, escolha o ícone Redefinir zoom igual a uma lupa com um símbolo de menos (-) no interior.

Ampliar um grafo

Para ampliar um grafo, selecione o ícone de menu no canto superior direito de um grafo individual e escolha Enlarge (Ampliar). Você também pode selecionar o ícone de ampliação exibido ao lado do ícone de menu ao passar o mouse sobre um grafo.

Ampliar um grafo permite modificar ainda mais a visualização de um grafo especificando um período diferente, um intervalo de tempo personalizado ou um intervalo de atualização. Essas alterações serão revertidas para as configurações padrão quando você fechar a visualização ampliada.

Modificar o período

1. Escolha o menu Period options (Opções do período). Por padrão, esse menu exibe o valor: 5 minutes (5 minutos).
2. Escolha um período, os períodos predefinidos variam de um segundo a 30 dias.

   Por exemplo, escolha uma exibição de um minuto, que pode ser útil durante a solução de problemas. Ou escolha uma visualização menos detalhada de uma hora. Isso pode ser útil ao visualizar um intervalo de tempo mais amplo (por exemplo, 3 dias) para que possa ver tendências ao longo do tempo. Para obter mais informações, consulte Períodos no Guia CloudWatch do usuário da Amazon.

Modificar o intervalo de tempo ou fuso horário

1. Selecione um dos intervalos de tempo predefinidos, que variam de uma hora a uma semana: (1h, 3h, 12h, 1d, 3d ou 1w). Como alternativa, você pode escolher Custom (Personalizado) para definir seu próprio intervalo de tempo.
2. Escolha Custom (Personalizado)

   a. Intervalo de tempo: selecione a guia Absolute (Absoluto) no canto superior esquerdo da caixa. Use o seletor de calendário ou as caixas de campos de texto para especificar um intervalo de tempo.

   b. Fuso horário: escolha a lista suspensa no canto superior direito da caixa. Você pode alterar o fuso horário para UTC ou Local time zone (Fuso horário local).
3. Depois de especificar um período, escolha Apply (Aplicar).

Modifique a frequência com que os dados do grafo serão atualizados

1. No canto superior direito, escolha o menu Refresh options (Opções de atualização).
2. Escolha um intervalo de atualização: Off (Desligado), 10 Seconds (10 segundos), 1 Minute (1 minuto), 2 Minutes (2 minutos), 5 Minutes (5 minutos) ou 15 Minutes (15 minutos).

Visualize gráficos no console da Amazon CloudWatch

Os gráficos na seção de monitoramento são derivados de métricas predefinidas que são AWS KMS publicadas na Amazon. CloudWatch Você pode abri-los no CloudWatch console e salvá-los nos CloudWatch painéis. Se você tiver vários armazenamentos de chaves externos, poderá abrir seus respectivos gráficos CloudWatch e salvá-los em um único painel para comparar sua integridade e uso.

Adicionar ao CloudWatch painel

Selecione Adicionar ao painel no canto superior direito para adicionar todos os gráficos a um CloudWatch painel da Amazon. Você pode selecionar um painel existente ou criar outro. Para obter informações sobre como usar esse painel para criar visualizações personalizadas dos gráficos e alarmes, consulte Usando CloudWatchpainéis da Amazon no Guia do usuário da Amazon CloudWatch .

Exibir nas CloudWatch métricas

Selecione o ícone do menu no canto superior direito de um gráfico individual e escolha Exibir em métricas para visualizar esse gráfico no CloudWatch console da Amazon. No CloudWatch console, você pode adicionar esse único gráfico a um painel e modificar intervalos de tempo, períodos e intervalos de atualização. Para obter mais informações, consulte Representação gráfica de métricas no Guia do CloudWatch usuário da Amazon.

Interpretar os grafos

O AWS KMS fornece vários grafos para monitorar a integridade do armazenamento de chaves externas no console do AWS KMS. Esses grafos são configurados automaticamente e derivados de métricas do AWS KMS.

Os dados de grafos são coletados como parte das chamadas que você faz para o armazenamento de chaves externas e chaves externas. É possível ver grafos de preenchimento de dados durante um intervalo de tempo em que você não fez nenhuma chamada. Esses dados vêm das chamadas `GetHealthStatus` periódicas que o AWS KMS faz em seu nome para verificar o status do proxy de armazenamento de chaves externas e do gerenciador de chaves externas. Se os grafos exibirem a mensagem No data available (Nenhum dado disponível), não houve chamadas gravadas durante esse intervalo de tempo ou o armazenamento de chaves externas está no estado `DISCONNECTED`. Talvez você consiga identificar a hora em que o armazenamento de chaves externas foi desconectado ajustando a visualização para um intervalo de tempo mais amplo.

Tópicos

- Total requests
- Confiabilidade
- Latência
- As cinco principais exceções
- Dias para o certificado expirar

Total requests

O número total de solicitações do AWS KMS recebidas para um armazenamento de chaves externas específico durante um intervalo de tempo específico. Use esse grafo para determinar se você corre o risco de controle de utilização.

O AWS KMS recomenda que o gerenciador de chaves externas seja capaz de lidar com até 1.800 solicitações de operações de criptografia por segundo. Se você abordar 540 mil chamadas em um período de cinco minutos, correrá o risco de controle de utilização.

Você pode monitorar o número de solicitações de operações de criptografia em chaves do KMS em seu armazenamento de chaves externas que o AWS KMS restringe com a métrica ExternalKeyStoreThrottle.

Se você estiver recebendo erros `KMSInvalidStateException` muito frequentes com uma mensagem explicando que a solicitação foi rejeitada “due to a very high request rate” [devido a uma taxa de solicitação muito alta], isso pode indicar que o gerenciador de chaves externas ou o proxy de armazenamento de chaves externas não consegue acompanhar a taxa de solicitação atual. Se possível, reduza a taxa de solicitação. Considere também solicitar uma redução no valor da cota de solicitação de armazenamento de chaves personalizado. Diminuir esse valor de cota poderá aumentar o controle de utilização, mas indica que o AWS KMS está rejeitando solicitações em excesso rapidamente antes de serem enviadas ao proxy de armazenamento de chaves externas ou ao gerenciador de chaves externas. Para solicitar uma redução de cota, acesse o AWS Support Center e crie um caso.

O grafo do total de solicitações é derivado da métrica XksProxyErrors, que coleta dados sobre as respostas bem-sucedidas e malsucedidas que o AWS KMS recebe de seu proxy de armazenamento de chaves externas. Quando você visualiza um ponto de dados específico, o pop-up exibe o valor da dimensão `CustomKeyStoreId` junto com o número total de solicitações do AWS KMS registradas nesse ponto de dados. `CustomKeyStoreId` será sempre o mesmo.

Confiabilidade

A porcentagem de solicitações do AWS KMS para as quais o proxy do armazenamento de chaves externas retornou uma resposta bem-sucedida ou um erro sem nova tentativa. Use esse grafo para avaliar a integridade operacional do proxy de armazenamento de chaves externas.

Ao exibir um valor menor que 100%, o grafo indica casos em que o proxy não respondeu ou respondeu com um erro com nova tentativa. Isso pode indicar problemas com a rede, lentidão do proxy de armazenamento de chaves externas ou do gerenciador de chaves externas ou bugs de implementação.

Se a solicitação incluir uma credencial inválida e seu proxy responder com `AuthenticationFailedException`, o grafo ainda indicará 100% de confiabilidade porque o proxy identificou um valor incorreto na solicitação da API do proxy de armazenamento de chaves externas e, portanto, a falha é esperada. Se a porcentagem do grafo de confiabilidade for de 100%, o proxy de armazenamento de chaves externas estará respondendo conforme o esperado. Se o grafo exibir um valor menor que 100%, o proxy respondeu com um erro com nova tentativa ou atingiu o tempo limite. Por exemplo, se o proxy responder com `ThrottlingException` devido a uma taxa de solicitação muito alta, ele exibirá uma porcentagem de confiabilidade menor porque o proxy não conseguiu identificar um problema específico na solicitação que causou a falha. Isso ocorre porque os erros com nova tentativa provavelmente são problemas transitórios que podem ser resolvidos ao repetir a solicitação.

As respostas de erro a seguir reduzirão a porcentagem de confiabilidade. Você pode usar o grafo As cinco principais exceções e a métrica XksProxyErrors para monitorar ainda mais a frequência com que seu proxy retorna cada erro com nova tentativa.

- `InternalException`
- `DependencyTimeoutException`
- `ThrottlingException`
- `XksProxyUnreachableException`

O grafo de confiabilidade é derivado da métrica XksProxyErrors, que coleta dados sobre as respostas bem-sucedidas e malsucedidas que o AWS KMS recebe de seu proxy de armazenamento de chaves externas. A porcentagem de confiabilidade só diminuirá se a resposta tiver um valor `ErrorType` de `Retryable`. Quando você visualiza um ponto de dados específico, o pop-up exibe o valor da dimensão `CustomKeyStoreId` junto com o percentual de confiabilidade do AWS KMS registrados nesse ponto de dados. `CustomKeyStoreId` será sempre o mesmo.

Recomendamos usar a XksProxyErrors métrica para criar um CloudWatch alarme que notifique você sobre possíveis problemas de rede, alertando-o quando mais de cinco erros repetidos forem registrados em um período de um minuto. Para ter mais informações, consulte Criação de um CloudWatch alarme da Amazon para erros que podem ser repetidos.

Latência

O número de milissegundos necessários para que um proxy de armazenamento de chaves externas responda a uma solicitação do AWS KMS. Use esse grafo para avaliar a performance do proxy de armazenamento de chaves externas e do gerenciador de chaves externas.

O AWS KMS espera que o proxy do armazenamento de chaves externas responda a cada solicitação em até 250 milissegundos. No caso de tempos limite de rede, o AWS KMS repetirá a solicitação uma vez. Se o proxy falhar pela segunda vez, a latência registrada será o limite de tempo limite combinado para as duas tentativas de solicitação, e o grafo exibirá aproximadamente 500 milissegundos. Em todos os outros casos em que o proxy não responder dentro do tempo limite de 250 milissegundos, a latência registrada será de 250 milissegundos. Se o proxy estiver frequentemente atingindo o tempo limite nas operações de criptografia e descriptografia, consulte seu administrador do proxy externo. Para obter ajuda na solução de problemas de latência, consulte Erros de latência e de tempo limite.

Respostas lentas também podem indicar que seu gerenciador de chaves externas não consegue lidar com o tráfego de solicitações atual. O AWS KMS recomenda que seu gerenciador de chaves externas seja capaz de lidar com até 1.800 solicitações de operações de criptografia por segundo. Se o gerenciador de chaves externas não conseguir lidar com a taxa de 1800 solicitações por segundo, considere solicitar uma redução na cota de solicitações de chaves do KMS em um armazenamento de chaves personalizado. As solicitações de operações de criptografia que usam as chaves do KMS em seu armazenamento de chaves externas se anteciparão à falha com uma exceção de controle de utilização, em vez de serem processadas e posteriormente rejeitadas pelo proxy de armazenamento de chaves externas ou pelo gerenciador de chaves externas.

O grafo de latência é derivado da métrica XksProxyLatency. Quando você visualiza um ponto de dados específico, o pop-up exibe os valores correspondentes de dimensão `KmsOperation` e `XksOperation` junto com a latência média registrada para as operações no ponto de dados. Os itens da lista são ordenados da maior para a menor latência.

Recomendamos usar a XksProxyLatency métrica para criar um CloudWatch alarme que notifique você quando sua latência estiver se aproximando do limite de tempo limite. Para ter mais

informações, consulte Criação de um CloudWatch alarme da Amazon para o tempo limite de resposta.

As cinco principais exceções

As cinco principais exceções para falhas nas operações de criptografia e de gerenciamento durante um intervalo de tempo específico. Use esse grafo para rastrear os erros mais frequentes e poder priorizar seus esforços de engenharia.

Essa contagem inclui as exceções que o AWS KMS recebeu do proxy de armazenamento de chaves externas e a `XksProxyUnreachableException` que o AWS KMS retorna internamente quando não consegue estabelecer comunicação com o proxy de armazenamento de chaves externas.

Altas taxas de erros com nova tentativa podem indicar erros de redes, enquanto altas taxas de erros sem nova tentativa podem indicar um problema com a configuração do armazenamento de chaves externas. Por exemplo, um pico de entrada em `AuthenticationFailedExceptions` indica uma discrepância entre as credenciais de autenticação configuradas no AWS KMS e o proxy de armazenamento de chaves externas. Para visualizar a configuração do armazenamento de chaves externas, consulte Visualizar um armazenamento de chaves externas. Para editar suas configurações de armazenamento de chaves externas, consulte Editar propriedades do armazenamento de chaves externas.

As exceções que o AWS KMS recebe do proxy de armazenamento de chaves externas são diferentes das exceções que o AWS KMS retorna quando uma operação falha. As operações criptográficas do AWS KMS retornam uma `KMSInvalidStateException` para todas as falhas relacionadas à configuração externa ou ao estado de conexão do armazenamento de chaves externas. Para identificar o problema, use o texto da mensagem de erro que o acompanha.

A tabela a seguir mostra as exceções que podem aparecer no grafo das cinco principais exceções e as exceções correspondentes que o AWS KMS retorna para você.

Tipo de erro	Exceção exibida no grafo	Exceção que o AWS KMS retornou para você
Sem nova tentativa	**`AccessDeniedException`** Para obter ajuda sobre a solução de problemas	**`CustomKeyStoreInvalidStateException`** em resposta às operações `CreateKey` .

Tipo de erro	Exceção exibida no grafo	Exceção que o AWS KMS retornou para você
	, consulte Problemas de autorização de proxy.	**`KMSInvalidStateException`** em resposta às operações de criptografia.
Sem nova tentativa	**`AuthenticationFailedException`** Para obter ajuda sobre a solução de problemas, consulte Erros de credenciais de autenticação.	**`XksProxyIncorrectAuthenticationCredentialException`** em resposta às operações `CreateCustomKeyStore` e `UpdateCustomKeyStore` . **`CustomKeyStoreInvalidStateException`** em resposta às operações `CreateKey` . **`KMSInvalidStateException`** em resposta às operações de criptografia.

Tipo de erro	Exceção exibida no grafo	Exceção que o AWS KMS retornou para você
Com nova tentativa	**`DependencyTimeoutException`** Para obter ajuda sobre a solução de problemas, consulte Erros de latência e de tempo limite.	**`XksProxyUriUnreachableException`** em resposta às operações `CreateCustomKeyStore` e `UpdateCustomKeyStore` . **`CustomKeyStoreInvalidStateException`** em resposta às operações `CreateKey` . **`KMSInvalidStateException`** em resposta às operações de criptografia.
Com nova tentativa	**`InternalException`** O proxy de armazenamento de chaves externas rejeitou a solicitação porque não consegue se comunicar com o gerenciador de chaves externas. Verifique se a configuração do proxy do armazenamento de chaves externas está correta e se o gerenciador de chaves externas está disponível.	**`XksProxyInvalidResponseException`** em resposta às operações `CreateCustomKeyStore` e `UpdateCustomKeyStore` . **`CustomKeyStoreInvalidStateException`** em resposta às operações `CreateKey` . **`KMSInvalidStateException`** em resposta às operações de criptografia.

Tipo de erro	Exceção exibida no grafo	Exceção que o AWS KMS retornou para você
Sem nova tentativa	**`InvalidCiphertextException`** Para obter ajuda sobre a solução de problemas, consulte Erros de descriptografia.	**`KMSInvalidStateException`** em resposta às operações de criptografia.
Sem nova tentativa	**`InvalidKeyUsageException`** Para obter ajuda sobre a solução de problemas, consulte Erros de operação de criptografia da chave externa.	**`XksKeyInvalidConfigurationException`** em resposta às operações `CreateKey` . **`KMSInvalidStateException`** em resposta às operações de criptografia.
Sem nova tentativa	**`InvalidStateException`** Para obter ajuda sobre a solução de problemas, consulte Erros de operação de criptografia da chave externa.	**`XksKeyInvalidConfigurationException`** em resposta às operações `CreateKey` . **`KMSInvalidStateException`** em resposta às operações de criptografia.

Tipo de erro	Exceção exibida no grafo	Exceção que o AWS KMS retornou para você
Sem nova tentativa	**`InvalidUriPathException`** Para obter ajuda sobre a solução de problemas, consulte Erros gerais de configuração.	**`XksProxyInvalidConfigurationException`** em resposta às operações `CreateCustomKeyStore` e `UpdateCustomKeyStore`. **`CustomKeyStoreInvalidStateException`** em resposta às operações `CreateKey`. **`KMSInvalidStateException`** em resposta às operações de criptografia.
Sem nova tentativa	**`KeyNotFoundException`** Para obter ajuda sobre a solução de problemas, consulte Erros de chave externa.	**`XksKeyNotFoundException`** em resposta às operações `CreateKey`. **`KMSInvalidStateException`** em resposta às operações de criptografia.

Tipo de erro	Exceção exibida no grafo	Exceção que o AWS KMS retornou para você
Com nova tentativa	**`ThrottlingException`** O proxy de armazenamento de chaves externas rejeitou a solicitação devido a uma taxa de solicitação muito alta. Reduza a frequência de suas chamadas usando chaves do KMS neste armazenamento de chaves externas.	**`XksProxyUriUnreachableException`** em resposta às operações `CreateCustomKeyStore` e `UpdateCustomKeyStore` . **`CustomKeyStoreInvalidStateException`** em resposta às operações `CreateKey` . **`KMSInvalidStateException`** em resposta às operações de criptografia.
Sem nova tentativa	**`UnsupportedOperationException`** Para obter ajuda sobre a solução de problemas, consulte Erros de operação de criptografia da chave externa.	**`XksKeyInvalidResponseException`** em resposta às operações `CreateKey` . **`KMSInvalidStateException`** em resposta às operações de criptografia.

Tipo de erro	Exceção exibida no grafo	Exceção que o AWS KMS retornou para você
Sem nova tentativa	**`ValidationException`** Para obter ajuda sobre a solução de problemas, consulte Problemas de proxy.	**`XksProxyInvalidResponseException`** em resposta às operações `CreateCustomKeyStore` e `UpdateCustomKeyStore` . **`CustomKeyStoreInvalidStateException`** em resposta às operações `CreateKey` . **`KMSInvalidStateException`** em resposta às operações de criptografia.
Com nova tentativa	**`XksProxyUnreachableException`** Caso veja esse erro repetidamente, verifique se o proxy de armazenamento de chaves externas está ativo e conectado à rede e se o caminho do URI e o URI do endpoint ou o nome do serviço da VPC estão corretos no armazenamento de chaves externas.	**`XksProxyUriUnreachableException`** em resposta às operações `CreateCustomKeyStore` e `UpdateCustomKeyStore` . **`CustomKeyStoreInvalidStateException`** em resposta às operações `CreateKey` . **`KMSInvalidStateException`** em resposta às operações de criptografia.

O grafo das cinco principais exceções é derivado da métrica XksProxyErrors. Quando você visualiza um ponto de dados específico, o pop-up exibe o valor da dimensão `ExceptionName` junto com

o número de vezes que a exceção foi registrada no ponto de dados. Os cinco itens da lista são ordenados da exceção mais frequente para a menos frequente.

Recomendamos usar a XksProxyErrors métrica para criar um CloudWatch alarme que notifique você sobre possíveis problemas de configuração, alertando-o quando mais de cinco erros que não podem ser repetidos forem registrados em um período de um minuto. Para ter mais informações, consulte Criação de um CloudWatch alarme da Amazon para erros que não podem ser repetidos.

Dias para o certificado expirar

O número de dias até o certificado TLS do endpoint do proxy de armazenamento de chaves externas (`XksProxyUriEndpoint`) expirar. Use esse grafo para monitorar a próxima expiração de seu certificado TLS.

Quando o certificado expira, o AWS KMS não consegue se comunicar com o proxy de armazenamento de chaves externas. Todos os dados protegidos por chaves do KMS em seu armazenamento de chaves externas ficarão inacessíveis até você renovar o certificado.

O grafo de dias até a expiração do certificado é derivado da métrica XksProxyCertificateDaysToExpire. É altamente recomendável usar essa métrica para criar um CloudWatch alarme que o notifique sobre o vencimento futuro. A expiração do certificado pode impedir que você acesse os recursos criptografados. Defina o alarme para dar tempo para a sua organização renovar o certificado antes que ele expire. Para ter mais informações, consulte Criação de um CloudWatch alarme da Amazon para expiração do certificado.

Definir alarmes

Os grafos na seção de monitoramento fornecem uma visão geral da integridade de seus armazenamentos de chaves externas e das chaves do KMS em armazenamentos de chaves externas por um período determinado. No entanto, você pode criar CloudWatch alarmes da Amazon com base em métricas externas de armazenamento de chaves para notificá-lo quando um valor de métrica exceder um limite especificado por você. O alarme pode enviar a mensagem para um tópico do Amazon Simple Notification Service (Amazon SNS) ou uma política do Amazon EC2 Auto Scaling. Para obter informações detalhadas sobre CloudWatch alarmes, consulte Como usar CloudWatch alarmes da Amazon no Guia CloudWatch do usuário da Amazon.

Antes de criar um CloudWatch alarme da Amazon, você precisa de um tópico do Amazon SNS. Para obter detalhes, consulte o tópico Criação de um Amazon SNS no Guia CloudWatch do usuário da Amazon.

Tópicos

- Criação de um CloudWatch alarme da Amazon para expiração do certificado
- Criação de um CloudWatch alarme da Amazon para o tempo limite de resposta
- Criação de um CloudWatch alarme da Amazon para erros que podem ser repetidos
- Criação de um CloudWatch alarme da Amazon para erros que não podem ser repetidos

Criação de um CloudWatch alarme da Amazon para expiração do certificado

Esse alarme usa a XksProxyCertificateDaysToExpire métrica AWS KMS publicada para registrar CloudWatch a expiração prevista do certificado TLS associado ao seu endpoint proxy externo de armazenamento de chaves. Você pode criar um alarme único para todos os armazenamentos de chaves externas de sua conta ou um alarme para armazenamentos de chaves externas que você possa criar futuramente.

Recomendamos configurar o alarme para alertar você dez dias antes do prazo de validade do certificado, mas você deve definir o limite que melhor atenda às suas necessidades.

Criar o alarme

Siga as instruções em Criar um CloudWatch alarme com base em um limite estático usando os seguintes valores obrigatórios. Para outros campos, aceite os valores padrão e forneça os nomes conforme solicitado.

Campo	Valor
Selecionar métrica	Escolha KMS e escolha XKS Proxy Certificate Metrics (Métricas de certificado do proxy XKS). Marque a caixa de seleção ao lado da `XksProxyCertificateName` que você deseja monitorar. Depois, escolha Select metric (Selecionar métrica).
Estatística	Mínimo
Período	5 minutos
Tipo de limite	Estático

Campo	Valor
Sempre que…	Sempre que XksProxyCertificateDaysToExpirefor `Lower` do que`10`.

Criação de um CloudWatch alarme da Amazon para o tempo limite de resposta

Esse alarme usa a XksProxyLatency métrica que AWS KMS publica CloudWatch para registrar o número de milissegundos necessários para que um proxy externo de armazenamento de chaves responda a uma AWS KMS solicitação. Você pode criar um alarme único para todos os armazenamentos de chaves externas de sua conta ou um alarme para armazenamentos de chaves externas que você possa criar futuramente.

O AWS KMS espera que o proxy do armazenamento de chaves externas responda a cada solicitação em até 250 milissegundos. Recomendamos configurar um alarme para alertar você quando o proxy de armazenamento de chaves externas levar mais de 200 milissegundos para responder, mas você deve definir o limite que melhor atenda às suas necessidades.

Criar o alarme

Siga as instruções em Criar um CloudWatch alarme com base em um limite estático usando os seguintes valores obrigatórios. Para outros campos, aceite os valores padrão e forneça os nomes conforme solicitado.

Campo	Valor
Selecionar métrica	Escolha KMS e escolha XKS Proxy Latency Metrics (Métricas de latência do proxy XKS). Marque a caixa de seleção ao lado da `KmsOperation` que você deseja monitorar. Depois, escolha Select metric (Selecionar métrica).
Estatística	Média
Período	5 minutos
Tipo de limite	Estático

Campo	Valor
Sempre que…	Sempre que XksProxyLatencyfor `Greater` do que`200`.

Criação de um CloudWatch alarme da Amazon para erros que podem ser repetidos

Esse alarme usa a XksProxyErrors métrica que AWS KMS publica CloudWatch para registrar o número de exceções relacionadas às AWS KMS solicitações ao proxy externo do armazenamento de chaves. Você pode criar um alarme único para todos os armazenamentos de chaves externas de sua conta ou um alarme para armazenamentos de chaves externas que você possa criar futuramente.

Erros com nova tentativa diminuirão sua porcentagem de confiabilidade e podem indicar erros de redes. Recomendamos configurar um alarme para alertar você quando mais de cinco erros com nova tentativa forem registrados em um período de um minuto, mas você deve definir o limite que atenda melhor às suas necessidades.

Siga as instruções em Criar um CloudWatch alarme com base em um limite estático usando os seguintes valores obrigatórios. Para outros campos, aceite os valores padrão e forneça os nomes conforme solicitado.

Campo	Valor
Selecionar métrica	Escolha a guia Queries (Consultas). Escolha `AWS/KMS` para Namespace. Insira `SUM(XksProxyErrors)` em Metric name (Nome da métrica). Insira `ErrorType = Retryable` em Filter by (Filtrar por). Escolha Executar. Depois, escolha Select metric (Selecionar métrica).
Rótulo	*Erros com nova tentativa*
Período	1 minuto
Tipo de limite	Estático
Sempre que…	Sempre que q1 for `Greater` que `5`.

Criação de um CloudWatch alarme da Amazon para erros que não podem ser repetidos

Esse alarme usa a XksProxyErrors métrica que AWS KMS publica CloudWatch para registrar o número de exceções relacionadas às AWS KMS solicitações ao proxy externo do armazenamento de chaves. Você pode criar um alarme único para todos os armazenamentos de chaves externas de sua conta ou um alarme para armazenamentos de chaves externas que você possa criar futuramente.

Erros sem nova tentativa podem indicar um problema com a configuração do armazenamento de chaves externas. Recomendamos configurar um alarme para alertar você quando mais de cinco erros sem nova tentativa forem registrados em um período de um minuto, mas você deve definir o limite que atenda melhor a suas necessidades.

Siga as instruções em Criar um CloudWatch alarme com base em um limite estático usando os seguintes valores obrigatórios. Para outros campos, aceite os valores padrão e forneça os nomes conforme solicitado.

Campo	Valor
Selecionar métrica	Escolha a guia Queries (Consultas). Escolha `AWS/KMS` para Namespace. Insira `SUM(XksProxyErrors)` em Metric name (Nome da métrica). Insira `ErrorType = Non-retryable` em Filter by (Filtrar por). Escolha Executar. Depois, escolha Select metric (Selecionar métrica).
Rótulo	*Erros sem nova tentativa*
Período	1 minuto
Tipo de limite	Estático
Sempre que…	Sempre que `q1` for `Greater` que `5`.

Conectar e desconectar um armazenamento de chaves externas

Os novos armazenamentos de chaves externas não são conectados. Para criar e usar AWS KMS keys em seu armazenamento de chaves externas, é necessário conectar o armazenamento

de chaves externas ao proxy de armazenamento de chaves externas. Você pode conectar e desconectar seu armazenamento de chaves externas a qualquer momento, e visualizar seu estado de conexão.

Enquanto o armazenamento de chaves externas estiver desconectado, o AWS KMS não poderá se comunicar com o proxy de armazenamento de chaves externas. Como resultado, você poderá visualizar e gerenciar o armazenamento de chaves externas e suas chaves do KMS existentes. No entanto, não é possível criar chaves do KMS em seu armazenamento de chaves externas nem usar suas chaves do KMS em operações de criptografia. Talvez seja necessário desconectar o armazenamento de chaves externas em algum momento, como ao editar as propriedades, mas planeje adequadamente. A desconexão do armazenamento de chaves poderá interromper a operação dos serviços da AWS que usam suas chaves do KMS.

Não é necessário conectar seu armazenamento de chaves externas. Você pode deixar um armazenamento de chaves externas em estado desconectado indefinidamente e conectá-lo somente quando precisar usá-lo. No entanto, você pode desejar testar a conexão periodicamente para verificar se as configurações estão corretas e se ele pode ser conectado.

Quando você desconecta um armazenamento de chaves personalizado, as chaves do KMS do armazenamento de chaves tornam-se inutilizáveis imediatamente (sujeitas a consistência posterior). Porém, os recursos criptografados com chaves de dados protegidas pela chave do KMS não serão afetados até que a chave do KMS seja usada novamente, por exemplo, para descriptografar a chave de dados. Esse problema afeta os Serviços da AWS, pois muitos deles usam chaves de dados para proteger recursos. Para obter detalhes, consulte Como as chaves do KMS inutilizáveis afetam as chaves de dados.

> **Note**
>
> Armazenamentos de chaves externas têm o estado `DISCONNECTED` somente quando nunca foram conectados ou quando você os desconecta explicitamente. Um estado `CONNECTED` não indica que o armazenamento de chaves externas ou seus componentes de apoio estejam operando com eficiência. Para obter informações sobre a performance dos componentes do armazenamento de chaves externas, consulte os grafos na seção Monitoring (Monitoramento) da página de detalhes de cada armazenamento de chaves externas. Para obter detalhes, consulte Monitorar um armazenamento de chaves externas. O gerenciador de chaves externas pode fornecer outros métodos para interromper e reiniciar a comunicação entre o armazenamento de chaves externas do AWS KMS e o proxy de armazenamento de chaves externas, ou entre o proxy de armazenamento de chaves

externas e o gerenciador de chaves externas. Para obter detalhes, consulte a documentação do gerenciador de chaves externas.

Tópicos

- Conectar um armazenamento de chaves externas
- Desconectar um armazenamento de chaves externas
- Estado da conexão
- Conectar um armazenamento de chaves externas (console)
- Conectar um armazenamento de chaves externas (API)
- Desconectar um armazenamento de chaves externas (console)
- Desconectar um armazenamento de chaves externas (API)

Conectar um armazenamento de chaves externas

Quando seu armazenamento de chaves externas está conectado ao proxy de armazenamento de chaves externas, é possível criar chaves do KMS no armazenamento de chaves externas e usar chaves do KMS existentes em operações de criptografia.

O processo que conecta um armazenamento de chaves externas ao proxy de armazenamento de chaves externas difere com base na conectividade do armazenamento de chaves externas.

- Quando você conecta um armazenamento de chaves externo com conectividade de endpoint público, AWS KMS envia uma GetHealthStatus solicitação ao proxy externo do armazenamento de chaves para validar o endpoint do URI do proxy, o caminho do URI do proxy e a credencial de autenticação do proxy. Uma resposta bem-sucedida do proxy confirma que o endpoint do URI do proxy e o caminho do URI do proxy estão corretos e acessíveis e que o proxy autenticou a solicitação assinada com a credencial de autenticação do proxy para o armazenamento de chaves externas.
- Quando você conecta um armazenamento de chaves externas com a conectividade do serviço de endpoint da VPC ao proxy de armazenamento de chaves externas, o AWS KMS faz o seguinte:
  - Confirma que o domínio do nome DNS privado especificado no endpoint do URI do proxy foi verificado.
  - Cria um endpoint de interface de uma VPC do AWS KMS para o serviço de endpoint da VPC.

- Cria uma zona hospedada privada para o nome DNS privado especificado no endpoint do URI do proxy
- Envia uma GetHealthStatussolicitação para o proxy externo do armazenamento de chaves. Uma resposta bem-sucedida do proxy confirma que o endpoint do URI do proxy e o caminho do URI do proxy estão corretos e acessíveis e que o proxy autenticou a solicitação assinada com a credencial de autenticação do proxy para o armazenamento de chaves externas.

A operação de conexão inicia o processo de conexão do armazenamento de chaves personalizado, mas conectar um armazenamento de chaves externas ao proxy externo leva aproximadamente cinco minutos. Uma resposta bem-sucedida da operação de conexão não indica que o armazenamento de chaves externas esteja conectado. Para confirmar que a conexão foi bem-sucedida, use o AWS KMS console ou a DescribeCustomKeyStoresoperação para visualizar o estado da conexão externa do seu armazenamento de chaves.

Quando o estado da conexão é `FAILED`, um código de erro de conexão é exibido no console do AWS KMS e adicionado à resposta `DescribeCustomKeyStore`. Para obter ajuda na interpretação dos códigos de erro de conexão, consulte Códigos de erro de conexão para armazenamentos de chaves externas.

Desconectar um armazenamento de chaves externas

Quando você desconecta um armazenamento de chaves externas com conectividade do serviço de endpoint da VPC do proxy de armazenamento de chaves externas, o AWS KMS exclui o endpoint de interface para o serviço de endpoint da VPC e remove a infraestrutura de rede que ele criou para oferecer suporte à conexão. Nenhum processo equivalente é necessário para armazenamentos de chaves externas com conectividade de endpoint público. Essa ação não afeta o serviço de endpoint da VPC ou seus componentes de apoio nem afeta o proxy de armazenamento de chaves externas ou componentes externos.

Enquanto o armazenamento de chaves externas estiver desconectado, o AWS KMS não enviará nenhuma solicitação ao proxy de armazenamento de chaves externas. O estado da conexão do armazenamento de chaves externas é `DISCONNECTED`. As chaves do KMS no armazenamento de chaves externas desconectado estão no estado de chave `UNAVAILABLE` (a menos que estejam pendentes de exclusão), isto é, não podem ser usadas em operações de criptografia. Porém, você ainda poderá visualizar e gerenciar o armazenamento de chaves externas e suas chaves do KMS existentes.

O estado desconectado foi criado para ser temporário e reversível. Você pode reconectar o armazenamento de chaves externas a qualquer momento. Normalmente, não é necessária nenhuma reconfiguração. Porém, se alguma propriedade do proxy de armazenamento de chaves externas associado tiver sido alterada enquanto ele estava desconectado, como a alternância de sua credencial de autenticação de proxy, você deverá editar as configurações do armazenamento de chaves externas antes de reconectar.

> **Note**
>
> Enquanto um armazenamento de chaves personalizado estiver desconectado, todas as tentativas de criar chaves do KMS nele ou de usar chaves do KMS existentes em operações de criptografia falharão. Essa ação pode impedir que os usuários armazenem e acessem dados sigilosos.

Para avaliar melhor o efeito de desconectar o armazenamento de chaves externas, identifique as chaves do KMS no armazenamento de chaves externas e determine seu uso anterior.

Você pode desconectar o armazenamento de chaves externas por motivos como estes:

- Para editar suas propriedades. Você pode editar o nome do armazenamento de chaves personalizado, o caminho do URI do proxy e a credencial de autenticação do proxy enquanto o armazenamento de chaves externas está conectado. No entanto, para editar o tipo de conectividade do proxy, o endpoint do URI do proxy ou o nome do serviço de endpoint da VPC, primeiro é necessário desconectar o armazenamento de chaves externas. Para obter detalhes, consulte Editar propriedades do armazenamento de chaves externas.
- Para interromper toda a comunicação entre o AWS KMS e o proxy de armazenamento de chaves externas. Você também pode interromper a comunicação entre o AWS KMS e o proxy desabilitando o endpoint ou o serviço de endpoint da VPC. Além disso, o proxy de armazenamento de chaves externas ou o software de gerenciamento de chaves pode fornecer outros mecanismos para impedir que o AWS KMS se comunique com o proxy ou impedir que o proxy acesse o gerenciador de chaves externas.
- Para desabilitar todas as chaves do KMS no armazenamento de chaves externas. Você pode desativar e reativar as chaves KMS em um armazenamento de chaves externo usando o AWS KMS console ou a DisableKeyoperação. Essas operações são concluídas rapidamente (sujeitas a consistência posterior), mas atuam em uma chave do KMS de cada vez. A desconexão do armazenamento de chaves externas altera o estado da chave de todas as chaves do KMS no

armazenamento de chaves externas para `Unavailable`, impedindo que elas sejam usadas em operações de criptografia.

- Para reparar uma falha na tentativa de conexão. Se ocorrer falha em uma tentativa de conectar-se a um armazenamento de chaves externas (o estado da conexão do armazenamento de chaves personalizado apresentado é `FAILED`), você deve desconectar o armazenamento de chaves externas antes de tentar se conectar novamente.

Estado da conexão

A conexão e desconexão altera o estado da conexão do armazenamento de chaves personalizado. Os valores do estado da conexão são os mesmos para armazenamentos de chaves do AWS CloudHSM e armazenamentos de chaves externas.

Para ver o estado da conexão do seu armazenamento de chaves personalizadas, use a DescribeCustomKeyStoresoperação ou o AWS KMS console. O estado da conexão é exibido em cada tabela de armazenamento de chaves personalizado, na seção General configuration (Configuração geral) da página de detalhes de cada armazenamento de chaves personalizado e na guia Cryptographic configuration (Configuração criptográfica) das chaves do KMS em um armazenamento de chaves personalizado. Para obter mais detalhes, consulte Visualizar um armazenamento de chaves do AWS CloudHSM e Visualizar um armazenamento de chaves externas.

O armazenamento de chaves personalizado pode ter um dos estados de conexão a seguir:

- `CONNECTED`: o armazenamento de chaves personalizado está conectado a seu armazenamento de chaves de reserva. Você pode criar e usar chaves do KMS no armazenamento de chaves personalizado.

  O armazenamento de chaves de reserva para um armazenamento de chaves do AWS CloudHSM é o cluster do AWS CloudHSM associado. O armazenamento de chaves de reserva para um armazenamento de chaves externas é o proxy de armazenamento de chaves externas e o gerenciador de chaves externas ao qual oferece suporte.

  Um estado CONNECTED significa que uma conexão foi bem-sucedida e que o armazenamento de chaves personalizado não foi desconectado intencionalmente. Isso não indica que a conexão está funcionando devidamente. Para obter informações sobre o status do AWS CloudHSM cluster associado ao seu armazenamento de AWS CloudHSM chaves, consulte Obter CloudWatch métricas para AWS CloudHSM no Guia do AWS CloudHSM usuário. Para obter informações sobre o status e a operação do armazenamento de chaves externas, consulte os grafos na seção

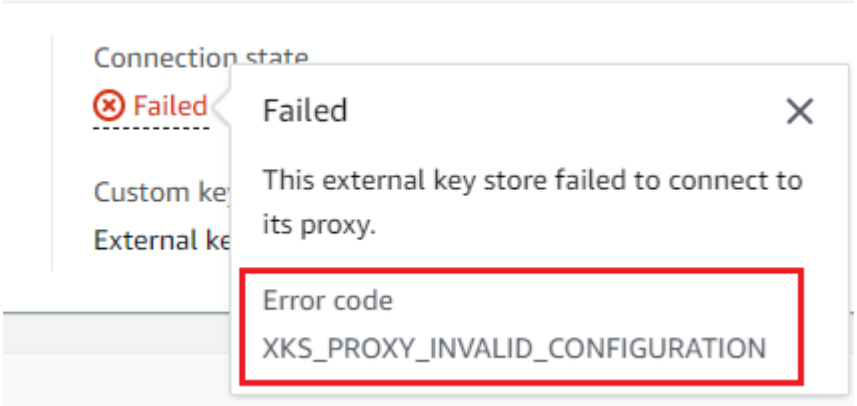
Monitoring (Monitoramento) da página de detalhes de cada armazenamento de chaves externas. Para obter detalhes, consulte Monitorar um armazenamento de chaves externas.

- `CONNECTING`: o processo de conexão de um armazenamento de chaves personalizado está em andamento. É um estado transitório.
- `DISCONNECTED`: o armazenamento de chaves personalizadas nunca foi conectado ao seu suporte ou foi desconectado intencionalmente usando o AWS KMS console ou a operação. DisconnectCustomKeyStore
- `DISCONNECTING`: o processo de desconexão de um armazenamento de chaves personalizado está em andamento. É um estado transitório.
- `FAILED`: falha na tentativa de conexão ao armazenamento de chaves personalizado. O `ConnectionErrorCode` na DescribeCustomKeyStoresresposta indica o problema.

Para conectar um armazenamento de chaves personalizado, o estado de conexão deve ser `DISCONNECTED`. Se o estado da conexão for `FAILED`, use `ConnectionErrorCode` para identificar e resolver o problema. Desconecte o armazenamento de chaves personalizado antes de tentar conectá-lo novamente. Para obter ajuda com falhas de conexão, consulte Erros de conexão do armazenamento de chaves externas. Para obter ajuda para responder a um código de erro de conexão, consulte Códigos de erro de conexão para armazenamentos de chaves externas.

Para visualizar o código de erro de conexão:

- Na DescribeCustomKeyStoresresposta, visualize o valor do `ConnectionErrorCode` elemento. Este elemento aparece na resposta de `DescribeCustomKeyStores` somente quando `ConnectionState` é `FAILED`.
- Para ver o código de erro de conexão no console do AWS KMS, acesse a página de detalhes do armazenamento de chaves externas e passe o mouse sobre o valor Failed.



Conectar um armazenamento de chaves externas (console)

Você pode usar o console do AWS KMS para conectar um armazenamento de chaves externas ao proxy de armazenamento de chaves externas.

1. Faça login no AWS Management Console e abra o console do AWS Key Management Service (AWS KMS) em https://console.aws.amazon.com/kms.
2. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.
3. No painel de navegação, selecione Custom key stores (Armazenamentos de chaves personalizados), External key stores (Armazenamentos de chaves externas).
4. Escolha a linha do armazenamento de chaves externas que deseja conectar.

   Se o estado de conexão do armazenamento de chaves externas for FAILED, você deverá desconectar o armazenamento de chaves externas antes de conectá-lo.
5. No menu Key store actions (Ações do armazenamento de chaves), escolha Connect (Conectar).

O processo de conexão normalmente leva cerca de cinco minutos para ser concluído. Quando a operação é concluída, o estado da conexão é alterado para CONNECTED.

Se o estado da conexão for Failed, passe o mouse sobre o estado da conexão para ver o código de erro da conexão, que explica a causa do erro. Para obter ajuda para responder a um código de erro de conexão, consulte Códigos de erro de conexão para armazenamentos de chaves externas. Para conectar um armazenamento de chaves externas com o estado de conexão Failed, você deve primeiro desconectar o armazenamento de chaves personalizado.

Conectar um armazenamento de chaves externas (API)

Para conectar um armazenamento de chaves externo desconectado, use a ConnectCustomKeyStoreoperação.

Antes de se conectar, o estado da conexão do armazenamento de chaves externas deve ser `DISCONNECTED`. Se o estado da conexão atual for `FAILED`, desconecte o armazenamento de chaves externas e conecte-o novamente.

O processo de conexão leva cerca de cinco minutos para ser concluído. A menos que ocorra uma falha rapidamente, `ConnectCustomKeyStore` retornará uma resposta HTTP 200 e um objeto JSON sem propriedades. No entanto, essa resposta inicial não indica que a conexão foi bem-sucedida. Para determinar se o armazenamento de chaves externo está conectado, veja o estado da conexão na DescribeCustomKeyStoresresposta.

Os exemplos nesta seção usam a AWS Command Line Interface (AWS CLI), mas você pode usar qualquer linguagem de programação compatível.

Para identificar o armazenamento de chaves externas, use o ID do armazenamento de chaves personalizado. Você pode encontrar o ID na página Armazenamentos de chaves personalizadas no console ou usando a DescribeCustomKeyStoresoperação. Antes de executar esse exemplo, substitua o ID de exemplo por um válido.

```
$ aws kms connect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

A operação `ConnectCustomKeyStore` não retorna `ConnectionState` na resposta. Para verificar se o armazenamento de chaves externo está conectado, use a DescribeCustomKeyStoresoperação. Por padrão, essa operação retorna todos os armazenamentos de chaves personalizados em sua conta e região. No entanto, você pode usar o parâmetro `CustomKeyStoreId` ou `CustomKeyStoreName` (mas não ambos) para limitar a resposta para determinados armazenamentos de chaves personalizados. Um valor `ConnectionState` de `CONNECTED` indica que o armazenamento de chaves externas está conectado ao proxy de armazenamento de chaves externas.

```
$ 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 o valor `ConnectionState` na resposta de `DescribeCustomKeyStores` for `FAILED`, o elemento `ConnectionErrorCode` indica o motivo da falha.

No exemplo a seguir, o valor `XKS_VPC_ENDPOINT_SERVICE_NOT_FOUND` para `ConnectionErrorCode` indica que o AWS KMS não consegue encontrar o serviço de endpoint da VPC que ele usa para se comunicar com o proxy de armazenamento de chaves externas. Verifique se `XksProxyVpcEndpointServiceName` está correto, se a entidade principal do serviço do AWS KMS é uma entidade principal permitida no serviço de endpoint da Amazon VPC e se o serviço de endpoint da VPC não exige a aceitação de solicitações de conexão. Para obter ajuda para responder a um código de erro de conexão, consulte Códigos de erro de conexão para armazenamentos de chaves externas.

```
$ 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"
      }
    }
  ]
}
```

Desconectar um armazenamento de chaves externas (console)

Você pode usar o console do AWS KMS para conectar um armazenamento de chaves externas ao proxy de armazenamento de chaves externas. Esse processo leva cerca de cinco minutos para ser concluído.

1. Faça login no AWS Management Console e abra o console do AWS Key Management Service (AWS KMS) em https://console.aws.amazon.com/kms.

2. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.
3. No painel de navegação, selecione Custom key stores (Armazenamentos de chaves personalizados), External key stores (Armazenamentos de chaves externas).
4. Escolha a linha do armazenamento de chaves externas que deseja desconectar.
5. No menu Key store actions (Ações do armazenamento de chaves), escolha Disconnect (Desconectar).

Quando a operação é concluída, o estado de conexão é alterado de DISCONNECTING (DESCONECTANDO) para DISCONNECTED (DESCONECTADO). Se ocorrer falha na operação, será exibida uma mensagem de erro descrevendo o problema e fornecendo ajuda para corrigi-lo. Se precisar de ajuda adicional, consulte Erros de conexão do armazenamento de chaves externas.

Desconectar um armazenamento de chaves externas (API)

Para desconectar um armazenamento de chaves externo conectado, use a DisconnectCustomKeyStoreoperação. Se a operação tiver êxito, o AWS KMS retornará uma resposta HTTP 200 e um objeto JSON sem propriedades. O processo leva cerca de cinco minutos para ser concluído. Para encontrar o estado da conexão do armazenamento de chaves externo, use a DescribeCustomKeyStoresoperação.

Os exemplos nesta seção usam a AWS Command Line Interface (AWS CLI), mas você pode usar qualquer linguagem de programação compatível.

Este exemplo desconecta um armazenamento de chaves externas da conectividade do serviço de endpoint da VPC. Antes de executar este exemplo, substitua o ID de exemplo do armazenamento de chaves personalizado por um válido.

```
$ aws kms disconnect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

Para verificar se o armazenamento de chaves externo está desconectado, use a DescribeCustomKeyStoresoperação. Por padrão, essa operação retorna todos os armazenamentos de chaves personalizados em sua conta e região. No entanto, você pode usar o parâmetro `CustomKeyStoreId` e `CustomKeyStoreName` (mas não ambos) para limitar a resposta para determinados armazenamentos de chaves personalizados. O valor `ConnectionState` de `DISCONNECTED` indica que esse exemplo de armazenamento de chaves externas não está mais conectado ao proxy de armazenamento de chaves externas.

```
$ 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"
      }
    }
  ]
}
```

Excluir um armazenamento de chaves externas

Quando você exclui um armazenamento de chaves externas, o AWS KMS exclui todos os metadados sobre o armazenamento de chaves externas do AWS KMS, inclusive informações sobre o proxy de armazenamento de chaves externas. Essa operação não afeta o proxy do armazenamento de chaves externas, o gerenciador de chaves externas, as chaves externas ou os recursos da AWS que você criou para dar suporte ao armazenamento de chaves externas, como uma Amazon VPC ou um serviço de endpoint da VPC.

Antes de excluir um armazenamento de chaves externas, você deve excluir todas as chaves do KMS do armazenamento de chaves e desconectar o armazenamento de chaves do proxy de armazenamento de chaves externas. Senão, as tentativas de excluir o armazenamento de chaves falharão.

A exclusão de um armazenamento de chaves externas é irreversível, mas você pode criar um novo armazenamento de chaves externas e associá-lo ao mesmo proxy de armazenamento de chaves externas e ao mesmo gerenciador de chaves externas. No entanto, você não pode recriar as chaves do KMS de criptografia simétrica no armazenamento de chaves externas, mesmo que tenha acesso ao mesmo material de chave externa. O AWS KMS inclui metadados no texto cifrado simétrico exclusivo para cada chave do KMS. Esse recurso de segurança garante que somente a chave do KMS que criptografou os dados poderá descriptografá-los.

Em vez de excluir o armazenamento de chaves externas, considere desconectá-lo. Enquanto um armazenamento de chaves externas está desconectado, é possível gerenciar o armazenamento de chaves externas e as respectivas AWS KMS keys, mas não é possível criar nem usar chaves do KMS no armazenamento de chaves externas. Você pode reconectar o armazenamento de chaves externas a qualquer momento e continuar usando suas chaves do KMS para criptografar e descriptografar dados. Não há custo para um proxy de armazenamento de chaves externas desconectado ou chaves do KMS indisponíveis.

Tópicos

- Excluir um armazenamento de chaves externas (console)
- Excluir um armazenamento de chaves externas (API)

Excluir um armazenamento de chaves externas (console)

Você pode usar o console do AWS KMS para excluir um armazenamento de chaves externas.

1. Faça login no AWS Management Console e abra o console do AWS Key Management Service (AWS KMS) em https://console.aws.amazon.com/kms.
2. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.
3. No painel de navegação, selecione Custom key stores (Armazenamentos de chaves personalizados), External key stores (Armazenamentos de chaves externas).
4. Encontre a linha que representa o armazenamento de chaves externas que você deseja excluir. Se o Connection state (Estado de conexão) do armazenamento de chaves externas não for DISCONNECTED, você deverá desconectar o armazenamento de chaves externas antes de excluí-lo.
5. No menu Key store actions (Ações de armazenamento de chaves), escolha Delete (Excluir).

Quando a operação for concluída, uma mensagem de êxito será exibida, e o armazenamento de chaves externas não será mais exibido na lista de armazenamentos de chaves. Se a operação não for bem-sucedida, será exibida uma mensagem de erro descrevendo o problema e fornecendo ajuda para corrigi-lo. Se precisar de ajuda adicional, consulte Solução de problemas de armazenamentos de chaves externas.

Excluir um armazenamento de chaves externas (API)

Para excluir um armazenamento de chaves externo, use a DeleteCustomKeyStoreoperação. Se a operação tiver êxito, o AWS KMS retornará uma resposta HTTP 200 e um objeto JSON sem propriedades.

Para começar, desconecte o armazenamento de chaves externas. Antes de executar um comando como esse, substitua o ID de exemplo do armazenamento de chaves personalizado por um válido.

```
$ aws kms disconnect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

Depois que o armazenamento de chaves externo for desconectado, você poderá usar a DeleteCustomKeyStoreoperação para excluí-lo.

```
$ aws kms delete-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

Para confirmar que o armazenamento de chaves externo foi excluído, use a DescribeCustomKeyStoresoperação.

```
$ aws kms describe-custom-key-stores

{
    "CustomKeyStores": []
}
```

Se você especificar um nome ou ID de armazenamento de chaves personalizado que não existe mais, o AWS KMS retornará uma exceção `CustomKeyStoreNotFoundException`.

```
$ aws kms describe-custom-key-stores --custom-key-store-id cks-1234567890abcdef0

An error occurred (CustomKeyStoreNotFoundException) when calling the
 DescribeCustomKeyStore operation:
```

Gerenciar chaves do KMS em um armazenamento de chaves externas

Para criar, visualizar, gerenciar, usar e programar a exclusão de chaves do KMS em um armazenamento de chaves externas, use procedimentos muito semelhantes aos usados para outras chaves do KMS. No entanto, ao criar uma chave do KMS em um armazenamento de chaves externas, especifique um armazenamento de chaves externas e uma chave externa. Quando você

usa uma chave do KMS em um armazenamento de chaves externas, as operações de criptografia e descriptografia são executadas pelo gerenciador de chaves externas usando a chave externa especificada.

O AWS KMS não pode criar, visualizar, atualizar ou excluir nenhuma chave de criptografia em seu gerenciador de chaves externa. O AWS KMS nunca acessa diretamente seu gerenciador de chaves externas ou qualquer chave externa. Todas as solicitações de operações de criptografia são mediadas por seu proxy de armazenamento de chaves externas. Para usar uma chave do KMS em um armazenamento de chaves externas, o armazenamento de chaves externas que hospeda a chave do KMS deve estar conectado ao proxy de armazenamento de chaves externas.

Recursos compatíveis

Além dos procedimentos discutidos nesta seção, você pode fazer o seguinte com chaves do KMS de um armazenamento de chaves externas:

- Use políticas de chaves, políticas do IAM e concessões para autorizar o acesso às chaves do KMS.
- Habilite e desabilite as chaves do KMS. Essas ações não afetam a chave externa no gerenciador de chaves externas.
- Atribua etiquetas, crie aliases e use o controle de acesso por atributo (ABAC) para autorizar o acesso às chaves do KMS.
- Usar as chaves do KMS com Serviços da AWS que se integram ao AWS KMS e oferecem suporte a chaves gerenciadas pelo cliente.

Recursos sem suporte

- Armazenamentos de chaves externas são compatíveis apenas com chaves do KMS de criptografia simétrica. Você não pode criar chaves do KMS de HMAC ou assimétricas em um armazenamento de chaves externas.
- GenerateDataKeyPaire não GenerateDataKeyPairWithoutPlaintextsão compatíveis com chaves KMS em um armazenamento de chaves externo.
- Você não pode usar um modelo do AWS CloudFormation para criar um armazenamento de chaves externas ou uma chave do KMS em um armazenamento de chaves externas.
- As chaves multirregionais não são compatíveis com o armazenamento de chaves externas.
- As chaves do KMS com material de chave importado não são compatíveis com o armazenamento de chaves externas.

- A alternância automática de chaves não é compatível com chaves do KMS em armazenamentos de chaves externas.

Tópicos

- Criar chaves do KMS em um armazenamento de chaves externas
- Visualizar chaves do KMS em um armazenamento de chaves externas
- Usar chaves do KMS em um armazenamento de chaves externas
- Agendar a exclusão de chaves do KMS de um armazenamento de chaves externas

Criar chaves do KMS em um armazenamento de chaves externas

Depois de criar e conectar o armazenamento de chaves, você poderá criar AWS KMS keys nesse armazenamento de chaves. Devem ser chaves do KMS de criptografia simétrica com um valor de origem de armazenamento de chaves externas (`EXTERNAL_KEY_STORE`). Não é possível criar chaves do KMS assimétricas, chaves do KMS de Hash-based message authentication code (HMAC – Código de autenticação de mensagem por hash) ou chaves do KMS com material de chave importado em um armazenamento personalizado de chave. Além disso, não é possível usar chaves do KMS de criptografia simétrica em um armazenamento personalizado de chaves para gerar pares de chaves assimétricos de dados.

Uma chave do KMS em um armazenamento de chaves externas pode ter menor latência, durabilidade e disponibilidade do que uma chave do KMS padrão, pois depende de componentes localizados fora da AWS. Antes de criar ou usar uma chave do KMS em um armazenamento de chaves externas, verifique se você precisa de uma chave com propriedades de armazenamento de chaves externas.

> **Note**
>
> Alguns gerenciadores de chaves externas fornecem um método mais simples de criar chaves do KMS em um armazenamento de chaves externas. Para obter detalhes, consulte a documentação do gerenciador de chaves externas.

Para criar uma chave do KMS no armazenamento de chaves externas, especifique:

- O ID do armazenamento de chaves externas.

- A origem do material de chave do armazenamento de chaves externas (`EXTERNAL_KEY_STORE`).
- O ID de uma chave externa existente no gerenciador de chaves externas associado a seu armazenamento de chaves externas. Essa chave externa serve como material de chave para a chave do KMS. Você pode alterar o ID da chave externa após criar a chave do KMS.

  O AWS KMS fornece o ID da chave externa para seu proxy de armazenamento de chaves externas em solicitações de operações de criptografia e descriptografia. O AWS KMS não consegue acessar diretamente seu gerenciador de chaves externas ou qualquer uma de suas chaves de criptografia.

Além da chave externa, uma chave do KMS em um armazenamento de chaves externas também tem material de chave do AWS KMS. Todos os dados criptografados na chave do KMS são criptografados primeiro no AWS KMS usando o material de chave do AWS KMS e depois no gerenciador de chaves externas usando a chave externa. Esse processo de criptografia dupla garante que o texto cifrado protegido pela chave do KMS em um armazenamento de chaves externas seja pelo menos tão forte quanto o texto cifrado protegido somente pelo AWS KMS. Para obter detalhes, consulte Como funcionam os armazenamentos de chaves externas.

Quando a operação `CreateKey` é bem-sucedida, o estado da chave da nova chave do KMS é `Enabled`. Ao visualizar uma chave do KMS em um armazenamento de chaves externas, é possível ver as propriedades comuns, como ID da chave, especificação da chave, uso da chave, estado da chave e a data da criação. Mas você também pode ver o ID e o estado da conexão do armazenamento de chaves externas e o ID da chave externa.

Se ocorrer uma falha na tentativa de criar uma chave do KMS no seu armazenamento de chaves externas, use a mensagem de erro para identificar a causa. Isso pode indicar que o armazenamento de chaves externas não está conectado (`CustomKeyStoreInvalidStateException`), que o proxy de armazenamento de chaves externas não consegue encontrar uma chave externa com o ID da chave externa especificada (`XksKeyNotFoundException`) ou que a chave externa já está associada a uma chave do KMS no mesmo armazenamento de chaves externas `XksKeyAlreadyInUseException`.

.

Para obter um exemplo do log do AWS CloudTrail da operação que cria uma chave do KMS em um armazenamento de chaves externas, consulte CreateKey.

Tópicos

- Requisitos para uma chave do KMS em um armazenamento de chaves externas
- Criar uma chave do KMS em um armazenamento de chaves externas (console)
- Criar uma chave do KMS em um armazenamento de chaves externas (API do AWS KMS)

Requisitos para uma chave do KMS em um armazenamento de chaves externas

Para criar uma chave do KMS em um armazenamento de chaves externas, as seguintes propriedades são obrigatórias no armazenamento de chaves externas, na chave do KMS e na chave externa que serve como material de chave de criptografia externa para a chave do KMS.

Requisitos de armazenamento de chaves externas

- Deve estar conectado ao proxy de armazenamento de chaves externas.

  Para visualizar o estado da conexão do armazenamento de chaves externas, consulte Visualizar um armazenamento de chaves externas. Para conectar o armazenamento de chaves externas, consulte Conectar e desconectar um armazenamento de chaves externas.

Requisitos de chaves do KMS

Você não pode alterar essas propriedades após criar a chave do KMS.

- Especificação da chave: SYMMETRIC_DEFAULT
- Uso da chave: ENCRYPT_DECRYPT
- Origem do material de chave: EXTERNAL_KEY_STORE
- Várias regiões: FALSE

Requisitos de chaves externas

- Chave de criptografia AES de 256 bits (256 bits aleatórios). O `KeySpec` da chave externa deve ser `AES_256`.
- Habilitadas e disponíveis para uso. O `Status` da chave externa deve ser `ENABLED`.
- Configurada para criptografia e descriptografia. O `KeyUsage` da chave externa deve incluir `ENCRYPT` e `DECRYPT`.
- Usado somente com essa chave do KMS. Cada `KMS key` em um armazenamento de chaves externas deve estar associada a uma chave externa diferente.

O AWS KMS também recomenda que a chave externa seja usada exclusivamente para o armazenamento de chaves externas. Essa restrição facilita identificar e resolver problemas da chave.

- Acessível pelo proxy de armazenamento de chaves externas para o armazenamento de chaves externas.

  Se o proxy de armazenamento de chaves externas não conseguir encontrar a chave usando o ID de chave externa especificado, a operação `CreateKey` falhará.
- Pode lidar com o tráfego previsto que seu uso dos Serviços da AWS gera. O AWS KMS recomenda que as chaves externas estejam preparadas para lidar com até 1800 solicitações por segundo.

Criar uma chave do KMS em um armazenamento de chaves externas (console)

Há duas maneiras de criar uma chave do KMS em um armazenamento de chaves externas.

- Método 1 (recomendado): escolha um armazenamento de chaves externas e crie uma chave do KMS nesse armazenamento de chaves externo.
- Método 2: crie uma chave do KMS e indique que ela está em um armazenamento de chaves externo.

Se você usar o Método 1, em que você escolhe o armazenamento de chaves externo antes de criar a chave, o AWS KMS escolherá todas as propriedades de chave do KMS obrigatórias para você e preencherá o ID do armazenamento de chaves externo. Esse método evita erros que você possa cometer ao criar sua chave do KMS.

> **Note**
>
> Não inclua informações confidenciais ou sigilosas no alias, na descrição ou nas tags. Esses campos podem aparecer em texto simples em CloudTrail registros e outras saídas.

Método 1 (recomendado): comece com o armazenamento de chaves externo

Para usar esse método, escolha seu armazenamento de chaves externas e crie uma chave do KMS. O console do AWS KMS escolhe todas as propriedades obrigatórias para você e preenche o ID do

armazenamento de chaves externas. Esse método evita muitos erros que você possa cometer ao criar sua chave do KMS.

1. Faça login no AWS Management Console e abra o console do AWS Key Management Service (AWS KMS) em https://console.aws.amazon.com/kms.
2. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.
3. No painel de navegação, selecione Custom key stores (Armazenamentos de chaves personalizados), External key stores (Armazenamentos de chaves externas).
4. Escolha o nome do armazenamento de chaves externas.
5. No canto superior direito, escolha Create a KMS key in this key store (Criar uma chave do KMS neste armazenamento de chaves).

   Se o armazenamento de chaves externas não estiver conectado, você verá um aviso para conectá-lo. Se a tentativa de conexão falhar, será necessário resolver o problema e conectar o armazenamento de chaves externas antes de criar uma nova chave do KMS nele.

   Se o armazenamento de chaves externas estiver conectado, você será redirecionado para a página Customer managed keys (Chaves gerenciadas pelo cliente) para criar uma chave. Os valores de Key configuration (Configuração de chave) obrigatórios já foram escolhidos para você. Além disso, o ID de armazenamento de chaves personalizado do armazenamento de chaves externas está preenchido, mas é possível alterá-lo.
6. Insira o ID da chave externa no gerenciador de chaves externas. Essa chave externa deve atender aos requisitos para uso com uma chave do KMS. Você não pode alterar o valor depois que a chave é criada.

   Se a chave externa tiver mais de um ID, insira o ID da chave que o proxy de armazenamento de chaves externas usa para identificar a chave externa.
7. Confirme que você pretende criar uma chave do KMS no armazenamento de chaves externas especificado.
8. Escolha Próximo.

   O restante desse procedimento é o mesmo que a criação de uma chave do KMS padrão.
9. Digite um alias (obrigatório) e uma descrição (opcional) para a chave do KMS.
10. (Opcional). Na página Add Tags (Adicionar etiquetas), adicione etiquetas que identificam ou categorizam a chave do KMS.

Ao adicionar tags aos recursos da AWS, a AWS gera um relatório de alocação de custos com utilização e custos agrupados por tags. Etiquetas também podem ser utilizadas para controlar o acesso a uma chave do KMS. Para informações sobre marcação de chaves do KMS, consulte Marcar chaves com tags e ABAC para AWS KMS.

11. Escolha Próximo.
12. Na seção Key Administrators (Administradores de chaves), selecione os usuários e as funções do IAM que podem gerenciar a chave do KMS. Para obter mais informações, consulte Permite que administradores de chaves administrem a chave do KMS.

> **Note**
>
> As políticas do IAM podem conceder permissão para usar a chave do KMS a outros usuários e funções do IAM.
> As práticas recomendadas do IAM não encorajam o uso de usuários do IAM com credenciais de longo prazo. Sempre que possível, use os perfis do IAM, por fornecerem credenciais temporárias. Para obter detalhes, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

13. (Opcional) Para evitar que esses administradores de chaves excluam essa chave do KMS, desmarque a caixa de seleção Allow key administrators to delete this key (Permitir que os administradores de chaves excluam essa chave).

    Excluir uma chave do KMS é uma operação destrutiva e irreversível que pode tornar o texto cifrado irrecuperável. Você não pode recriar uma chave do KMS simétrica em um armazenamento de chaves externas, mesmo que você tenha o material de chave externa. No entanto, a exclusão de uma chave do KMS não afeta a chave externa associada. Para obter informações sobre como excluir uma chave do KMS de um armazenamento de chaves externas, consulte Agendar a exclusão de chaves do KMS de um armazenamento de chaves externas.
14. Escolha Próximo.
15. Na seção This account (Esta conta), selecione os usuários e as funções do IAM nessa Conta da AWS que podem usar a chave do KMS em operações de criptografia. Para obter mais informações, consulte Permite que os usuários de chaves usem a chave do KMS.

> **Note**
>
> As políticas do IAM podem conceder permissão para usar a chave do KMS a outros usuários e funções do IAM.
> As práticas recomendadas do IAM não encorajam o uso de usuários do IAM com credenciais de longo prazo. Sempre que possível, use os perfis do IAM, por fornecerem credenciais temporárias. Para obter detalhes, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

16. (Opcional) Você pode permitir que outras Contas da AWS usem essa chave do KMS para operações de criptografia. Para fazer isso, na seção Other Contas da AWS (Outras Conta da AWS) na parte inferior da página, escolha Add another Conta da AWS (Adicionar outra) e insira o ID da de uma conta externa. Para adicionar várias contas externas, repita essa etapa.

> **Note**
>
> Os administradores das outras Contas da AWS também devem permitir o acesso à chave do KMS criando políticas do IAM para seus usuários. Para ter mais informações, consulte Permitir que usuários de outras contas usem uma chave do KMS.

17. Escolha Próximo.
18. Revise as configurações que você escolheu. Ainda é possível voltar e alterar todas as configurações.
19. Quando terminar, escolha Finish (Terminar) para criar a chave.

Método 2: comece com chaves gerenciadas pelo cliente

Esse procedimento é igual ao procedimento para criar uma chave de criptografia simétrica com material de chave do AWS KMS. Mas, nesse procedimento, você especificará o ID de armazenamento de chaves personalizado do armazenamento de chaves externas e o ID da chave externa. Também é necessário especificar os valores de propriedade obrigatórios para uma chave do KMS em um armazenamento de chaves externas, como a especificação da chave e o uso da chave.

1. Faça login no AWS Management Console e abra o console do AWS Key Management Service (AWS KMS) em https://console.aws.amazon.com/kms.

2. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.
3. No painel de navegação, escolha Customer managed keys (Chaves gerenciadas pelo cliente).
4. Escolha Create key (Criar chave).
5. Selecione Symmetric (Simétrica).
6. Em Key usage (Uso da chave), a opção Encrypt and decrypt (Criptografar e descriptografar) é selecionada para você. Não altere essa opção.
7. Escolha Advanced options (Opções avançadas).
8. Para Key material origin (Origem do material de chave), escolha External key store (Armazenamento de chaves externas).
9. Confirme que você pretende criar uma chave do KMS no armazenamento de chaves externas especificado.
10. Escolha Próximo.
11. Escolha a linha que representa o armazenamento de chaves externas para a nova chave do KMS.

    Você pode escolher um armazenamento de chaves externas desconectado. Para conectar um armazenamento de chaves que esteja desconectado, escolha o nome do armazenamento de chaves e, em Key store actions (Ações do armazenamento de chaves), escolha Connect (Conectar). Para obter detalhes, consulte Conectar um armazenamento de chaves externas (console).
12. Insira o ID da chave externa no gerenciador de chaves externas. Essa chave externa deve atender aos requisitos para uso com uma chave do KMS. Você não pode alterar o valor depois que a chave é criada.

    Se a chave externa tiver mais de um ID, insira o ID da chave que o proxy de armazenamento de chaves externas usa para identificar a chave externa.
13. Escolha Próximo.

    O restante desse procedimento é o mesmo que a criação de uma chave do KMS padrão.
14. Digite um alias e uma descrição opcional para a chave do KMS.
15. (Opcional). Na página Add Tags (Adicionar etiquetas), adicione etiquetas que identificam ou categorizam a chave do KMS.

    Ao adicionar tags aos recursos da AWS, a AWS gera um relatório de alocação de custos com utilização e custos agrupados por tags. Etiquetas também podem ser utilizadas para controlar o

acesso a uma chave do KMS. Para informações sobre marcação de chaves do KMS, consulte Marcar chaves com tags e ABAC para AWS KMS.

16. Escolha Próximo.
17. Na seção Key Administrators (Administradores de chaves), selecione os usuários e as funções do IAM que podem gerenciar a chave do KMS. Para obter mais informações, consulte Permite que administradores de chaves administrem a chave do KMS.

    > **Note**
    >
    > As políticas do IAM podem conceder permissão para usar a chave do KMS a outros usuários e funções do IAM.

18. (Opcional) Para evitar que esses administradores de chaves excluam essa chave do KMS, desmarque a caixa de seleção Allow key administrators to delete this key (Permitir que os administradores de chaves excluam essa chave).

    Excluir uma chave do KMS é uma operação destrutiva e irreversível que pode tornar o texto cifrado irrecuperável. Você não pode recriar uma chave do KMS simétrica em um armazenamento de chaves externas, mesmo que você tenha o material de chave externa. No entanto, a exclusão de uma chave do KMS não afeta a chave externa associada. Para obter informações sobre como excluir uma chave do KMS de um armazenamento de chaves externas, consulte Agendar a exclusão de chaves do KMS de um armazenamento de chaves externas.
19. Escolha Próximo.
20. Na seção This account (Esta conta), selecione os usuários e as funções do IAM nessa Conta da AWS que podem usar a chave do KMS em operações de criptografia. Para obter mais informações, consulte Permite que os usuários de chaves usem a chave do KMS.

    > **Note**
    >
    > As políticas do IAM podem conceder permissão para usar a chave do KMS a outros usuários e funções do IAM.

21. (Opcional) Você pode permitir que outras Contas da AWS usem essa chave do KMS para operações de criptografia. Para fazer isso, na seção Other Contas da AWS (Outras Conta da AWS) na parte inferior da página, escolha Add another Conta da AWS (Adicionar outra) e insira o ID da de uma conta externa. Para adicionar várias contas externas, repita essa etapa.

> **Note**
>
> Os administradores das outras Contas da AWS também devem permitir o acesso à chave do KMS criando políticas do IAM para seus usuários. Para ter mais informações, consulte Permitir que usuários de outras contas usem uma chave do KMS.

22. Escolha Próximo.
23. Revise as configurações que você escolheu. Ainda é possível voltar e alterar todas as configurações.
24. Quando terminar, escolha Finish (Terminar) para criar a chave.

Se o procedimento for bem-sucedido, a tela exibirá a nova chave do KMS no armazenamento de chaves externas que você escolheu. Ao escolher o nome ou alias para a nova chave do KMS, a guia Cryptographic configuration (Configuração criptográfica) da página de detalhes exibe a origem da chave do KMS (External key store [Armazenamento de chaves externas]), o nome, o ID e o tipo de armazenamento de chaves personalizado, o uso da chave e o status da chave externa. Se houver falha no procedimento, uma mensagem descrevendo a falha será exibida. Em , consulte Solução de problemas de armazenamentos de chaves externas.

> **Tip**
>
> Para facilitar a identificação de chaves do KMS em um armazenamento de chaves personalizado, na página Customer managed keys (Chaves gerenciadas pelo cliente), adicione a coluna Origin (Origem) e Custom key store ID (ID de armazenamento de chaves personalizado) à exibição. Para alterar os campos da tabela, escolha o ícone de engrenagem no canto superior direito da página. Para obter detalhes, consulte Personalizar suas tabelas de chaves do KMS.

Criar uma chave do KMS em um armazenamento de chaves externas (API do AWS KMS)

Para criar uma nova chave KMS em um armazenamento de chaves externo, use a CreateKeyoperação. Os seguintes parâmetros são obrigatórios:

- O valor de `Origin` deve ser `EXTERNAL_KEY_STORE`.

- O parâmetro `CustomKeyStoreId` identifica o armazenamento de chaves externas. O `ConnectionState` do armazenamento de chaves externas especificado deve ser `CONNECTED`. Para encontrar `CustomKeyStoreId` e `ConnectionState`, use a operação `DescribeCustomKeyStores`.
- O parâmetro `XksKeyId` identifica a chave externa. Essa chave externa deve atender aos requisitos para associação com uma chave do KMS.

Você também pode usar qualquer um dos parâmetros opcionais da operação `CreateKey`, como usar os parâmetros de `Policy` ou de Tags (Etiquetas).

> **Note**
>
> Não inclua informações confidenciais ou sigilosas nos campos `Description` ou `Tags`. Esses campos podem aparecer em texto simples em CloudTrail registros e outras saídas.

Os exemplos nesta seção usam a AWS Command Line Interface (AWS CLI), mas você pode usar qualquer linguagem de programação compatível.

Este exemplo de comando usa a CreateKeyoperação para criar uma chave KMS em um armazenamento de chaves externo. A resposta inclui as propriedades das chaves do KMS, o ID do armazenamento de chaves externas e o ID, uso e status da chave externa. Para obter informações detalhadas sobre esses campos, consulte Visualizar chaves do KMS em um armazenamento de chaves externas.

Antes de executar um comando como esse, substitua o ID de exemplo do armazenamento de chaves personalizado por um ID válido.

```
$ 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"
    }
  }
}
```

Visualizar chaves do KMS em um armazenamento de chaves externas

Para visualizar as chaves KMS em um armazenamento de chaves externo, use o AWS KMS console ou a DescribeKeyoperação. Você pode usar as mesmas técnicas que você usaria para visualizar as chaves gerenciadas pelo cliente do AWS KMS. Para aprender os conceitos básicos, consulte Visualizar chaves.

No console do AWS KMS, as chaves do KMS do armazenamento de chaves externas são exibidas na página Customer managed keys (Chaves gerenciadas pelo cliente) juntamente com todas as outras chaves gerenciadas pelo cliente em sua Conta da AWS e região. Para identificar chaves do KMS em um armazenamento de chaves externas, filtre pelo valor de origem distinto, External key store (Armazenamento de chaves externas), e pelo ID do armazenamento de chaves personalizado.

Para obter mais informações, consulte Visualizar um armazenamento de chaves externas, Monitorar um armazenamento de chaves externas e Registrando chamadas de AWS KMS API com AWS CloudTrail.

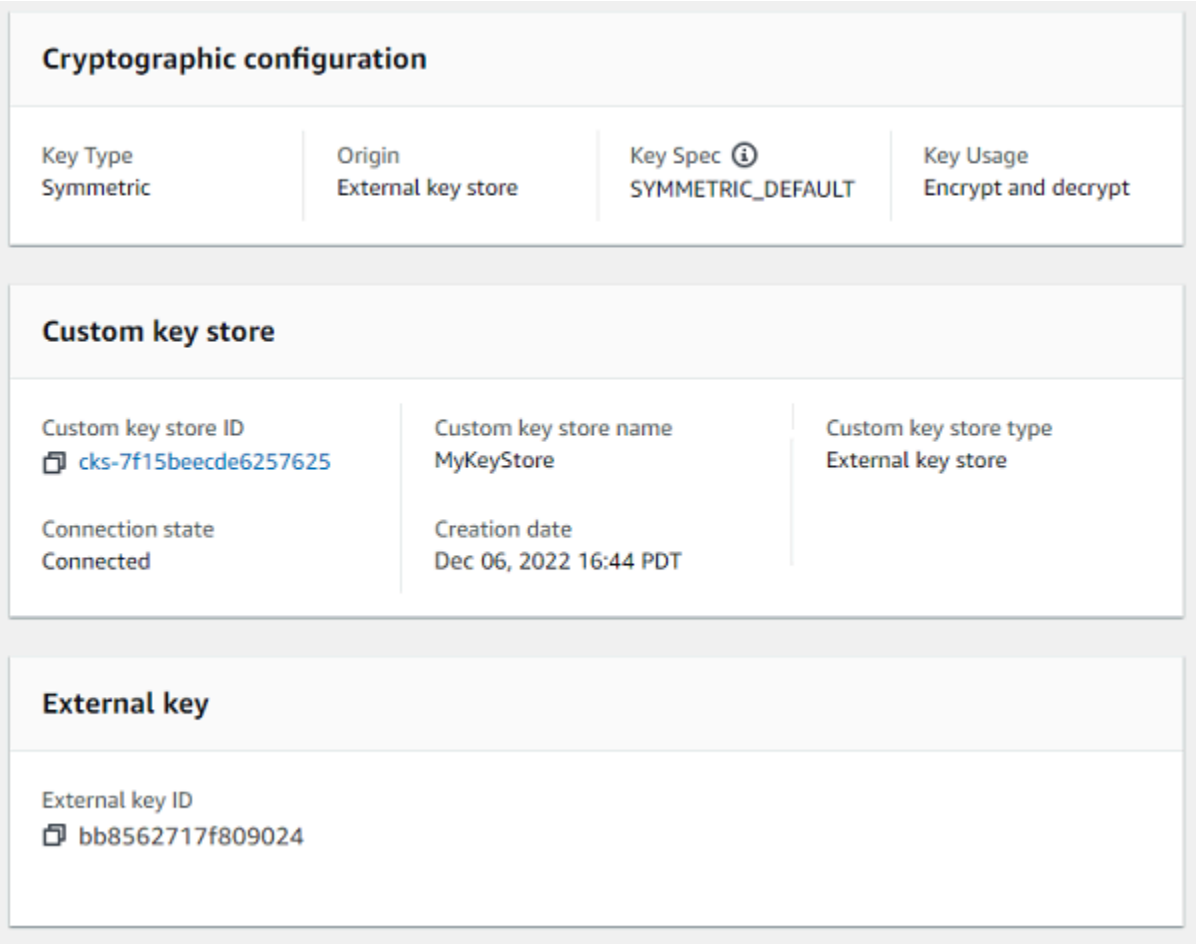
Tópicos

- Propriedades das chaves do KMS em um armazenamento de chaves externas
- Visualizar chaves do KMS em um armazenamento de chaves externas (console)
- Visualizar chaves do KMS em um armazenamento de chaves externas (API do AWS KMS)

Propriedades das chaves do KMS em um armazenamento de chaves externas

Como todas as chaves do KMS, as chaves do KMS em um armazenamento de chaves externas têm um ARN da chave, especificação da chave e valores de uso da chave, mas também têm propriedades e valores de propriedade específicos para chaves do KMS em um armazenamento de chaves externas. Por exemplo, o valor de Origin (Origem) para todas as chaves do KMS em armazenamentos de chaves externas é External key store (Armazenamento de chaves externas).

Para uma chave do KMS em um armazenamento de chaves externas, a guia Cryptographic configuration (Configuração criptográfica) no console do AWS KMS contém mais duas seções, Custom key store (Armazenamento de chaves personalizado) e External key (Chave externa).



Propriedades do armazenamento de chaves personalizado

Os valores a seguir aparecem na seção Armazenamento de chaves personalizadas da guia Configuração criptográfica e na DescribeKeyresposta. Essas propriedades se aplicam a todos os armazenamentos de chaves personalizados, inclusive armazenamentos de chaves do AWS CloudHSM e armazenamentos de chaves externas.

ID do armazenamento de chaves personalizado

Um ID exclusivo que o AWS KMS atribui ao armazenamento de chaves personalizado.

Nome do armazenamento de chaves personalizado

Um nome amigável que você atribui ao armazenamento de chaves personalizado ao criá-lo. Você pode alterar esse valor a qualquer momento.

Tipo do armazenamento de chaves personalizado

O tipo do armazenamento de chaves personalizado. Os valores válidos são AWS CloudHSM (`AWS_CLOUDHSM`) ou External key store (Armazenamento de chaves externas) (`EXTERNAL_KEY_STORE`). Você não pode alterar o tipo depois de criar o armazenamento de chaves personalizado.

Data de Criação

A data em que o armazenamento de chaves personalizado foi criado. Essa data é exibida na hora local da Região da AWS.

Estado da conexão

Indica se o armazenamento de chaves personalizado está conectado a seu armazenamento de chaves de reserva. O estado da conexão será `DISCONNECTED` somente se o armazenamento de chaves personalizado nunca tiver sido conectado ao armazenamento de chaves de reserva ou se tiver sido desconectado intencionalmente. Para obter detalhes, consulte the section called “Estado da conexão”.

Propriedades da chave externa

As propriedades da chave externa aparecem na seção Chave externa da guia Configuração criptográfica e no `XksKeyConfiguration` elemento da DescribeKeyresposta.

A seção External key (Chave externa) é exibida no console do AWS KMS somente para chaves do KMS em armazenamentos de chaves externas. Ela fornece informações sobre a chave externa associada à chave do KMS. A chave externa é uma chave de criptografia fora da AWS que serve como material de chave para a chave do KMS no armazenamento de chaves externas. Quando você criptografa ou descriptografa com a chave do KMS, a operação é executada pelo gerenciador de chaves externas usando a chave externa especificada.

Os valores a seguir são exibidos na seção External key (Chave externa).

ID da chave externa

O identificador da chave externa no gerenciador de chaves externas. Este é o valor que o proxy de armazenamento de chaves externas usa para identificar a chave externa. Você especifica o ID da chave externa ao criar a chave do KMS e não pode alterá-la. Se o valor do ID da chave externa que você usou para criar a chave do KMS for alterado ou se tornar inválido, você deverá agendar a exclusão da chave do KMS e criar uma nova chave do KMS com o valor correto do ID da chave externa.

Visualizar chaves do KMS em um armazenamento de chaves externas (console)

Para visualizar chaves do KMS em um armazenamento de chaves externas (console)

1. Abra o console do AWS KMS em https://console.aws.amazon.com/kms.
2. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.
3. No painel de navegação, escolha Customer managed keys (Chaves gerenciadas pelo cliente).
4. Para identificar as chaves do KMS em seu armazenamento de chaves externas, adicione os campos Origin (Origem) e Custom key store ID (ID do armazenamento de chaves personalizado) à tabela de chaves. As chaves do KMS em qualquer armazenamento de chaves externas têm um valor de origem de armazenamento de chaves externas.

   No canto superior direito, selecione o ícone de engrenagem, escolha Origin (Origem), Custom key store ID (ID de armazenamento de chaves personalizado) e escolha Confirm (Confirmar).
5. Escolha o alias ou ID de chave de uma chave do KMS em um armazenamento de chaves externas.
6. Para visualizar as propriedades específicas das chaves do KMS em um armazenamento de chaves externas, escolha a guia Cryptographic configuration (Configuração criptográfica). Valores especiais para chaves do KMS em um armazenamento de chaves externas são exibidos nas seções Custom key store (Armazenamento de chaves personalizado) e External key (Chave externa).

Visualizar chaves do KMS em um armazenamento de chaves externas (API do AWS KMS)

Para visualizar chaves do KMS em um armazenamento de chaves externas (API)

Você usa as mesmas operações de AWS KMS API para visualizar as chaves KMS em um armazenamento de chaves externo que você usaria para qualquer chave KMS, incluindo

ListKeysDescribeKey, e. GetKeyPolicy Por exemplo, a seguinte operação `describe-key` na AWS CLI mostra os campos especiais de uma chave do KMS em um armazenamento de chaves externas. Antes de executar um comando como esse, substitua o ID de exemplo por um valor válido.

```
$ 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"
    }
  }
}
```

Usar chaves do KMS em um armazenamento de chaves externas

Após criar uma chave do KMS de criptografia simétrica em um armazenamento de chaves externas, é possível usá-la para as seguintes operações de criptografia:

- Encrypt
- Decrypt
- GenerateDataKey
- GenerateDataKeyWithoutPlaintext
- ReEncrypt

As operações de criptografia simétrica que geram pares de chaves de dados assimétricos GenerateDataKeyPaire GenerateDataKeyPairWithoutPlaintext, não são suportadas em armazenamentos de chaves personalizadas.

Um contexto de criptografia é compatível com todas as operações de criptografia com chaves do KMS em um armazenamento de chaves externas. Como sempre, usar um contexto de criptografia é uma das práticas de segurança recomendadas pelo AWS KMS.

Ao usar sua chave do KMS em uma solicitação, identifique a chave do KMS pelo ID de chave, ARN de chave, alias ou ARN do alias. Não é necessário especificar o armazenamento de chaves externas. A resposta inclui os mesmos campos que são retornados para qualquer chave do KMS de criptografia simétrica. Porém, quando você usa uma chave do KMS em um armazenamento de chaves externas, as operações de criptografia e descriptografia são executadas pelo gerenciador de chaves externas usando a chave externa que está associada à chave do KMS.

Para garantir que o texto cifrado criptografado por uma chave do KMS em um armazenamento de chaves externas seja pelo menos tão seguro quanto o texto cifrado criptografado por uma chave do KMS padrão, o AWS KMS usa criptografia dupla. Os dados são criptografados no AWS KMS usando material de chave do AWS KMS. Em seguida, ele é criptografado pelo gerenciador de chaves externas usando a chave externa para a chave do KMS. Para descriptografar texto cifrado com criptografia dupla, o texto cifrado é primeiro descriptografado pelo gerenciador de chaves externas usando a chave externa para a chave do KMS. Em seguida, ele é descriptografado no AWS KMS usando o material de chave do AWS KMS para a chave do KMS.

Para tornar isso possível, as seguintes condições são necessárias.

- O estado de chave da chave do KMS deve ser `Enabled`. Para encontrar o estado da chave, consulte o campo Status das chaves gerenciadas pelo cliente, o AWS KMSconsole ou o `KeyState` campo na DescribeKeyresposta.
- O armazenamento de chaves externas que hospeda a chave do KMS deve estar conectado ao proxy de armazenamento de chaves externas, ou seja, o estado da conexão do armazenamento de chaves externas deve ser `CONNECTED`.

  Você pode ver o estado da conexão na página Armazenamentos externos de chaves no AWS KMS console ou na DescribeCustomKeyStoresresposta. O estado de conexão do armazenamento de chaves externas também é exibido na página de detalhes da chave do KMS no console do AWS KMS. Na página de detalhes, escolha a guia Cryptographic configuration (Configuração criptográfica) e veja o campo Connection state (Estado da conexão) na seção Custom key store (Armazenamento de chaves personalizado).

Se o estado da conexão for `DISCONNECTED`, primeiro é necessário conectá-lo. Se o estado da conexão for `FAILED`, você deverá resolver o problema, desconectar o armazenamento de chaves externas e conectá-lo. Para obter instruções, consulte Conectar e desconectar um armazenamento de chaves externas.

- O proxy de armazenamento de chaves externas deve ser capaz de encontrar a chave externa.
- A chave externa deve estar habilitada e deve executar criptografia e descriptografia.

  O status da chave externa é independente e não é afetado por alterações no estado da chave da chave do KMS, inclusive habilitar e desabilitar a chave do KMS. Da mesma forma, desabilitar ou excluir a chave externa não alterará o estado da chave do KMS, mas as operações de criptografia que usam a chave do KMS associada falharão.

Se essas condições não forem atendidas, haverá falha na operação de criptografia, e o AWS KMS retornará uma exceção `KMSInvalidStateException`. Talvez seja necessário reconectar o armazenamento de chaves externas ou usar as ferramentas do gerenciador de chaves externas para reconfigurar ou reparar a chave externa. Para obter ajuda adicional, consulte the section called "Solução de problemas de armazenamentos de chaves externas".

Ao usar as chaves do KMS em um armazenamento de chaves externas, esteja ciente de que as chaves do KMS em cada armazenamento de chaves externas compartilha uma cota de solicitações de armazenamento de chaves personalizado para operações de criptografia. Se você exceder a cota, o AWS KMS retornará um `ThrottlingException`. Para obter detalhes sobre a cota de solicitações do armazenamento de chaves personalizado, consulte Cotas de solicitação de armazenamento de chaves personalizadas.

Agendar a exclusão de chaves do KMS de um armazenamento de chaves externas

Quando tiver certeza de que não será necessário usar uma AWS KMS key para nenhuma operação criptográfica, você poderá programar a exclusão da chave do KMS. Use o mesmo procedimento que você usaria para programar a exclusão de qualquer chave do KMS do AWS KMS. Excluir uma chave do KMS de um armazenamento de chaves externas não afetará a chave externa que serviu como material de chave.

Você pode cancelar a exclusão programada de uma chave do KMS durante o período de espera programada. No entanto, não é possível recuperar uma chave do KMS excluída. Você não pode recriar uma chave do KMS de criptografia simétrica em um armazenamento de chaves externas, mesmo que você use a mesma chave externa. Como cada chave do KMS simétrica em um

armazenamento de chaves externas tem material de chave do AWS KMS e metadados exclusivos, somente a chave do AWS KMS que criptografou um texto cifrado simétrico pode descriptografá-la.

> **Warning**
>
> A exclusão de uma chave do KMS é uma operação destrutiva e potencialmente perigosa que evita a recuperação de todos os dados criptografados sob essa chave do KMS. Antes de programar a exclusão da chave KMS, examine o uso anterior da chave KMS e crie um CloudWatch alarme da Amazon que alerta você quando alguém tentar usar a chave KMS enquanto ela estiver pendente de exclusão. Sempre que possível, desabilite a chave do KMS em vez de excluí-la.

Se você agendar a exclusão de uma chave do KMS de um armazenamento de chaves externas, o estado da chave será alterado para Pending deletion (Exclusão pendente). A chave do KMS permanecerá no estado Pending deletion (Exclusão pendente) durante todo o período de espera, mesmo que ela fique indisponível porque você desconectou o armazenamento de chaves externas. Isso permite que você cancele a exclusão da chave do KMS a qualquer momento durante o período de espera. Quando o período de espera expirar, o AWS KMS excluirá a chave do KMS do AWS KMS.

Quando você agenda a exclusão de uma chave do KMS de um armazenamento de chaves externas, a chave do KMS torna-se inutilizável imediatamente (sujeita a consistência posterior). Contudo, os recursos criptografados com chaves de dados protegidas pela chave do KMS não serão afetados até que a chave do KMS seja usada novamente, por exemplo, para descriptografar a chave de dados. Esse problema afeta os Serviços da AWS, pois muitos deles usam chaves de dados para proteger recursos. Para obter detalhes, consulte Como as chaves do KMS inutilizáveis afetam as chaves de dados.

Você pode monitorar o agendamento, o cancelamento e a exclusão da chave do KMS em seus logs do AWS CloudTrail.

Solução de problemas de armazenamentos de chaves externas

A resolução da maioria dos problemas com armazenamentos de chaves externos é indicada pela mensagem de erro AWS KMS exibida com cada exceção ou pelo código de erro de conexão que AWS KMS retorna quando uma tentativa de conectar o armazenamento de chaves externo ao proxy externo do armazenamento de chaves falha. Porém, alguns problemas são um pouco mais complexos.

Ao diagnosticar um problema com um armazenamento de chaves externas, primeiro localize a causa. Isso reduzirá a variação de soluções e tornará a solução de problemas mais eficiente.

- AWS KMS — O problema pode estar dentro AWS KMS, como um valor incorreto na configuração do armazenamento de chaves externo.
- Externo — O problema pode ter origem externa AWS KMS, incluindo problemas com a configuração ou operação do proxy externo do armazenamento de chaves, do gerenciador de chaves externo, das chaves externas ou do serviço de endpoint VPC.
- Redes: pode ser um problema de conectividade ou de redes, como um problema com o proxy de endpoint, porta ou nome ou domínio de DNS privado.

> **Note**
>
> Quando as operações de gerenciamento em armazenamentos de chaves externas falham, elas geram várias exceções diferentes. Mas as operações AWS KMS criptográficas retornam `KMSInvalidStateException` para todas as falhas relacionadas à configuração externa ou ao estado da conexão do armazenamento de chaves externo. Para identificar o problema, use o texto da mensagem de erro que o acompanha.
>
> A ConnectCustomKeyStoreoperação é bem-sucedida rapidamente antes que o processo de conexão seja concluído. Para determinar se o processo de conexão foi bem-sucedido, veja o estado da conexão do armazenamento de chaves externas. Se o processo de conexão falhar, o AWS KMS retornará um código de erro de conexão que explica a causa e sugere uma solução.

Tópicos

- Ferramentas de solução de problemas de armazenamentos de chaves externas
- Erros de configuração
- Erros de conexão do armazenamento de chaves externas
- Erros de latência e de tempo limite
- Erros de credenciais de autenticação
- Erros de estado da chave
- Erros de descriptografia
- Erros de chave externa

- Problemas de proxy
- Problemas de autorização de proxy

Ferramentas de solução de problemas de armazenamentos de chaves externas

AWS KMS fornece várias ferramentas para ajudá-lo a identificar e resolver problemas com seu armazenamento de chaves externo e suas chaves. Use essas ferramentas em conjunto com as ferramentas fornecidas com o proxy de armazenamento de chaves externas e o gerenciador de chaves externas.

> **Note**
>
> Seu proxy de armazenamento de chaves externas e seu gerenciador de chaves externas podem fornecer métodos mais fáceis de criar e manter seu armazenamento de chaves externas e as respectivas chaves do KMS. Para obter detalhes, consulte a documentação de suas ferramentas externas.

AWS KMS exceções e mensagens de erro

AWS KMS fornece uma mensagem de erro detalhada sobre qualquer problema encontrado. Você pode encontrar informações adicionais sobre AWS KMS exceções na Referência da AWS Key Management Service API e nos AWS SDKs. Mesmo se você estiver usando o AWS KMS console, talvez essas referências sejam úteis. Por exemplo, consulte a lista de erros da operação `CreateCustomKeyStores`.

Se o problema surgir em um AWS serviço diferente, como quando você usa uma chave KMS em seu armazenamento de chaves externo para proteger um recurso em outro AWS serviço, o AWS serviço pode fornecer informações adicionais para ajudá-lo a identificar o problema. Se o AWS serviço não fornecer a mensagem, você poderá ver a mensagem de erro nos CloudTrail registros que registram o uso da sua chave KMS.

CloudTrail troncos

Cada operação AWS KMS da API, incluindo ações no AWS KMS console, é registrada em AWS CloudTrail registros. AWS KMS registra uma entrada de registro para operações bem-sucedidas e malsucedidas. Para operações com falha, a entrada de log inclui o nome da exceção do AWS KMS (`errorCode`) e a mensagem de erro (`errorMessage`). Use essas informações para ajudar

a identificar e resolver o erro. Para ver um exemplo, consulte Descriptografar falhas com uma chave do KMS em um armazenamento de chaves externas.

A entrada de log também inclui o ID da solicitação. Se a solicitação atingiu seu proxy de armazenamento de chaves externas, você poderá usar o ID da solicitação na entrada de log para encontrar a solicitação correspondente em seus logs de proxy, caso o proxy os forneça.

CloudWatch métricas

AWS KMS registra CloudWatch métricas detalhadas da Amazon sobre a operação e o desempenho do seu armazenamento de chaves externo, incluindo latência, limitação, erros de proxy, status do gerenciador de chaves externo, o número de dias até que seu certificado TLS expire e a idade relatada de suas credenciais de autenticação de proxy. Você pode usar essas métricas para desenvolver modelos de dados para a operação do seu armazenamento externo de chaves e CloudWatch alarmes que alertem você sobre problemas iminentes antes que eles ocorram.

> **Important**
>
> AWS KMS recomenda que você crie CloudWatch alarmes para monitorar as métricas externas do armazenamento de chaves. Esses alarmes alertarão sobre os primeiros sinais de problemas antes que eles se desenvolvam.

Grafos de monitoramento

AWS KMS exibe gráficos das CloudWatch métricas do armazenamento de chaves externo na página de detalhes de cada armazenamento de chaves externo no AWS KMS console. Você pode usar os dados nos gráficos para ajudar a localizar a origem dos erros, detectar problemas iminentes, estabelecer linhas de base e refinar seus limites de alarme. CloudWatch Para obter detalhes sobre como interpretar os grafos de monitoramento e usar seus dados, consulte Monitorar um armazenamento de chaves externas.

Exibições de armazenamentos de chaves externas e chaves do KMS

AWS KMS exibe informações detalhadas sobre seus armazenamentos de chaves externos e as chaves KMS no armazenamento de chaves externo no AWS KMS console e na resposta às DescribeCustomKeyStoresDescribeKeyoperações e. Essas exibições incluem campos especiais para armazenamentos de chaves externas e chaves do KMS com informações que você pode usar para solucionar problemas, como o estado da conexão do armazenamento de

chaves externas e o ID da chave externa associada à chave do KMS. Para obter mais detalhes, consulte Visualizar um armazenamento de chaves externas e Visualizar chaves do KMS em um armazenamento de chaves externas.

Cliente de teste do proxy XKS

AWS KMS fornece um cliente de teste de código aberto que verifica se o proxy externo do armazenamento de chaves está em conformidade com a especificação da API AWS KMS External Key Store Proxy. Você pode usar esse cliente de teste para identificar e resolver problemas com seu proxy de armazenamento de chaves externas.

Erros de configuração

Ao criar um armazenamento de chaves externas, você especifica valores de propriedade que abrangem a configuração do armazenamento de chaves externas, como a credencial de autenticação do proxy, o endpoint do URI do proxy, o caminho do URI do proxy e o nome do serviço de endpoint da VPC. Quando AWS KMS detecta um erro no valor de uma propriedade, a operação falha e retorna um erro que indica o valor defeituoso.

Muitos problemas de configuração podem ser resolvidos ao corrigir o valor incorreto. Você pode corrigir um caminho do URI do proxy inválido ou uma credencial de autenticação do proxy sem desconectar o armazenamento de chaves externas. Para obter definições desses valores, inclusive requisitos de exclusividade, consulte Organizar os pré-requisitos. Para obter instruções sobre como atualizar esses valores, consulte Editar propriedades do armazenamento de chaves externas.

Para evitar erros com o caminho do URI do proxy e os valores da credencial de autenticação do proxy, ao criar ou atualizar o armazenamento de chaves externas, carregue um arquivo de configuração de proxy para o console do AWS KMS . É um arquivo baseado em JSON com caminho do URI do proxy e valores de credencial de autenticação de proxy que é fornecido pelo proxy de armazenamento de chaves externas ou pelo gerenciador de chaves externas. Você não pode usar um arquivo de configuração de proxy com operações de AWS KMS API, mas pode usar os valores no arquivo para ajudá-lo a fornecer valores de parâmetros para suas solicitações de API que correspondam aos valores em seu proxy.

Erros gerais de configuração

Exceções: `CustomKeyStoreInvalidStateException` (`CreateKey`), `KMSInvalidStateException` (operações de criptografia), `XksProxyInvalidConfigurationException` (operações de gerenciamento, exceto para `CreateKey`)

Códigos de erro de conexão: `XKS_PROXY_INVALID_CONFIGURATION`, `XKS_PROXY_INVALID_TLS_CONFIGURATION`

Para armazenamentos de chaves externos com conectividade de endpoint público, AWS KMS testa os valores da propriedade ao criar e atualizar o armazenamento de chaves externo. Para armazenamentos de chaves externas com conectividade de serviço de endpoint da VPC, o AWS KMS testa os valores das propriedades ao criar e atualizar o armazenamento de chaves externas.

> **Note**
>
> A operação `ConnectCustomKeyStore`, que é assíncrona, pode ser bem-sucedida mesmo que a tentativa de conectar o armazenamento de chaves externas ao proxy de armazenamento de chaves externas falhe. Nesse caso, não há exceção, mas o estado da conexão do armazenamento de chaves externas é Failed, e um código de erro de conexão explica a mensagem de erro. Para ter mais informações, consulte Erros de conexão do armazenamento de chaves externas.

Se AWS KMS detectar um erro no valor de uma propriedade, a operação falhará e retornará `XksProxyInvalidConfigurationException` com uma das seguintes mensagens de erro.

O proxy de armazenamento de chaves externas rejeitou a solicitação devido a um caminho de URI inválido. Verifique o caminho do URI para o armazenamento de chaves externas e atualize, se necessário.

- O caminho do URI do proxy é o caminho base para AWS KMS solicitações às APIs do proxy. Se o caminho estiver incorreto, todas as solicitações ao proxy falharão. Para visualizar o caminho atual do URI do proxy para o armazenamento de chaves externas, use o console do AWS KMS ou a operação `DescribeCustomKeyStores`. Para encontrar o caminho correto do URI do proxy, consulte a documentação do proxy de armazenamento de chaves externas. Para obter ajuda na correção do valor do caminho do URI do proxy, consulte Editar propriedades do armazenamento de chaves externas.
- O caminho do URI do proxy para o proxy de armazenamento de chaves externas pode ser alterado com as atualizações no proxy de armazenamento de chaves externas ou no gerenciador de chaves externas. Para obter informações sobre essas alterações, consulte a documentação do proxy de armazenamento de chaves externas ou do gerenciador de chaves externas.

`XKS_PROXY_INVALID_TLS_CONFIGURATION`
O AWS KMS não consegue estabelecer uma conexão TLS com o proxy de armazenamento de chaves externas. Verifique a configuração do TLS, inclusive o certificado.

- Todos os proxies de armazenamento de chaves externas precisam de um certificado TLS. O certificado TLS deve ser emitido por uma autoridade de certificação (CA) pública com suporte para armazenamentos de chaves externas. Para ver uma lista de CAs compatíveis, consulte Trusted Certificate Authorities (Autoridades de certificação confiáveis) em AWS KMS External Key Store Proxy API Specification (Especificação da API de proxy de armazenamento de chaves externas do).
- Para conectividade de endpoints públicos, o nome comum (CN) da entidade no certificado TLS deve corresponder ao nome do domínio no endpoint do URI do proxy do armazenamento de chaves externas. Por exemplo, se o endpoint público for https://myproxy.xks.example.com, o TLS, o CN no certificado TLS deverá ser `myproxy.xks.example.com` ou `*.xks.example.com`.
- Para conectividade de serviços de endpoint da VPC, o nome comum (CN) do assunto no certificado TLS deve corresponder ao nome DNS privado do serviço de endpoint da VPC. Por exemplo, se o nome DNS privado for myproxy-private.xks.example.com, o CN no certificado TLS deverá ser `myproxy-private.xks.example.com` ou `*.xks.example.com`.
- O certificado TLS não pode ter expirado. Para obter o prazo de validade de um certificado TLS, use ferramentas SSL, como o OpenSSL. Para monitorar a data de expiração de um certificado TLS associado a um armazenamento de chaves externo, use a XksProxyCertificateDaysToExpire CloudWatch métrica. O número de dias até a data de expiração da certificação TLS também aparece na seção Monitoramento do AWS KMS console.
- Se você estiver usando conectividade de endpoint público, use ferramentas de teste SSL para testar a configuração de SSL. Os erros de conexão TLS podem ser resultado do encadeamento incorreto de certificados.

Erros de configuração de conectividade do serviço de endpoint da VPC

Exceções: `XksProxyVpcEndpointServiceNotFoundException`, `XksProxyVpcEndpointServiceInvalidConfigurationException`

Além dos problemas gerais de conectividade, você pode encontrar os seguintes problemas ao criar, conectar ou atualizar um armazenamento de chaves externo com a conectividade do serviço de endpoint VPC. AWS KMS testa os valores das propriedades de um armazenamento de

chaves externo com a conectividade do serviço de endpoint VPC ao criar, conectar e atualizar o armazenamento de chaves externo. Quando as operações de gerenciamento falham devido a erros de configuração, elas geram as seguintes exceções:

`XksProxyVpcEndpointServiceNotFoundException`

A causa pode ser uma das seguintes:

- Um nome de serviço de endpoint da VPC incorreto. Verifique se o nome do serviço de endpoint da VPC para o armazenamento de chaves externas está correto e corresponde ao valor do endpoint do URI do proxy para o armazenamento de chaves externas. Para encontrar o nome do serviço do VPC endpoint, use o console Amazon VPC ou a operação. DescribeVpcEndpointServices Para encontrar o nome do serviço do VPC endpoint e o endpoint do URI do proxy de um armazenamento de chaves externo existente, use o AWS KMS console ou a operação. DescribeCustomKeyStores Para obter detalhes, consulte Visualizar um armazenamento de chaves externas.
- O serviço de endpoint da VPC pode estar em um local Região da AWS diferente do armazenamento de chaves externo. Verifique se o serviço de endpoint da VPC e o armazenamento de chaves externas estão na mesma região. (O nome externo do nome da região, como, faz parte do nome do serviço do VPC endpoint`us-east-1`, como com.amazonaws.vpce.us-east-1. vpce-svc-example.) Para obter uma lista dos requisitos do serviço de endpoint da VPC para um armazenamento de chaves externas, consulte Serviço de VPC endpoint. Você não pode migrar um serviço de endpoint da VPC ou um armazenamento de chaves externas para uma região diferente. Contudo, você pode criar um novo armazenamento de chaves externas na mesma região do serviço de endpoint da VPC. Para obter mais detalhes, consulte Configurar a conectividade do serviço de endpoint da VPC e Criar um armazenamento de chaves externas.
- AWS KMS não é um principal permitido para o serviço de endpoint da VPC. A lista de entidades principais autorizadas para o serviço de endpoint da VPC deve incluir o valor de `cks.kms.<region>.amazonaws.com`, como `cks.kms.eu-west-3.amazonaws.com`. Para obter instruções sobre como adicionar esse valor, consulte Manage permissions (Gerenciar permissões) no Guia do AWS PrivateLink .

`XksProxyVpcEndpointServiceInvalidConfigurationException`

Esse erro ocorre quando o serviço de endpoint da VPC não atende a um dos seguintes requisitos:

- A VPC requer pelo menos duas sub-redes privadas, cada uma em uma zona de disponibilidade diferente. Para obter ajuda para adicionar uma sub-rede à sua VPC, consulte Crie uma sub-rede na VPC no Guia do usuário da Amazon VPC.
- Seu tipo de serviço de endpoint da VPC deve usar um balanceador de carga de rede, não um balanceador de carga de gateway.
- A aceitação não deve ser obrigatória para o serviço de endpoint da VPC (Acceptance required [Aceitação obrigatória] deve ser false). Se a aceitação manual de cada solicitação de conexão for necessária, AWS KMS não será possível usar o serviço de VPC endpoint para se conectar ao proxy externo do armazenamento de chaves. Para obter detalhes, consulte Accept or reject connection requests (Aceitar ou rejeitar solicitações de conexão) no Guia do AWS PrivateLink .
- O serviço de endpoint da VPC deve ter um nome DNS privado que seja o subdomínio de um domínio público. Por exemplo, se o nome DNS privado for `https://myproxy-private.xks.example.com`, os domínios `xks.example.com` ou `example.com` devem ter um servidor DNS público. Para visualizar ou alterar o nome DNS privado do serviço de endpoint da VPC, consulte Manage DNS names for VPC endpoint services (Gerenciar nomes de DNS para serviços de endpoint da VPC) no Guia do AWS PrivateLink .
- O status da verificação do domínio do domínio de seu nome DNS privado deverá ser `verified`. Para visualizar e atualizar o status de verificação do domínio do nome DNS privado, consulte Verificar o domínio do DNS privado. Pode levar alguns minutos para que o status de verificação atualizado seja exibido depois que você adicionar o registro de texto obrigatório.

  > **Note**
  >
  > O domínio DNS privado só poderá ser verificado se for o subdomínio de um domínio público. Caso contrário, o status de verificação do domínio DNS privado não será alterado, mesmo depois de adicionar o registro TXT obrigatório.

- O nome DNS privado do serviço de endpoint da VPC deve corresponder ao valor do endpoint do URI do proxy para o armazenamento de chaves externas. Para um armazenamento de chaves externas com conectividade de serviço de endpoint da VPC, o endpoint do URI do proxy deve ser `https://` seguido pelo nome DNS privado do serviço de endpoint da VPC. Para visualizar o valor do endpoint do URI do proxy, consulte Visualizar um armazenamento de chaves externas. Para alterar o valor do endpoint do URI do proxy, consulte Editar propriedades do armazenamento de chaves externas.

Erros de conexão do armazenamento de chaves externas

O processo de conexão de um armazenamento de chaves externas ao proxy de armazenamento de chaves externas leva cerca de cinco minutos para ser concluído. A menos que se antecipe à falha, a operação `ConnectCustomKeyStore` retornará uma resposta HTTP 200 e um objeto JSON sem propriedades. No entanto, essa resposta inicial não indica que a conexão foi bem-sucedida. Para determinar se o armazenamento de chaves externas está conectado, consulte o estado da conexão. Se a conexão falhar, o estado da conexão do armazenamento de chaves externo mudará para `FAILED` e AWS KMS retornará um código de erro de conexão que explica a causa da falha.

> **Note**
>
> Quando o estado de conexão de um armazenamento de chaves personalizado é `FAILED`, você deve desconectar o armazenamento de chaves personalizado antes de tentar reconectá-lo. Não é possível conectar um armazenamento de chaves personalizado a um status de conexão `FAILED`.

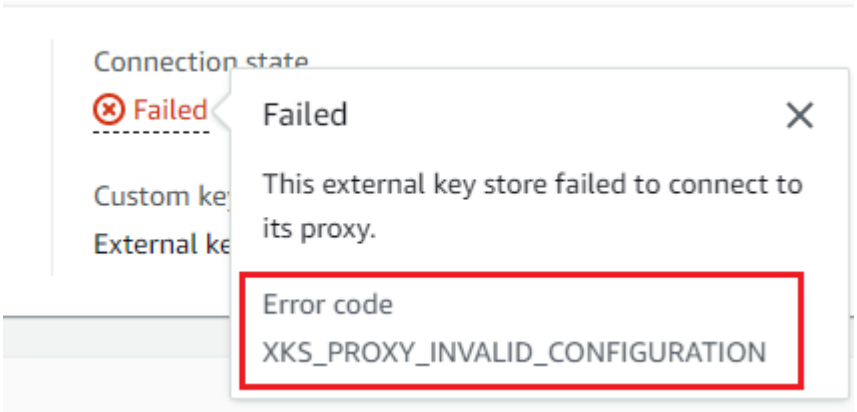
Para visualizar o estado da conexão de um armazenamento de chaves externas:

- Na DescribeCustomKeyStoresresposta, visualize o valor do `ConnectionState` elemento.
- No AWS KMS console, o estado da conexão aparece na tabela de armazenamento de chaves externo. Além disso, na página de detalhes de cada armazenamento de chaves externas, o estado da conexão é exibido na seção General configuration (Configuração geral).

Quando o estado da conexão é `FAILED`, o código de erro de conexão ajuda a explicar o erro.

Para visualizar o código de erro de conexão:

- Na DescribeCustomKeyStoresresposta, visualize o valor do `ConnectionErrorCode` elemento. Este elemento aparece na resposta de `DescribeCustomKeyStores` somente quando `ConnectionState` é `FAILED`.
- Para visualizar o código de erro de conexão no AWS KMS console, na página de detalhes do armazenamento externo de chaves e passe o mouse sobre o valor Falha.



Códigos de erro de conexão para armazenamentos de chaves externas

Os códigos de erro de conexão a seguir se aplicam a armazenamentos de chaves externas

`INTERNAL_ERROR`

AWS KMS não foi possível concluir a solicitação devido a um erro interno. Repetir a solicitação . Para solicitações `ConnectCustomKeyStore`, desconecte o armazenamento de chaves personalizado antes de tentar se conectar novamente.

`INVALID_CREDENTIALS`

Um ou ambos os valores de `XksProxyAuthenticationCredential` não são válidos no proxy de armazenamento de chaves externas especificado.

`NETWORK_ERRORS`

Os erros de rede estão AWS KMS impedindo a conexão do armazenamento de chaves personalizadas ao armazenamento de chaves de apoio.

`XKS_PROXY_ACCESS_DENIED`

AWS KMS as solicitações têm acesso negado ao proxy externo do armazenamento de chaves. Se o proxy de armazenamento de chaves externas tiver regras de autorização, verifique se elas permitem que o AWS KMS se comunique com o proxy em seu nome.

`XKS_PROXY_INVALID_CONFIGURATION`

Um erro de configuração está impedindo que o armazenamento de chaves externas se conecte ao proxy. Verifique o valor de `XksProxyUriPath`.

`XKS_PROXY_INVALID_RESPONSE`

AWS KMS não é possível interpretar a resposta do proxy externo do armazenamento de chaves. Caso veja esse código de erro de conexão repetidamente, notifique seu fornecedor de proxy de armazenamento de chaves externas.

`XKS_PROXY_INVALID_TLS_CONFIGURATION`

AWS KMS não é possível se conectar ao proxy externo do armazenamento de chaves porque a configuração do TLS é inválida. Verifique se o proxy de armazenamento de chaves externas é compatível com TLS 1.2 ou 1.3. Além disso, verifique se o certificado TLS não expirou, se corresponde ao nome do host no valor `XksProxyUriEndpoint` e se está assinado por uma autoridade de certificação confiável incluída na lista de autoridades de certificação confiáveis.

`XKS_PROXY_NOT_REACHABLE`

AWS KMS não consegue se comunicar com seu proxy externo de armazenamento de chaves. Verifique se `XksProxyUriEndpoint` e `XksProxyUriPath` estão corretos. Use as ferramentas do proxy de armazenamento de chaves externas para verificar se o proxy está ativo e disponível em sua rede. Além disso, verifique se as instâncias do gerenciador de chaves externas estão operando corretamente. As tentativas de conexão falharão com esse código de erro de conexão se o proxy relatar que todas as instâncias do gerenciador de chaves externas estão indisponíveis.

`XKS_PROXY_TIMED_OUT`

AWS KMS pode se conectar ao proxy externo do armazenamento de chaves, mas o proxy não responde AWS KMS no tempo alocado. Caso veja esse código de erro de conexão repetidamente, notifique seu fornecedor de proxy de armazenamento de chaves externas.

`XKS_VPC_ENDPOINT_SERVICE_INVALID_CONFIGURATION`

A configuração do serviço de endpoint do Amazon VPC não está em conformidade com os requisitos de um AWS KMS armazenamento de chaves externo.

- O serviço de endpoint da VPC deve ser um serviço de endpoint para endpoints de interface na Conta da AWS do autor da chamada.
- Deve ter um balanceador de carga de rede (NLB) conectado a pelo menos duas sub-redes, cada uma em uma zona de disponibilidade diferente.
- A `Allow principals` lista deve incluir o principal AWS KMS de serviço da região,`cks.kms.<region>.amazonaws.com`, tal como`cks.kms.us-east-1.amazonaws.com`.
- Não deve exigir a aceitação de solicitações de conexão.

- Ele deve ter um nome DNS privado. O nome DNS privado de um armazenamento de chaves externas com conectividade `VPC_ENDPOINT_SERVICE` deve ser exclusivo na Região da AWS.
- O domínio do nome DNS privado deve ter o status de verificação `verified`.
- O certificado TLS especifica o nome de host DNS privado no qual o endpoint é acessível.

`XKS_VPC_ENDPOINT_SERVICE_NOT_FOUND`

AWS KMS não consigo encontrar o serviço de endpoint VPC que ele usa para se comunicar com o proxy externo do armazenamento de chaves. Verifique se `XksProxyVpcEndpointServiceName` está correto e se a entidade principal do serviço do AWS KMS tem permissões de consumidor no serviço de endpoint da Amazon VPC.

Erros de latência e de tempo limite

Exceções: `CustomKeyStoreInvalidStateException` (`CreateKey`), `KMSInvalidStateException` (operações de criptografia), `XksProxyUriUnreachableException` (operações de gerenciamento)

Códigos de erro de conexão: `XKS_PROXY_NOT_REACHABLE`, `XKS_PROXY_TIMED_OUT`

Quando não é AWS KMS possível contatar o proxy dentro do intervalo de tempo limite de 250 milissegundos, ele retorna uma exceção. `CreateCustomKeyStoree UpdateCustomKeyStore` retorne`XksProxyUriUnreachableException`. As operações criptográficas retornam o padrão `KMSInvalidStateException` com uma mensagem de erro que descreve o problema. Se `ConnectCustomKeyStore` falhar, AWS KMS retorna um código de erro de conexão que descreve o problema.

Os erros de tempo limite poderão ser problemas transitórios que podem ser resolvidos ao repetir a solicitação. Se o problema persistir, verifique se o proxy de armazenamento de chaves externas está ativo e conectado à rede e se o endpoint do URI do proxy, o caminho do URI do proxy e o nome do serviço de endpoint da VPC (se houver) estão corretos no armazenamento de chaves externas. Além disso, verifique se o gerenciador de chaves externo está próximo ao do Região da AWS armazenamento de chaves externo. Se precisar atualizar qualquer um desses valores, consulte Editar propriedades do armazenamento de chaves externas.

Para rastrear os padrões de latência, use a `XksProxyLatency` CloudWatch métrica e o gráfico de latência média (com base nessa métrica) na seção Monitoramento do AWS KMS console. Seu proxy de armazenamento de chaves externas também pode gerar logs e métricas que rastreiam a latência e os tempos limite.

`XksProxyUriUnreachableException`
AWS KMS não pode se comunicar com o proxy externo do armazenamento de chaves. Pode ser um problema de rede transitório. Caso veja esse erro repetidamente, verifique se o proxy de armazenamento de chaves externas está ativo e conectado à rede e se o URI do endpoint está correto no armazenamento de chaves externas.

- O proxy externo do armazenamento de chaves não respondeu a uma solicitação de API de AWS KMS proxy dentro do intervalo de tempo limite de 250 milissegundos. Isso pode indicar um problema de rede transitório ou um problema operacional ou de performance com o proxy. Se uma nova tentativa não resolver o problema, notifique o administrador do proxy de armazenamento de chaves externas.

Erros de latência e de tempo limite geralmente se manifestam como falhas de conexão. Quando a ConnectCustomKeyStoreoperação falha, o estado da conexão do armazenamento de chaves externo muda para `FAILED` e AWS KMS retorna um código de erro de conexão que explica o erro. Para obter uma lista de códigos de erro de conexão e sugestões para resolver os erros, consulte Códigos de erro de conexão para armazenamentos de chaves externas. As listas de códigos de conexão de todos os armazenamentos de chaves personalizados e Armazenamentos de chaves externas se aplicam aos armazenamentos de chaves externas. Os erros de conexão a seguir estão relacionados à latência e aos tempos limite.

`XKS_PROXY_NOT_REACHABLE`

- ou -

`CustomKeyStoreInvalidStateException` , `KMSInvalidStateException` , `XksProxyUriUnreachableException`
O AWS KMS não consegue se comunicar com o proxy de armazenamento de chaves externas. Verifique se o proxy de armazenamento de chaves externas está ativo e conectado à rede e se o caminho do URI e o URI do endpoint ou o nome do serviço da VPC estão corretos no armazenam ento de chaves externas.

Esse erro poderá ocorrer pelos seguintes motivos:

- O proxy do armazenamento de chaves externas não está ativo ou não está conectado à rede.

- Há um erro nos valores do endpoint do URI do proxy, do caminho do URI do proxy ou do nome do serviço de endpoint da VPC (se aplicável) na configuração do armazenamento de chaves externas. Para visualizar a configuração do armazenamento de chaves externo, use a DescribeCustomKeyStoresoperação ou visualize a página de detalhes do armazenamento de chaves externo no AWS KMS console.
- Pode haver um erro de configuração de rede, como um erro de porta, no caminho de rede entre AWS KMS e o proxy externo do armazenamento de chaves. AWS KMS se comunica com o proxy externo do armazenamento de chaves na porta 443. Esse valor não é configurável.
- Quando o proxy externo do armazenamento de chaves relata (em uma GetHealthStatusresposta) que todas as instâncias externas do gerenciador de chaves sãoUNAVAILABLE, a ConnectCustomKeyStoreoperação falha com um `ConnectionErrorCode` deXKS_PROXY_NOT_REACHABLE. Para obter ajude, consulte a documentação do gerenciador de chaves externas.
- Esse erro pode resultar de uma longa distância física entre o gerenciador de chaves externo e Região da AWS o armazenamento de chaves externo. A latência de ping (tempo de ida e volta da rede (RTT)) entre o Região da AWS e o gerenciador de chaves externo não deve ser superior a 35 milissegundos. Talvez seja necessário criar um armazenamento de chaves externo em um Região da AWS que esteja mais próximo do gerenciador de chaves externo ou mover o gerenciador de chaves externo para um data center mais próximo do Região da AWS.

`XKS_PROXY_TIMED_OUT`

- ou -

`CustomKeyStoreInvalidStateException` , `KMSInvalidStateException` , `XksProxyUriUnreachableException`
O AWS KMS rejeitou a solicitação porque o proxy de armazenamento de chaves externas não respondeu a tempo. Repetir a solicitação . Caso veja esse erro repetidamente, informe-o ao administrador do proxy de armazenamento de chaves externas.

Esse erro poderá ocorrer pelos seguintes motivos:

- Esse erro pode resultar de uma longa distância física entre o gerenciador de chaves externas e o proxy de armazenamento de chaves externas. Se possível, mova o proxy de armazenamento de chaves externas para mais perto do gerenciador de chaves externas.

- Erros de tempo limite podem ocorrer quando o proxy não foi projetado para lidar com o volume e a frequência das solicitações de AWS KMS. Se suas CloudWatch métricas indicarem um problema persistente, notifique o administrador externo do proxy do armazenamento de chaves.
- Podem ocorrer erros de tempo limite quando a conexão entre o gerenciador de chaves externas e a Amazon VPC para o armazenamento de chaves externas não está funcionando corretamente. Se você estiver usando AWS Direct Connect, verifique se sua VPC e seu gerenciador de chaves externo podem se comunicar de forma eficaz. Para obter ajuda para resolver qualquer problema, consulte Solução de problemas AWS Direct Connect no Guia do AWS Direct Connect usuário.

`XKS_PROXY_TIMED_OUT`

- ou -

`CustomKeyStoreInvalidStateException` , `KMSInvalidStateException` , `XksProxyUriUnreachableException`
O proxy de armazenamento de chaves externas não respondeu à solicitação no tempo estipulado. Repetir a solicitação . Caso veja esse erro repetidamente, informe-o ao administrador do proxy de armazenamento de chaves externas.

- Esse erro pode resultar de uma longa distância física entre o gerenciador de chaves externas e o proxy de armazenamento de chaves externas. Se possível, mova o proxy de armazenamento de chaves externas para mais perto do gerenciador de chaves externas.

Erros de credenciais de autenticação

Exceções: `CustomKeyStoreInvalidStateException` (`CreateKey`), `KMSInvalidStateException` (operações de criptografia), `XksProxyIncorrectAuthenticationCredentialException` (operações de gerenciamento, exceto `CreateKey`)

Você estabelece e mantém uma credencial de autenticação AWS KMS em seu proxy externo de armazenamento de chaves. Em seguida, você informa os valores AWS KMS das credenciais ao criar um armazenamento de chaves externo. Para alterar a credencial de autenticação, faça a alteração no proxy de armazenamento de chaves externas. Em seguida, atualize a credencial do armazenamento de chaves externas. Se o proxy alternar a credencial, você deverá atualizar a credencial do armazenamento de chaves externas.

Se o proxy de armazenamento de chaves externas não autenticar uma solicitação assinada com a credencial de autenticação do proxy para seu armazenamento de chaves externas, o efeito dependerá da solicitação:

- `CreateCustomKeyStore` e `UpdateCustomKeyStore` falham com uma `XksProxyIncorrectAuthenticationCredentialException`.
- `ConnectCustomKeyStore` é bem-sucedido, mas a conexão falha. O estado da conexão é `FAILED`, e o código de erro da conexão é `INVALID_CREDENTIALS`. Para obter detalhes, consulte Erros de conexão do armazenamento de chaves externas.
- As operações criptográficas retornam `KMSInvalidStateException` para todos os erros de configuração externa e erros de estado de conexão em um armazenamento de chaves externas. A mensagem de erro que acompanha descreve o problema.

> O proxy de armazenamento de chaves externas rejeitou a solicitação porque não conseguiu autenticar o AWS KMS. Verifique as credenciais para o armazenamento de chaves externas e atualize-as, se necessário.

Esse erro poderá ocorrer pelos seguintes motivos:

- O ID da chave de acesso ou a chave de acesso secreta para o armazenamento de chaves externas não correspondem aos valores estabelecidos no proxy de armazenamento de chaves externas.

  Para corrigir esse erro, atualize a credencial de autenticação do proxy para o armazenamento de chaves externas. Você pode fazer essa alteração sem desconectar o armazenamento de chaves externas.
- Um proxy reverso entre AWS KMS e o proxy externo do armazenamento de chaves pode estar manipulando cabeçalhos HTTP de forma a invalidar as assinaturas SigV4. Para corrigir esse erro, notifique o administrador do proxy.

Erros de estado da chave

Exceções: `KMSInvalidStateException`

Utiliza-se `KMSInvalidStateException` para duas finalidades distintas para as chaves do KMS em armazenamentos de chaves personalizados.

- Quando uma operação de gerenciamento, como `CancelKeyDeletion`, falha e retorna essa exceção, isso indica que o estado da chave do KMS não é compatível com a operação.
- Quando uma operação de criptografia em uma chave do KMS em um armazenamento de chaves personalizado falha com `KMSInvalidStateException`, pode indicar um problema no estado da chave do KMS. Mas a operação AWS KMS criptográfica retorna `KMSInvalidStateException` para todos os erros de configuração externa e erros de estado de conexão em um armazenamento de chaves externo. Para identificar o problema, use o texto da mensagem de erro que acompanha a exceção.

Para encontrar o estado de chave necessário para as operações de uma AWS KMS API, consultePrincipais estados das AWS KMS chaves. Para encontrar o estado de chave de uma chave do KMS, na página Customer managed keys (Chaves gerenciadas pelo cliente), visualize o campo Status da chave do KMS. Ou use a DescribeKeyoperação e visualize o `KeyState` elemento na resposta. Para obter detalhes, consulte Visualizar chaves.

> **Note**
>
> O estado da chave de uma chave do KMS em um armazenamento de chaves externas não indica nada sobre o status da chave externa associada. Para obter informações sobre o status da chave externa, use o gerenciador de chaves externas e as ferramentas de proxy de armazenamento de chaves externas.
> `CustomKeyStoreInvalidStateException` refere-se ao estado da conexão do armazenamento de chaves externas, não ao estado da chave de uma chave do KMS.

Uma operação criptográfica em uma chave do KMS em um armazenamento personalizado poderá falhar se o estado da chave do KMS for `Unavailable` ou `PendingDeletion`. (As chaves desativadas retornam `DisabledException`.)

- Uma chave KMS tem um estado de `Disabled` chave somente quando você desativa intencionalmente a chave KMS no AWS KMS console ou usando a operação. DisableKey Enquanto uma chave do KMS está desabilitada, é possível visualizar e gerenciar a chave, mas não é possível usá-la para operações de criptografia. Para corrigir o problema, habilite a chave. Para obter detalhes, consulte Habilitar e desabilitar chaves.
- Uma chave do KMS tem um estado da chave `Unavailable` quando o armazenamento de chaves externas é desconectado do proxy de armazenamento de chaves externas. Para corrigir uma chave do KMS indisponível, reconecte o armazenamento de chaves externas. Após a

reconexão do armazenamento de chaves externas, o estado de chave das chaves do KMS nesse armazenamento de chaves externas é automaticamente restaurado ao estado anterior, como `Enabled` ou `Disabled`.

Uma chave do KMS tem um estado de chave `PendingDeletion` quando foi programada para exclusão e está no período de espera. Um erro de estado da chave em uma chave do KMS que está pendente de exclusão indica que a chave não deve ser excluída, seja porque está sendo usada para criptografia, seja porque é obrigatória para descriptografia. Para reabilitar a chave do KMS, cancele a exclusão programada e habilite a chave. Para obter detalhes, consulte Programar e cancelar a exclusão de chaves.

Erros de descriptografia

Exceções: `KMSInvalidStateException`

Quando uma operação de descriptografia com uma chave KMS em um armazenamento de chaves externo falha, AWS KMS retorna o padrão `KMSInvalidStateException` que as operações criptográficas usam para todos os erros de configuração externa e erros de estado de conexão em um armazenamento de chaves externo. A mensagem de erro indica o problema.

Para descriptografar um texto cifrado que foi criptografado usando criptografia dupla, o gerenciador de chaves externas usa primeiro a chave externa para descriptografar a camada externa do texto cifrado. Em seguida, AWS KMS usa o material AWS KMS chave na chave KMS para decifrar a camada interna do texto cifrado. O gerenciador de chaves externas ou o AWS KMS podem rejeitar um texto cifrado inválido ou corrompido.

As mensagens de erro a seguir acompanham a `KMSInvalidStateException` quando a descriptografia falha. Isso indica um problema no texto cifrado ou no contexto de criptografia opcional da solicitação.

O proxy de armazenamento de chaves externas rejeitou a solicitação porque o texto cifrado especificado ou os dados autenticados adicionais estão corrompidos, ausentes ou são inválidos.

- Quando o proxy externo do armazenamento de chaves ou o gerenciador de chaves externo relatam que um texto cifrado ou seu contexto de criptografia é inválido, isso normalmente indica um problema com o texto cifrado ou o contexto de criptografia na solicitação enviada para.

`Decrypt` AWS KMS Para `Decrypt` operações, AWS KMS envia ao proxy o mesmo texto cifrado e contexto de criptografia que ele recebe na `Decrypt` solicitação.

Esse erro pode ser causado por um problema de redes em trânsito, como um bit invertido. Repetir a solicitação `Decrypt`. Se o problema persistir, verifique se o texto cifrado não foi alterado ou corrompido. Além disso, verifique se o contexto de criptografia na `Decrypt` solicitação AWS KMS corresponde ao contexto de criptografia na solicitação que criptografou os dados.

O texto cifrado que o proxy de armazenamento de chaves externas enviou para descriptografia, ou o contexto de criptografia, está corrompido, ausente ou é inválido.

- Quando AWS KMS rejeita o texto cifrado recebido do proxy, indica que o gerenciador de chaves externo ou proxy retornou um texto cifrado inválido ou corrompido para. AWS KMS

  Esse erro pode ser causado por um problema de redes em trânsito, como um bit invertido. Repetir a solicitação `Decrypt`. Se o problema persistir, verifique se o gerenciador de chaves externo está funcionando corretamente e se o proxy externo do armazenamento de chaves não altera o texto cifrado que recebe do gerenciador de chaves externo antes de retorná-lo. AWS KMS

Erros de chave externa

A chave externa é uma chave de criptografia do gerenciador de chaves externas que serve como material de chave externa para uma chave do KMS. O AWS KMS não consegue acessar diretamente a chave externa. Ele deve solicitar que o gerenciador de chaves externas (por meio do proxy de armazenamento de chaves externas) use a chave externa para criptografar dados ou descriptografar um texto cifrado.

Você especifica o ID da chave externa em seu gerenciador de chaves externas ao criar uma chave do KMS em seu armazenamento de chaves externas. Você não pode alterar o ID da chave externa depois que a chave do KMS é criada. Para evitar problemas com a chave do KMS, a operação `CreateKey` solicita que o proxy de armazenamento de chaves externas verifique o ID e a configuração da chave externa. Se a chave externa não atender aos requisitos de uso com uma chave do KMS, a operação `CreateKey` falhará com uma exceção e uma mensagem de erro que identificam o problema.

No entanto, poderão ocorrer problemas depois que a chave do KMS for criada. Se uma operação criptográfica falhar devido a um problema com a chave externa, a operação falhará e retornará um `KMSInvalidStateException` com uma mensagem de erro que indica o problema.

CreateKey erros na chave externa

Exceções: `XksKeyAlreadyInUseException`, `XksKeyNotFoundException`, `XksKeyInvalidConfigurationException`

A CreateKeyoperação tenta verificar a ID e as propriedades da chave externa que você fornece no parâmetro ID da chave externa (console) ou `XksKeyId` (API). Essa prática foi criada para detectar erros antes de você tentar usar a chave externa com a chave do KMS.

Chave externa em uso

Cada chave do KMS em um armazenamento de chaves externas deve usar uma chave externa diferente. Quando `CreateKey` reconhece que o ID da chave externa (XksKeyId) de uma chave KMS não é exclusivo no armazenamento de chaves externo, ele falha com um. `XksKeyAlreadyInUseException`

Se você usar vários IDs para a mesma chave externa, `CreateKey` não reconhecerá a duplicata. No entanto, as chaves KMS com a mesma chave externa não são interoperáveis porque têm materiais de AWS KMS chave e metadados diferentes.

Chave externa não encontrada

Quando o proxy externo do armazenamento de chaves relata que não consegue encontrar a chave externa usando o ID da chave externa (XksKeyId) da chave KMS, a `CreateKey` operação falha e retorna `XksKeyNotFoundException` com a seguinte mensagem de erro.

> O proxy de armazenamento de chaves externas rejeitou a solicitação porque não conseguiu localizar a chave externa.

Esse erro poderá ocorrer pelos seguintes motivos:

- Talvez o ID da chave externa (`XksKeyId`) da chave do KMS seja inválido. Para encontrar o ID usado pelo proxy de chaves externas para identificar a chave externa, consulte a documentação do proxy de armazenamento de chaves externas ou do gerenciador de chaves externas.

- A chave externa pode ter sido excluída do gerenciador de chaves externas. Para investigar, use suas ferramentas de gerenciamento de chaves externas. Se a chave externa for excluída permanentemente, use outra chave externa com a chave do KMS. Para obter uma lista ou requisitos da chave externa, consulte Requisitos para uma chave do KMS em um armazenamento de chaves externas.

Requisitos de chaves externas não atendidos

Quando o proxy de armazenamento de chaves externas relata que a chave externa não atende aos requisitos de uso com uma chave do KMS, a operação `CreateKey` apresenta falhas e retorna `XksKeyInvalidConfigurationException` com uma das mensagens de erro abaixo.

A especificação de chave da chave externa deve ser AES_256. A especificação de chave da chave externa especificada é *<key-spec>* .

- A chave externa deve ser uma chave de criptografia simétrica de 256 bits com uma especificação de chave AES_256. Se a chave externa especificada for de um tipo diferente, especifique o ID de uma chave externa que atenda a esse requisito.

O status da chave externa deve ser ENABLED. O status da chave externa especificada é *<status>*.

- A chave externa deve estar habilitada no gerenciador de chaves externas. Se a chave externa especificada não estiver habilitada, use as ferramentas do gerenciador de chaves externas para habilitá-la ou especifique uma chave externa habilitada.

O uso de chave da chave externa deve incluir ENCRYPT e DECRYPT. O uso de chave da chave externa especificada é <*key-usage* >.

- A chave externa deve estar configurada para criptografia e descriptografia no gerenciador de chaves externas. Se a chave externa especificada não incluir essas operações, use as

ferramentas do gerenciador de chaves externas para alterar as operações ou especifique outra chave externa.

Erros de operação de criptografia da chave externa

Exceções: `KMSInvalidStateException`

Quando o proxy de armazenamento de chaves externas não consegue encontrar a chave externa associada à chave do KMS, ou quando a chave externa não atende aos requisitos de uso com uma chave do KMS, a operação de criptografia falha.

Os problemas de chave externa detectados durante uma operação de criptografia são mais difíceis de resolver do que os problemas de chave externa detectados antes de criar a chave do KMS. Você não pode alterar o ID da chave externa depois que a chave do KMS é criada. Se a chave do KMS ainda não tiver criptografado nenhum dado, você poderá excluir a chave do KMS e criar uma nova com outro ID de chave externa. No entanto, o texto cifrado gerado com a chave KMS não pode ser descriptografado por nenhuma outra chave KMS, mesmo com a mesma chave externa, porque as chaves terão metadados e materiais de chave diferentes. AWS KMS Em vez disso, na medida do possível, use suas ferramentas de gerenciamento de chaves externas para resolver o problema com a chave externa.

Quando o proxy de armazenamento de chaves externas relata um problema com a chave externa, as operações criptográficas retornam `KMSInvalidStateException` com uma mensagem de erro que identifica o problema.

Chave externa não encontrada

Quando o proxy externo do armazenamento de chaves relata que não consegue encontrar a chave externa usando o ID da chave externa (XksKeyId) da chave KMS, as operações criptográficas retornam a `KMSInvalidStateException` com a seguinte mensagem de erro.

> O proxy de armazenamento de chaves externas rejeitou a solicitação porque não conseguiu localizar a chave externa.

Esse erro poderá ocorrer pelos seguintes motivos:

- O ID da chave externa (`XksKeyId`) da chave do KMS não é mais válido.

Para encontrar o ID da chave externa associada à sua chave do KMS, visualize os detalhes da chave do KMS. Para encontrar o ID que o proxy de chaves externas usa para identificar a chave externa, consulte a documentação do proxy de armazenamento de chaves externas ou do gerenciador de chaves externas.

AWS KMS verifica o ID da chave externa ao criar uma chave KMS em um armazenamento de chaves externo. Porém, o ID poderá se tornar inválido, sobretudo se o valor do ID da chave externa for um alias ou nome mutável. Você não pode alterar o ID da chave externa associada a uma chave do KMS existente. Para descriptografar qualquer texto cifrado criptografado sob a chave do KMS, é necessário associar novamente a chave externa ao ID da chave externa existente.

Se você ainda não usou a chave do KMS para criptografar dados, poderá criar uma nova chave do KMS com um ID de chave externa válido. No entanto, se você gerou texto cifrado com a chave do KMS, não poderá usar nenhuma outra chave do KMS para descriptografar o texto cifrado, mesmo usando a mesma chave externa.

- A chave externa pode ter sido excluída do gerenciador de chaves externas. Para investigar, use suas ferramentas de gerenciamento de chaves externas. Se possível, tente recuperar o material de chave de uma cópia ou backup do gerenciador de chaves externas. Se a chave externa for excluída permanentemente, todo texto cifrado criptografado sob a chave do KMS associada se tornará irrecuperável.

Erros de configuração de chave externa

Quando o proxy de armazenamento de chaves externas relata que a chave externa não atende aos requisitos de uso com uma chave do KMS, a operação criptográfica retorna `KMSInvalidStateException` com uma das mensagens de erro abaixo.

> O proxy de armazenamento de chaves externas rejeitou a solicitação porque a chave externa não é compatível com a operação solicitada.

- A chave externa deve oferecer suporte a criptografia e descriptografia. Se o uso da chave não incluir criptografia e descriptografia, use suas ferramentas de gerenciamento de chaves externas para alterar o uso da chave.

O proxy de armazenamento de chaves externas rejeitou a solicitação porque a chave externa não está habilitada no gerenciador de chaves externas.

- A chave externa deve estar habilitada e disponível para uso no gerenciador de chaves externas. Se o status da chave externa não for `Enabled`, use as ferramentas do gerenciador de chaves externas para habilitá-la.

Problemas de proxy

Exceções:

`CustomKeyStoreInvalidStateException` (`CreateKey`), `KMSInvalidStateException` (operações de criptografia), `UnsupportedOperationException`, `XksProxyUriUnreachableException`, `XksProxyInvalidResponseException` (operações de gerenciamento, exceto `CreateKey`)

O proxy externo do armazenamento de chaves medeia toda a comunicação entre AWS KMS e o gerenciador de chaves externo. Ele traduz AWS KMS solicitações genéricas em um formato que seu gerente de chaves externo possa entender. Se o proxy externo do armazenamento de chaves não estiver em conformidade com a especificação da API AWS KMS External Key Store Proxy, se não estiver operando corretamente ou não conseguir se comunicar com ele AWS KMS, você não poderá criar ou usar chaves KMS no seu armazenamento de chaves externo.

Embora muitos erros mencionem o proxy de armazenamento de chaves externas por causa de seu papel essencial na arquitetura de armazenamento de chaves externas, esses problemas podem se originar no gerenciador de chaves externas ou na chave externa.

Os problemas nesta seção estão relacionados a problemas no design ou na operação do proxy de armazenamento de chaves externas. A solução desses problemas pode exigir uma alteração no software do proxy. Consulte o administrador do proxy. Para ajudar a diagnosticar problemas de proxy, o AWS KMS fornece o XKS Proxy Text Client, um cliente de teste de código aberto que verifica se seu proxy de armazenamento de chaves externas está em conformidade com a AWS KMS External Key Store Proxy API Specification (Especificação da API de proxy de armazenamento de chaves externas do).

`CustomKeyStoreInvalidStateException` , `KMSInvalidStateException` ou `XksProxyUriUnreachableException`

O proxy de armazenamento de chaves externas está no estado não íntegro. Caso veja essa mensagem repetidamente, notifique o administrador do proxy de armazenamento de chaves externas.

- Esse erro pode indicar um problema operacional ou erro de software no proxy de armazenamento de chaves externas. Você pode encontrar entradas de CloudTrail registro para a operação AWS KMS da API que gerou cada erro. É possível resolver esse erro repetindo a operação. No entanto, se persistir, notifique o administrador do proxy de armazenamento de chaves externas.
- Quando o proxy do armazenamento de chaves externo relata (em GetHealthStatusresposta) que todas as instâncias externas do gerenciador de chaves sãoUNAVAILABLE, as tentativas de criar ou atualizar um armazenamento de chaves externo falham com essa exceção. Se esse erro persistir, consulte a documentação do gerenciador de chaves externas.

`CustomKeyStoreInvalidStateException` , `KMSInvalidStateException` ou `XksProxyInvalidResponseException`

AWS KMS não é possível interpretar a resposta do proxy externo do armazenamento de chaves. Caso veja esse erro repetidamente, consulte o administrador do proxy de armazenamento de chaves externas.

- AWS KMS as operações geram essa exceção quando o proxy retorna uma resposta indefinida que AWS KMS não pode ser analisada ou interpretada. Esse erro poderá ocorrer ocasionalmente devido a problemas externos temporários ou a erros de rede esporádicos. Porém, se persistir, isso pode indicar que o proxy do armazenamento de chaves externas não está em conformidade com a AWS KMS External Key Store Proxy API Specification (Especificação da API de proxy de armazenamento de chaves externas do). Notifique o administrador ou fornecedor do armazenamento de chaves externas.

`CustomKeyStoreInvalidStateException` , `KMSInvalidStateException` ou `UnsupportedOperationException`

O proxy de armazenamento de chaves externas rejeitou a solicitação porque não é compatível com a operação de criptografia solicitada.

- O proxy de armazenamento de chaves externas deve oferecer suporte a todas as APIs de proxy definidas na AWS KMS External Key Store Proxy API Specification (Especificação da API de proxy do armazenamento de chaves externas do). Esse erro indica que o proxy não é compatível com a operação relacionada à solicitação. Notifique o administrador ou fornecedor do armazenamento de chaves externas.

Problemas de autorização de proxy

Exceções: `CustomKeyStoreInvalidStateException`, `KMSInvalidStateException`

Alguns proxies de armazenamento de chaves externas implementam requisitos de autorização para o uso de suas chaves externas. O proxy de armazenamento de chaves externas é permitido, mas não obrigatório, para criar e implementar um esquema de autorização que permita que usuários específicos solicitem operações específicas sob certas condições. Por exemplo, o proxy pode dar ao usuário A permissão para criptografar com uma chave externa específica, mas não para descriptografar com ela. Para ter mais informações, consulte Autorização de proxy de armazenamento de chaves externas (opcional).

A autorização de proxy é baseada nos metadados AWS KMS incluídos em suas solicitações ao proxy. Os campos `awsSourceVpc` e `awsSourceVpce` são incluídos nos metadados somente quando a solicitação vem de um endpoint da VPC e somente quando o autor da chamada está na mesma conta da chave do KMS.

```
"requestMetadata": {
    "awsPrincipalArn": string,
    "awsSourceVpc": string, // optional
    "awsSourceVpce": string, // optional
    "kmsKeyArn": string,
    "kmsOperation": string,
    "kmsRequestId": string,
    "kmsViaService": string // optional
}
```

Quando o proxy rejeita uma solicitação devido a uma falha de autorização, a operação do AWS KMS relacionada apresenta falhas. `CreateKey` retorna `CustomKeyStoreInvalidStateException`. As operações criptográficas do AWS KMS retornam `KMSInvalidStateException`. Ambos usam esta mensagem de erro:

O proxy de armazenamento de chaves externas negou o acesso à operação. Verifique se o usuário e a chave externa estão autorizados para essa operação e repita a solicitação.

- Para resolver o erro, use o gerenciador de chaves externas ou as ferramentas de proxy de armazenamento de chaves externas para determinar por que a autorização falhou. Em seguida, atualize o procedimento que causou a solicitação não autorizada ou use suas ferramentas de proxy de armazenamento de chaves externas para atualizar a política de autorização. Você não pode solucionar este erro no AWS KMS.

Referência de tipos de chaves

O AWS KMS é compatível com diferentes recursos para chaves do KMS de tipos diferentes. Por exemplo, só é possível usar chaves do KMS de criptografia simétrica para gerar chaves de dados simétricas e pares de chaves de dados assimétricas. Além disso, a importação do material de chave e a alternância automática de chaves só são compatíveis com chaves do KMS de criptografia simétrica, e só é possível criar chaves do KMS de criptografia simétrica em um armazenamento personalizado de chaves.

Esta referência contém duas tabelas.

- A tabela de tipos de chaves apresenta as operações do AWS KMS que são válidas para chaves de criptografia do KMS simétricas, chaves do KMS assimétricas e chaves do KMS de HMAC.
- A tabela de recursos especiais apresenta as operações do AWS KMS que são válidas para chaves do KMS multirregionais, chaves do KMS com material de chave importado e chaves do KMS em armazenamentos de chaves personalizados.

Tabela de tipos de chave

Talvez seja necessário rolar horizontalmente ou verticalmente para ver todos os dados nessa tabela.

AWS KMS Operação de API	Chaves do KMS de criptografia simétrica	Chaves do KMS de HMAC	Chaves do KMS assimétricas (ENCRYPT_DECRYPT)	Chaves do KMS assimétricas (SIGN_VERIFY)
CancelKeyDeletion	✓	✓	✓	✓
CreateAlias	✓	✓	✓	✓
CreateGrant	✓	✓	✓	✓
CreateKey	✓	✓	✓	✓
Decrypt	✓	⊗	✓	⊗
DeleteAlias	✓	✓	✓	✓
DeleteImportedKeyMaterial É válido somente em chaves do KMS com material de chave importado (`Origin` é `EXTERNAL`).	✓	✓	✓	✓
DescribeKey	✓	✓	✓	✓
DisableKey	✓	✓	✓	✓
DisableKeyRotation	✓	⊗	⊗	⊗

AWS KMS Operação de API	Chaves do KMS de criptografia simétrica	Chaves do KMS de HMAC	Chaves do KMS assimétricas (ENCRYPT_DECRYPT)	Chaves do KMS assimétricas (SIGN_VERIFY)
	É válido somente em chaves do KMS com material de chave do AWS KMS (`Origin` é `AWS_KMS`).			
EnableKey	✓	✓	✓	✓
EnableKeyRotation	✓ É válido somente em chaves do KMS com material de chave do AWS KMS (`Origin` é `AWS_KMS`).	⊗	⊗	⊗
Encrypt	✓	⊗	✓	⊗
GenerateDataKey	✓	⊗	⊗	⊗

AWS KMS Operação de API	Chaves do KMS de criptografia simétrica	Chaves do KMS de HMAC	Chaves do KMS assimétricas (ENCRYPT_DECRYPT)	Chaves do KMS assimétricas (SIGN_VERIFY)
GenerateDataKeyPair Gera um par de chaves de dados assimétricas que é protegido por uma chave do KMS de criptografia simétrica.	✓ Não é válido com chaves do KMS em armazenamentos de chaves personalizados.	⊗	⊗	⊗
GenerateDataKeyPairWithoutPlaintext Gera um par de chaves de dados assimétricas que é protegido por uma chave do KMS de criptografia simétrica.	✓ Não é válido com chaves do KMS em armazenamentos de chaves personalizados.	⊗	⊗	⊗
GenerateDataKeyWithoutPlaintext	✓	⊗	⊗	⊗
GenerateMac	⊗	✓	⊗	⊗

AWS KMS Operação de API	Chaves do KMS de criptografia simétrica	Chaves do KMS de HMAC	Chaves do KMS assimétricas (ENCRYPT_DECRYPT)	Chaves do KMS assimétricas (SIGN_VERIFY)
GetKeyPolicy	✓	✓	✓	✓
GetKeyRotationStatus	✓	✓ (`KeyRotationEnabled` sempre será `false`.)	✓ (`KeyRotationEnabled` sempre será `false`.)	✓ (`KeyRotationEnabled` sempre será `false`.)
GetParametersForImport É válido somente em chaves do KMS com material de chave importado (`Origin` é `EXTERNAL`).	✓	✓	✓	✓
GetPublicKey	⊗	⊗	✓	✓
ImportKeyMaterial É válido somente em chaves do KMS com material de chave importado (`Origin` é `EXTERNAL`).	✓	✓	✓	✓
ListAliases	✓	✓	✓	✓

AWS KMS Operação de API	Chaves do KMS de criptografia simétrica	Chaves do KMS de HMAC	Chaves do KMS assimétricas (ENCRYPT_DECRYPT)	Chaves do KMS assimétricas (SIGN_VERIFY)
ListGrants	✓	✓	✓	✓
ListKeyPolicies	✓	✓	✓	✓
ListResourceTags	✓	✓	✓	✓
ListRetirableGrants	✓	✓	✓	✓
PutKeyPolicy	✓	✓	✓	✓
ReEncrypt	✓	⊗	✓	⊗
ReplicateKey - Válido somente em chaves de várias regiões	✓	✓	✓	✓
RetireGrant	✓	✓	✓	✓
RevokeGrant	✓	✓	✓	✓
ScheduleKeyDeletion	✓	✓	✓	✓
Sign	⊗	⊗	⊗	✓
TagResource	✓	✓	✓	✓

AWS KMS Operação de API	Chaves do KMS de criptografia simétrica	Chaves do KMS de HMAC	Chaves do KMS assimétricas (ENCRYPT_DECRYPT)	Chaves do KMS assimétricas (SIGN_VERIFY)
UntagResource	✓	✓	✓	✓
UpdateAlias A chave do KMS atual e a nova chave do KMS devem ser do mesmo tipo (ambas simétricas, assimétricas ou HMAC) e devem ter o mesmo uso de chave.	✓	✓	✓	✓
UpdateKeyDescription	✓	✓	✓	✓
UpdateReplicaRegion - Válido somente em chaves de várias regiões	✓	✓	✓	✓
Verificar	⊗	⊗	⊗	✓
VerifyMac	⊗	✓	⊗	⊗

Tabela de recursos especiais

Esta tabela mostra as operações de API do AWS KMS compatíveis com cada tipo de chave de propósito especial.

Ao ler esta tabela, esteja ciente destas interações:

- Chaves de várias regiões:
  - Chaves do KMS multirregionais podem ser chaves de criptografia do KMS simétricas, chaves do KMS assimétricas, chaves do KMS de HMAC e chaves do KMS com material de chave importado.
  - Não é possível criar chaves de várias Regiões em um armazenamento de chaves personalizado.
- Material de chave importado
  - É possível importar material de chave importado para chave do KMS simétricas, chaves do KMS assimétricas e chaves do KMS de HMAC.
  - É possível chaves de várias regiões com material de chave importado.
  - Você não pode criar chaves do KMS com material de chave em um armazenamento de chaves personalizado.
  - A alternância automática de chaves (`EnableKeyRotation`, `DisableKeyRotation`) não é compatível com chaves do KMS com material de chave importado.
- Armazenamentos de chaves personalizados
  - Armazenamentos personalizados de chaves são compatíveis apenas com chaves do KMS de criptografia simétrica.
  - Operações simétricas em pares de chaves assimétricas (`GenerateDataKeyPair`, `GenerateDataKeyPairWithoutPlaintext`) não são compatíveis com chaves do KMS em armazenamentos de chaves personalizados.
  - A alternância automática de chaves (`EnableKeyRotation`, `DisableKeyRotation`) não é compatível com chaves do KMS em armazenamentos personalizados de chaves.
  - Não é possível criar chaves de várias regiões em armazenamentos personalizados de chaves.

Talvez seja necessário rolar horizontalmente ou verticalmente para ver todos os dados nessa tabela.

AWS KMS Operação de API	Chaves de várias regiões	Material de chave importado	Chaves do KMS em um armazenamento de chaves personalizado
CancelKeyDeletion	✓	✓	✓

AWS KMS Operação de API	Chaves de várias regiões	Material de chave importado	Chaves do KMS em um armazenamento de chaves personalizado
CreateAlias	✓	✓	✓
CreateGrant	✓	✓	✓
CreateKey Você pode usar `CreateKey` para criar uma chave primária multirregional, chaves do KMS com material de chave importado ou uma chave do KMS em um armazenamento de chaves personalizado. Para criar uma chave de réplica multirregional, use `ReplicateKey` .	✓	✓	✓
Decrypt	✓ Válido somente quando `KeyUsage` é `ENCRYPT_DECRYPT`	✓	✓
DeleteAlias	✓	✓	✓

AWS KMS Operação de API	Chaves de várias regiões	Material de chave importado	Chaves do KMS em um armazenamento de chaves personalizado
DeleteImportedKeyMaterial	✓ É válido somente para chaves do KMS com material de chave importado (`Origin` é `EXTERNAL`)	✓	⊗
DescribeKey	✓	✓	✓
DisableKey	✓	✓	✓
DisableKeyRotation	✓ Válido somente em chaves de criptografia simétricas com material de chave do AWS KMS (`Origin` é `AWS_KMS`).	⊗	⊗

AWS KMS Operação de API	Chaves de várias regiões	Material de chave importado	Chaves do KMS em um armazenamento de chaves personalizado
EnableKey	✓ Válido somente em chaves do KMS de criptografia simétricas	✓	✓
EnableKeyRotation	✓ Válido somente em chaves de criptografia simétricas com material de chave do AWS KMS (`Origin` é `AWS_KMS`).	⊗	⊗
Encrypt	✓ Válido somente quando `KeyUsage` é `ENCRYPT_DECRYPT`	✓	✓

AWS KMS Operação de API	Chaves de várias regiões	Material de chave importado	Chaves do KMS em um armazenamento de chaves personalizado
GenerateDataKey	✓ Válido somente em chaves do KMS de criptografia simétricas	✓	✓
GenerateDataKeyPair	✓ Válido somente em chaves do KMS de criptografia simétricas	✓	⊗
GenerateDataKeyPairWithoutPlaintext	✓ Válido somente em chaves do KMS de criptografia simétricas	✓	⊗

AWS KMS Operação de API	Chaves de várias regiões	Material de chave importado	Chaves do KMS em um armazenamento de chaves personalizado
GenerateDataKeyWithoutPlaintext	✓ Válido somente em chaves do KMS de criptografia simétricas	✓	✓
GenerateMac Válido somente em chaves do KMS de HMAC	✓	✓	⊗
GetKeyPolicy	✓	✓	✓
GetKeyRotationStatus	✓	✓ (`KeyRotationEnabled` sempre será `false`.)	⊗

AWS KMS Operação de API	Chaves de várias regiões	Material de chave importado	Chaves do KMS em um armazenamento de chaves personalizado
GetParametersForImport	✓ É válido somente para chaves do KMS com material de chave importado (`Origin` é `EXTERNAL`).	✓	⊗
GetPublicKey Válido somente para chaves do KMS assimétricas.	✓	✓	⊗
ImportKeyMaterial	✓ É válido somente para chaves do KMS com material de chave importado (`Origin` é `EXTERNAL`).	✓	⊗
ListAliases	✓	✓	✓
ListGrants	✓	✓	✓
ListKeyPolicies	✓	✓	✓

AWS KMS Operação de API	Chaves de várias regiões	Material de chave importado	Chaves do KMS em um armazenamento de chaves personalizado
ListResourceTags	✓	✓	✓
ListRetirableGrants	✓	✓	✓
PutKeyPolicy	✓	✓	✓
ReEncrypt	✓ Válido somente quando `KeyUsage` é `ENCRYPT_DECRYPT`	✓	✓
ReplicateKey	✓ Válido somente em chaves primárias multirregionais.	✓ Válido somente em chaves primárias multirregionais.	⊗
RetireGrant	✓	✓	✓
RevokeGrant	✓	✓	✓
ScheduleKeyDeletion	✓	✓	✓

AWS KMS Operação de API	Chaves de várias regiões	Material de chave importado	Chaves do KMS em um armazenamento de chaves personalizado
Sign Válido apenas quando `KeyUsage` é `SIGN_VERIFY` .	✓	✓	⊗
TagResource	✓	✓	✓
UntagResource	✓	✓	✓
UpdateAlias - A chave do KMS atual e a nova chave do KMS devem ser do mesmo tipo (ambas simétricas, assimétricas ou HMAC) e devem ter o mesmo uso de chave.	✓	✓	✓
UpdateKeyDescription	✓	✓	✓
UpdateReplicaRegion	✓	✓ Válido somente em chaves multirregionais.	⊗
Verificar Válido somente quando `KeyUsage` é `SIGN_VERIFY` .	✓	✓	⊗

AWS KMS Operação de API	Chaves de várias regiões	Material de chave importado	Chaves do KMS em um armazenamento de chaves personalizado
VerifyMac Válido somente em chaves do KMS de HMAC			

Segurança do AWS Key Management Service

A segurança da nuvem na AWS é a nossa maior prioridade. Como cliente da AWS, você se beneficiará de um datacenter e de uma arquitetura de rede criados para atender aos requisitos das empresas com as maiores exigências de segurança.

A segurança é uma responsabilidade compartilhada entre a AWS e você. O modelo de responsabilidade compartilhada descreve isso como a segurança da nuvem e a segurança na nuvem:

- Segurança da nuvem – A AWS é responsável pela proteção da infraestrutura que executa serviços da AWS na nuvem da AWS. A AWS também fornece serviços que você pode usar com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos Programas de conformidade da AWS. Para saber mais sobre os programas de conformidade aplicáveis ao AWS Key Management Service (AWS KMS), consulte Serviços da AWS no escopo por programa de conformidade.
- Segurança na nuvem – Sua responsabilidade é determinada pelo serviço da AWS que você usa. No AWS KMS, além da configuração e do uso de AWS KMS keys, você é responsável por outros fatores, incluindo a confidencialidade dos dados, os requisitos da sua empresa e as leis e os regulamentos aplicáveis

Esta documentação ajuda a entender como aplicar o modelo de responsabilidade compartilhada ao usar o AWS Key Management Service. Ela mostra como configurar o AWS KMS para atender aos objetivos de segurança e conformidade.

Tópicos

- Proteção de dados no AWS Key Management Service
- Gerenciamento de identidade e acesso para o AWS Key Management Service
- Registrar em log e monitorar no AWS Key Management Service
- Validação de conformidade do AWS Key Management Service
- Resiliência no AWS Key Management Service
- Segurança da infraestrutura no AWS Key Management Service
- Melhores práticas de segurança do AWS Key Management Service

Proteção de dados no AWS Key Management Service

AWS Key Management ServiceO armazena e protege suas chaves de criptografia para torná-las altamente disponíveis e, ao mesmo tempo, oferece controle de acesso forte e flexível.

Tópicos

- Proteger material de chave
- Criptografia de dados
- Privacidade do tráfego entre redes

Proteger material de chave

Por padrão, o AWS KMS gera e protege o material da chave criptográfica para chaves do KMS. Além disso, o AWS KMS oferece opções para materiais de chave criados e protegidos fora do AWS KMS. Para obter detalhes sobre o gerenciamento de chaves do KMS e do material de chave, consulte Detalhes criptográficos do AWS Key Management Service

Proteger o material essencial gerado em AWS KMS

Quando você cria uma chave do KMS, por padrão, o AWS KMS gera o material de chave para essa chave do KMS.

Para proteger o material de chave para chaves do KMS, o AWS KMS conta com uma frota distribuída de módulos de segurança de hardware (HSMs) validados para FIPS 140-2 Nível de segurança 3 - validado. Cada HSM do AWS KMS é um dispositivo de hardware independente projetado para fornecer funções criptográficas dedicadas a fim de atender aos requisitos de segurança e escalabilidade do AWS KMS. (Os HSMs usados pelo AWS KMS nas regiões China (Pequim) e China (Ningxia) são certificados pelaOSCCA e estão em conformidade com todos os regulamentos chineses pertinentes, mas não são validados pelo Programa de validação de módulos criptográficos FIPS 140-2.)

O material de chave de uma chave do KMS é criptografado por padrão quando é gerado no HSM. O material da chave é descriptografado somente na memória volátil do HSM e somente por alguns milissegundos necessários para ser usado em uma operação criptográfica. Sempre que o material da chave não está em uso ativo, ele é criptografado no HSM e transferido para um armazenamento persistente altamente durável (99,999999999%) e de baixa latência, onde permanece separado e isolado dos HSMs. O material de chave em texto nunca deixa o limite de segurança de HSM; ele

nunca é gravado em disco ou em qualquer mídia de armazenamento persistente. (A única exceção é a chave pública de um par de chaves assimétricas, que não é secreta.)

A AWS afirma como princípio fundamental de segurança que não há interação humana com material de chave criptográfica de texto simples de qualquer tipo em nenhum AWS service (Serviço da AWS). Não há mecanismo para que ninguém, incluindo os operadores de AWS service (Serviço da AWS), visualize, acesse ou exporte material de chave em texto simples. Esse princípio se aplica mesmo durante falhas catastróficas e eventos de recuperação de desastres. O material de chave do cliente em texto simples do AWS KMS é usado para operações criptográficas em HSMs validados pelo FIPS do AWS KMS somente em resposta às solicitações autorizadas feitas ao serviço pelo cliente ou seu representante.

Para chaves gerenciadas pelo cliente, a Conta da AWS que cria a chave é a proprietária única e intransferível da chave. A conta proprietária tem controle total e exclusivo sobre as políticas de autorização que controlam o acesso à chave. Para Chaves gerenciadas pela AWS, a Conta da AWS tem controle total sobre as políticas do IAM que autorizam solicitações para o AWS service (Serviço da AWS).

Proteger o material de chave gerado no AWS KMS

O AWS KMS fornece alternativas aos principais materiais gerados em AWS KMS.

Repositórios de chaves personalizados, um recurso opcional do AWS KMS, permitem criar chaves do KMS apoiadas por material de chave gerado e usado fora do AWS KMS. As chaves do KMS nos repositórios de chaves do AWS CloudHSM são apoiadas por chaves nos módulos de segurança de hardware do AWS CloudHSM que você controla. Esses HSMs têm certificação FIPS 140-2 Nível de segurança 3. As chaves do KMS em repositórios de chaves externos são apoiadas por chaves em um gerenciador de chaves externo que você controla e gerencia fora da AWS, como um HSM físico em seu datacenter privado.

Outro recurso opcional permite importar o material de chave para uma chave do KMS. Para proteger o material de chaves importado enquanto ele está em trânsito para o AWS KMS, você criptografa o material de chaves usando uma chave pública de um par de chaves RSA gerado em um HSM do AWS KMS. O material de chave importada é descriptografado em um HSM do AWS KMS e criptografado novamente sob chaves simétricas no HSM. Como todo material de chave do AWS KMS, material de chave importado em texto não criptografado nunca sai dos seus HSMs sem estarem criptografados. No entanto, o cliente que forneceu o material de chave é responsável pelo uso seguro, a durabilidade e a manutenção do material de chave fora do AWS KMS.

Criptografia de dados

Os dados no AWS KMS consistem em AWS KMS keys e no material de chave de criptografia que eles representam. Esse material de chave existe em texto simples somente dentro de módulos de segurança de hardware (HSMs) do AWS KMS e somente quando em uso. Caso contrário, o material de chave é criptografado e armazenado em armazenamento persistente durável.

O material de chave gerado pelo AWS KMS para chaves do KMS nunca deixam os limites dos HSMs do AWS KMS em estado não criptografado. Ele não é exportado nem transmitido em nenhuma operação de API do AWS KMS. A exceção é para chaves de várias regiões, em que o AWS KMS usa um mecanismo de replicação entre regiões para copiar o material de chaves para uma chave de várias regiões de um HSM em uma Região da AWS para um HSM em uma Região da AWS. Para obter mais detalhes, consulte Processo de replicação para chaves em multirregiões em Detalhes criptográficos AWS Key Management Service.

Tópicos

- Criptografia inativa
- Criptografia em trânsito

Criptografia inativa

O AWS KMS gera material de chave para AWS KMS keys em FIPS 140-2 Nível de segurança 3 - compatíveis com módulos de segurança de hardware (HSMs). A única exceção são as regiões da China, nas quais os HSMs usados pelo AWS KMS para gerar chaves do KMS estão em conformidade com todos os regulamentos chineses pertinentes, mas não são validados pelo Programa de validação de módulos criptográficos FIPS 140-2. Quando não estiver em uso, o material de chave é criptografado por uma chave do HSM e gravado em um armazenamento durável e persistente. O material de chave para chaves do KMS e as chaves de criptografia que protegem o material de chave nunca deixam os HSMs em formato de texto simples.

A criptografia e o gerenciamento de material de chave para chaves do KMS são tratados inteiramente pelo AWS KMS.

Para obter mais detalhes, consulte .Trabalhar comAWS KMS keys, em Detalhes criptográficos do AWS Key Management Service.

Criptografia em trânsito

O material de chave gerado pelo AWS KMS para chaves do KMS nunca é exportado nem transmitido em operações de API do AWS KMS. O AWS KMS usa identificadores de chave para representar as chaves do KMS em operações de API. Da mesma forma, o material de chave para chaves do KMS em armazenamentos de chaves personalizados do AWS KMS não é exportável e nunca é transmitido em operações de API do AWS KMS ou do AWS CloudHSM.

No entanto, algumas operações de API do AWS KMS retornam chaves de dados. Além disso, os clientes podem usar operações de API para importar material de chave para chaves do KMS selecionadas.

Todas as chamadas de API do AWS KMS devem ser assinadas e transmitidas usando Transport Layer Security (TLS). O AWS KMS requer o TLS 1.2 e recomenda o TLS 1.3 em todas as regiões. O AWS KMS também oferece suporte a TLS híbrido pós-quântico para terminais do serviço AWS KMS em todas as regiões, exceto nas regiões da China. O AWS KMS não é compatível com o TLS pós-quântico híbrido para endpoints FIPS em AWS GovCloud (US). Chamadas para o AWS KMS também exigem um pacote de codificação moderno que seja compatível com sigilo de encaminhamento perfeito, o que significa que o comprometimento de qualquer segredo, como uma chave privada, não compromete também a chave de sessão.

Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar a AWS por meio de uma interface de linha de comando ou uma API, use um endpoint do FIPS. Para usar os endpoints padrão do AWS KMS ou endpoins do FIPS do AWS KMS, os clientes devem ser compatíveis com TLS 1.2 ou posterior. Para ter mais informações sobre endpoints do FIPS, consulte Federal Information Processing Standard (FIPS) 140-2. Para obter uma lista de endpoints FIPS do AWS KMS, consulte Endpoints e cotas do AWS Key Management Service no Referência geral da AWS.

As comunicações entre hosts de serviço do AWS KMS e HSMs são protegidas usando ECC (Elliptic Curve Cryptography) e Advanced Encryption Standard (AES) em um esquema de criptografia autenticado. Para obter mais detalhes, consulte Segurança da comunicação interna, em Detalhes criptográficos do AWS Key Management Service.

Privacidade do tráfego entre redes

O AWS KMS é compatível com um AWS Management Console e um conjunto de operações de API que permitem criar e gerenciar AWS KMS keys e usá-las em operações de criptografia.

O AWS KMS é compatível com duas opções de conectividade de rede da sua rede privada para a AWS.

- Uma conexão VPN IPSec pela Internet
- AWS Direct Connect, que vincula sua rede interna a um local do AWS Direct Connect usando um cabo de fibra óptica Ethernet padrão.

Todas as chamadas de API do AWS KMS devem ser assinadas e transmitidas usando Transport Layer Security (TLS). As chamadas também exigem um conjunto de codificação moderno que seja compatível com o sigilo de encaminhamento perfeito. O tráfego para os módulos de segurança de hardware (HSMs) que armazenam material de chave para chaves do KMS é permitido somente de hosts de API do AWS KMS pela rede interna da AWS.

Para se conectar diretamente ao AWS KMS partir de sua Virtual Private Cloud (VPC) sem enviar tráfego pela Internet pública, use endpoint da VPCs, alimentados por AWS PrivateLink. Para obter mais informações, consulte Conectar-se ao AWS KMS por meio de um endpoint da VPC.

O AWS KMS também é compatível com uma opção de troca de chaves pós-quântica híbrida para o protocolo de criptografia de rede Transport Layer Security (TLS). É possível usar essa opção com o TLS ao conectar-se aos endpoints de API do AWS KMS.

Gerenciamento de identidade e acesso para o AWS Key Management Service

O AWS Identity and Access Management (IAM) ajuda você a controlar com segurança o acesso aos recursos da AWS. Os administradores controlam quem pode ser autenticado (conectado) e autorizado (ter permissões) a usar os recursos do AWS KMS. Para ter mais informações, consulte Usando políticas do IAM com AWS KMS.

Políticas de chaves são o mecanismo principal para controlar o acesso a chaves do KMS no AWS KMS. Cada chave do KMS deve ter uma política de chaves. Você também pode usar políticas do IAM e concessões, juntamente com políticas de chaves, para controlar o acesso às suas chaves do KMS. Para ter mais informações, consulte Autenticação e controle de acesso para o AWS KMS.

Se estiver usando uma Amazon Virtual Private Cloud (Amazon VPC), você poderá criar um endpoint da VPC de interface com o AWS KMS desenvolvido pela AWS PrivateLink. Também é possível usar políticas de endpoint da VPC para determinar quais entidades principais podem acessar o endpoint

do AWS KMS, quais chamadas de API elas podem fazer e qual chave do KMS elas podem acessar. Para obter mais detalhes, consulte Controlar o acesso a um endpoint da VPC.

Registrar em log e monitorar no AWS Key Management Service

O monitoramento é uma parte importante para entender a disponibilidade, o estado e o uso das suas AWS KMS keys no AWS KMS. O monitoramento ajuda a manter a segurança, a confiabilidade, a disponibilidade e a performance das suas soluções da AWS. A AWS fornece várias ferramentas para o monitoramento das suas chaves do KMS.

Logs do AWS CloudTrail

Toda chamada para uma operação de API do AWS KMS é capturada como um evento em um log do AWS CloudTrail. Esses logs registram todas as chamadas de API do console do AWS KMS e as chamadas feitas pelo AWS KMS e outros serviços da AWS. As chamadas de API entre contas, como uma chamada para usar uma chave KMS em outraConta da AWS, são registradas nos CloudTrail registros de ambas as contas.

Ao solucionar problemas ou fazer auditorias, você pode usar o log para reconstruir o ciclo de vida de uma chave do KMS. Também é possível visualizar seu gerenciamento e uso da chave do KMS em operações de criptografia. Para ter mais informações, consulte the section called “Fazendo login com AWS CloudTrail”.

CloudWatch Registros da Amazon

Monitore, armazene e acesse seus arquivos de log do AWS CloudTrail ou de outras origens. Para obter mais informações, consulte o Guia CloudWatch do usuário da Amazon.

ForAWS KMS, CloudWatch armazena informações úteis que ajudam você a evitar problemas com suas chaves KMS e os recursos que elas protegem. Para ter mais informações, consulte the section called “Monitoramento com CloudWatch”.

Amazon EventBridge

AWS KMSgera EventBridge eventos quando sua chave KMS é girada ou excluída ou o material da chave importada em sua chave KMS expira. Pesquise eventos do AWS KMS (operações de API) e encaminhe-os para uma ou mais funções ou streams de destino para capturar informações de estado. Para obter mais informações, consulte the section called “Monitoramento com a Amazon EventBridge” o Guia do EventBridge usuário da Amazon.

CloudWatch Métricas da Amazon

Você pode monitorar suas chaves KMS usando CloudWatch métricas, que coletam e processam dados brutos AWS KMS em métricas de desempenho. Os dados são registrados em intervalos de duas semanas para que você possa visualizar tendências de informações atuais e históricas. Isso ajuda você a entender como as suas chaves do KMS são usadas e como seu uso muda ao longo do tempo. Para obter informações sobre o uso de CloudWatch métricas para monitorar chaves KMS, consulteAWS KMS métricas e dimensões.

CloudWatch Alarmes da Amazon

Observe uma única métrica mudar ao longo de um período que você especificar. Depois, execute uma ou mais ações com base no valor da métrica relativa a um limite por um número de períodos. Por exemplo, você pode criar um CloudWatch alarme que é acionado quando alguém tenta usar uma chave KMS programada para ser excluída em uma operação criptográfica. Isso indica que a chave do KMS ainda está sendo usada e provavelmente não deve ser excluída. Para ter mais informações, consulte the section called “Criar um alarme”.

AWS Security Hub

É possível monitorar o uso do AWS KMS conforme os padrões do setor de segurança e a conformidade com as melhores práticas usando o AWS Security Hub. O Security Hub usa controles de segurança para avaliar configurações de recursos e padrões de segurança que ajudam você a cumprir vários frameworks de conformidade. Para obter mais informações, consulte Controles do AWS Key Management Service no Manual do usuário do AWS Security Hub.

Validação de conformidade do AWS Key Management Service

Auditores de terceiros avaliam a segurança e a conformidade do AWS Key Management Service como parte de vários programas de conformidade da AWS. Isso inclui SOC, PCI, FedRAMP, HIPAA e outros.

Tópicos

- Documentos de conformidade e segurança
- Saiba mais

Documentos de conformidade e segurança

Os seguintes documentos de conformidade e segurança abrangem o AWS KMS. Para visualizá-los, use AWS Artifact.

- Cloud Computing Compliance Controls Catalogue (C5)
- ISO 27001:2013 Statement of Applicability (SoA)
- Certificado ISO 27001:2013
- ISO 27017:2015 Statement of Applicability (SoA)
- Certificado ISO 27017:2015
- ISO 27018:2015 Statement of Applicability (SoA)
- Certificado ISO 27018:2014
- Certificado ISO 9001:2015
- Certificado de Conformidade do PCI DSS (AOC) e Resumo de Responsabilidade
- Relatório Service Organization Controls (SOC) 1
- Relatório Service Organization Controls (SOC) 2
- Relatório de Confidencialidade Service Organization Controls (SOC) 2
- FedRAMP-High

Para obter ajuda sobre o uso do AWS Artifact, consulte Baixar relatórios no AWS Artifact.

Saiba mais

Sua responsabilidade de conformidade ao usar o AWS KMS é determinada pela confidencialidade dos seus dados, pelos objetivos de conformidade da sua empresa e pelos regulamentos e leis aplicáveis. Se o uso do AWS KMS estiver sujeito à conformidade com um padrão publicado, a AWS fornecerá recursos para ajudar:

- Serviços da AWS em escopo por programa de conformidade – Esta página lista os serviços da AWS no escopo de programas de conformidade específicos. Para obter informações gerais, consulte Programas de conformidade da AWS.
- Guias de início rápido de segurança e conformidade – Esses guias de implantação discutem considerações sobre arquitetura e fornecem medidas para implantar ambientes de linha de base focados em segurança e conformidade na AWS.

- Recursos de compatibilidade da AWS – Esta coleção de guias e pastas de trabalho pode ser aplicada ao seu setor e local.
- AWS Config: esse serviço da AWS avalia até que ponto suas configurações de recursos atendem adequadamente às práticas internas e às diretrizes e regulamentações do setor.
- AWS Security Hub - Este serviço da AWS fornece uma visão abrangente do seu estado de segurança na AWS. O Security Hub usa controles de segurança para avaliar os atributos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.

Resiliência no AWS Key Management Service

A infraestrutura global da AWS se baseia em Regiões da AWS e zonas de disponibilidade. A Regiões da AWS oferece várias zonas de disponibilidade separadas e isoladas fisicamente que são conectadas com baixa latência, altas taxas de throughput e em redes altamente redundantes. Com as Zonas de Disponibilidade, você pode projetar e operar aplicativos e bancos de dados que executam o failover automaticamente entre as Zonas de Disponibilidade sem interrupção. As Zonas de Disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de datacenter tradicionais.

Além da infraestrutura global da AWS, o AWS KMS oferece vários atributos para ajudar a oferecer suporte às suas necessidades de resiliência de dados e backup. Para obter mais informações sobre Regiões da AWS e zonas de disponibilidade, consulteAWS Infraestrutura global.

Isolamento regional

O AWS Key Management Service (AWS KMS) é um serviço regional autossustentável que está disponível em todas as Regiões da AWS. O design regionalmente isolado do AWS KMS garante que um problema de disponibilidade em uma Região da AWS não possa afetar a operação do AWS KMS em nenhuma outra região. O AWS KMS foi projetado para garantir zero de tempo de inatividade planejada, com todas as atualizações de software e operações de dimensionamento realizadas de maneira impecável e imperceptível.

O Acordo de Serviço (SLA) do AWS KMS inclui um compromisso de serviço de 99,999% para todas as APIs do KMS. Para cumprir esse compromisso, o AWS KMS garante que todos os dados e informações de autorização necessários para executar uma solicitação de API estejam disponíveis em todos os hosts regionais que recebem a solicitação.

A infraestrutura do AWS KMS é replicada em pelo menos três zonas de disponibilidade (AZ) em cada região. Para garantir que várias falhas de host não afetem a performance do AWS KMS, o AWS KMS foi projetado para atender ao tráfego de clientes de qualquer uma das AZs em uma região.

As alterações feitas nas propriedades ou permissões de uma chave do KMS são replicadas para todos os hosts na região a fim de garantir que a solicitação subsequente possa ser processada corretamente por qualquer host na região. Solicitações de operações criptográficas usando sua chave do KMS são encaminhadas para uma frota de hardware security modules (HSM – Módulo de segurança de hardware) do AWS KMS, e qualquer um deles pode executar a operação com a chave do KMS.

Design de vários locatários

O design de vários locatários do AWS KMS permite que o serviço cumpra o SLA de 99,999% de disponibilidade e mantenha altas taxas de solicitação enquanto protege a confidencialidade de suas chaves e dados.

Há vários mecanismos de imposição de integridade implantados para garantir que a chave do KMS especificada para a operação criptográfica sempre seja a chave usada.

O material da chave em texto não criptografado para suas chaves do KMS é extensivamente protegido. Assim que é criado, o material da chave é criptografado no HSM e o material de chave criptografado é imediatamente movido para armazenamento seguro e de baixa latência. A chave criptografada é recuperada e descriptografada no HSM no momento do uso. A chave em texto não criptografado permanece na memória do HSM apenas pelo tempo necessário para a conclusão da operação criptográfica. Em seguida, ela é criptografada novamente no HSM e a chave criptografada é devolvida para o armazenamento. O material de chave em texto não criptografado nunca deixa os HSMs e nunca é gravado no armazenamento persistente.

Para obter mais informações sobre os mecanismos que o AWS KMS usa para proteger suas chaves, consulte Detalhes criptográficos do AWS Key Management Service.

Práticas recomendadas de resiliência no AWS KMS

Considere o uso das seguintes estratégias para otimizar a resiliência de seus recursos do AWS KMS.

- Para apoiar sua estratégia de backup e recuperação de desastres, considere o uso de chaves de várias regiões, que são chaves do KMS criadas em uma Região da AWS e replicadas somente para regiões que você especifica. Com chaves de várias regiões, você pode mover recursos

criptografados entre Regiões da AWS (dentro da mesma partição) sem nunca expor o texto não criptografado, e, quando necessário, descriptografar o recurso em qualquer uma de suas regiões de destino. As chaves de várias regiões relacionadas são interoperáveis porque compartilham o mesmo material de chave e ID de chave, mas têm políticas independentes de chave para controle de acesso em alta resolução. Para obter detalhes, consulte Chaves de várias regiões em AWS KMS.

- Para proteger suas chaves em um serviço de vários locatários como o AWS KMS, certifique-se de usar controles de acesso, incluindo políticas de chaves e políticas do IAM. Além disso, você pode enviar suas solicitações para o AWS KMS usando um endpoint de interface de VPC habilitado pelo AWS PrivateLink. Se você fizer isso, toda a comunicação entre seu Amazon VPC e o AWS KMS será realizada inteiramente na rede da AWS usando um endpoint dedicado do AWS KMS restrito à sua VPC. É possível proteger adicionalmente essas solicitações criando uma camada adicional de autorização usando políticas de endpoint da VPC. Para obter mais detalhes, consulte Conectar-se ao AWS KMS por meio de um endpoint da VPC.

Segurança da infraestrutura no AWS Key Management Service

Como serviço gerenciado, o AWS Key Management Service (AWS KMS) é protegido pelos procedimentos de segurança de rede global da AWS que estão descritos no whitepaper Amazon Web Services: visão geral dos processos de segurança.

Para acessar o AWS KMS pela rede, é possível chamar as operações de API do AWS KMS descritas na Referência de APIS AWS Key Management Service. O AWS KMS requer o TLS 1.2 e recomenda o TLS 1.3 em todas as regiões. O AWS KMS também é compatível com TLS híbrido pós-quântico para terminais de serviço do AWS KMS em todas as regiões, exceto nas regiões da China. O AWS KMS não é compatível com TLS híbrido pós-quântico para endpoints FIPS em AWS GovCloud (US). Para usar os endpoints padrão do AWS KMS ou endpoins do FIPS do AWS KMS, os clientes devem ser compatíveis com TLS 1.2 ou posterior. Os clientes também devem ter suporte a conjuntos de criptografia com perfect forward secrecy (PFS) como Ephemeral Diffie-Hellman (DHE) ou Ephemeral Elliptic Curve Diffie-Hellman (ECDHE). A maioria dos sistemas modernos, como o Java 7 e versões posteriores, oferece suporte a esses modos.

Além disso, as solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou você pode usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Você pode chamar essas operações de API de qualquer local da rede, mas o AWS KMS é compatível com condições de política globais que permitem controlar o acesso a uma chave do KMS com base no endereço IP de origem, na VPC e no endpoint da VPC. É possível usar essas chaves de condição em políticas de chaves e em políticas do IAM. No entanto, essas condições podem impedir que a AWS use a chave do KMS em seu nome. Para obter mais detalhes, consulte AWS chaves de condição globais.

Por exemplo, a seguinte instrução de política de chaves permite que os usuários que podem assumir a função `KMSTestRole` utilizem essa AWS KMS keypara operações de criptografia especificadas, a não ser que o endereço IP de origem seja um dos endereços IP especificados na política.

```
{
  "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 de hosts físicos

A segurança da infraestrutura física usada pelo AWS KMS está sujeita aos controles descritos na seção Segurança física e ambiental do whitepaper Amazon Web Services: Visão geral dos

processos de segurança. É possível encontrar mais detalhes em relatórios de conformidade e em descobertas de auditoria de terceiros listados na seção anterior.

AWS KMSO é compatível com módulos de segurança de hardware (HSMs) dedicados projetados com controles específicos para resistir a ataques físicos. Os HSMs são dispositivos físicos que não têm uma camada de virtualização, como um hipervisor, que compartilha o dispositivo físico entre vários locatários lógicos. O material de chave para AWS KMS keys é armazenado somente na memória volátil nos HSMs e apenas enquanto a chave do KMS está em uso. Essa memória é apagada quando o HSM sai do estado operacional, incluindo desligamentos e definições intencionais e não intencionais. Para obter informações detalhadas sobre a operação de HSMs do AWS KMS, consulte Detalhes criptográficos do AWS Key Management Service.

Melhores práticas de segurança do AWS Key Management Service

O AWS Key Management Service (AWS KMS) oferece suporte a vários recursos de segurança que podem ser implementados para melhorar a proteção de suas chaves de criptografia, incluindo políticas de chaves e políticas do IAM, uma opção de contexto de criptografia para operações criptográficas em chaves de criptografia simétricas, um extenso conjunto de chaves de condição para refinar suas políticas de chave e de políticas do IAM, e restrições de concessão para limitar concessões.

Esses recursos de segurança são descritos em detalhes nas Práticas recomendadas do AWS Key Management Service (PDF). As diretrizes gerais neste artigo técnico não representam uma solução de segurança completa. Como nem todas as melhores práticas são apropriadas para todas as situações, elas não se destinam a ser prescritivas.

Consulte também

- Práticas recomendadas para políticas do IAM
- Práticas recomendadas para concessões do AWS KMS
- Práticas recomendadas de segurança no IAM, noManual do usuário do IAM

Cotas

Para tornar AWS KMS responsivo e eficiente para todos os usuários, AWS KMS aplique dois tipos de cotas: cotas de recursos e cotas de solicitação. Cada cota é calculada independentemente para cada Região de cada Conta da AWS.

Todas as AWS KMS cotas são ajustáveis, exceto a cota de recursos do tamanho do documento de política principal, a cota de recursos de rotação sob demanda e a cota de solicitação do armazenamento de AWS CloudHSM chaves. Para solicitar um aumento da cota, consulte Requesting a quota increase no Guia do usuário do Service Quotas. Para solicitar uma redução de cota, alterar uma cota que não está listada nas Cotas de Serviço ou alterar uma cota em uma área em que as Cotas de Região da AWS Serviço não estejam disponíveis, visite AWS Support o Centro e crie um caso. AWS KMS

Tópicos

- Cotas de recurso
- Cotas de solicitações
- Solicitações de AWS KMS limitação

Cotas de recurso

AWS KMS estabelece cotas de recursos para garantir que possa fornecer um serviço rápido e resiliente a todos os nossos clientes. Algumas cotas de recursos se aplicam somente aos recursos que você cria, mas não aos recursos que os AWS serviços criam para você. Os recursos que você usa, mas que não estão na sua Conta da AWS, como o Chaves pertencentes à AWS, não contam em relação a essas cotas.

Se você exceder um limite de recurso, as solicitações para criar um recurso adicional desse tipo geram uma mensagem de erro `LimitExceededException`.

Todas as cotas de AWS KMS recursos são ajustáveis, exceto a cota de tamanho do documento de política principal e a cota de recursos de rotação sob demanda. Para solicitar um aumento da cota, consulte Requesting a quota increase no Guia do usuário do Service Quotas. Para solicitar uma redução de cota, alterar uma cota que não está listada nas Cotas de Serviço ou alterar uma cota em uma área em que as Cotas de Região da AWS Serviço não estejam disponíveis, visite AWS Support o Centro e crie um caso. AWS KMS

A tabela a seguir lista e descreve as cotas de AWS KMS recursos em cada Conta da AWS região.

Nome da cota	Valor padrão	Aplica-se a	Ajustável
AWS KMS keys	100.000	Chaves gerenciadas pelo cliente	Sim
Aliases por chave do KMS	50	Aliases criados pelo cliente	Sim
Concessões por chave do KMS	50.000	Chaves gerenciadas pelo cliente	Sim
Tamanho do documento da política de chaves	32 KB (32.768 bytes)	Chaves gerenciadas pelo cliente Chaves gerenciadas pela AWS	Não
Cota de recurso de armazenamento de chaves personalizadas	10	Conta da AWS e região	Sim

Além das cotas de recursos, AWS KMS usa cotas de solicitação para garantir a capacidade de resposta do serviço. Para obter detalhes, consulte the section called “Cotas de solicitações”.

AWS KMS keys: 100,000

Você pode ter até 100.000 chaves gerenciadas pelo cliente em cada região da sua Conta da AWS. Esta cota é aplicável a todas as chaves gerenciadas pelo cliente em todas as Regiões da AWS , independentemente da especificação da chave ou do estado da chave. Cada chave do KMS é considerada um recurso. Chaves gerenciadas pela AWS e Chaves pertencentes à AWS não contam para essa cota.

Aliases por chave do KMS: 50

É possível associar até 50 aliases a cada chave gerenciada pelo cliente. Os aliases AWS associados a Chaves gerenciadas pela AWSnão contam para essa cota. É possível encontrar essa cota ao criar ou atualizar um alias.

> **Note**
>
> A ResourceAliases condição kms: é efetiva somente quando a chave KMS está em conformidade com essa cota. Se uma chave do KMS exceder essa cota, as entidades principais autorizadas a usar essa chave pela condição `kms:ResourceAliases` terão acesso negado a ela. Para obter detalhes, consulte Acesso negado devido à cota de aliases.

A cota de aliases por chave KMS substitui a cota de aliases por região, que limitava o número total de aliases em cada região de um. Conta da AWS AWS KMS eliminou a cota de aliases por região.

Concessões por chave do KMS: 50.000

Cada chave gerenciada pelo cliente pode ter até 50.000 concessões, incluindo as concessões criadas pelos serviços da AWS integrados ao AWS KMS. Essa cota não se aplica a Chaves gerenciadas pela AWS ou a Chaves pertencentes à AWS.

Um efeito dessa cota é que não é possível executar mais de 50.000 operações autorizadas por concessão que usam a mesma chave do KMS ao mesmo tempo. Depois de atingir a cota, será possível criar concessões na chave do KMS apenas quando uma concessão ativa for retirada ou revogada.

Por exemplo, quando você anexa um volume do Amazon Elastic Block Store (Amazon EBS) a uma instância do Amazon Elastic Compute Cloud (Amazon EC2), o volume é descriptografado para poder ser lido. Para obter permissão para descriptografar os dados, o Amazon EBS cria uma concessão para cada volume. Portanto, se todos os volumes do Amazon EBS usarem a mesma chave do KMS, não será possível anexar mais de 50.000 volumes de uma vez.

Tamanho do documento da política de chaves: 32 KB

O tamanho máximo de cada documento de política de chaves é 32 KB (32.768 bytes). Se você usar um documento de política maior para criar ou atualizar a política de chaves de uma chave do KMS, a operação falhará.

Esta cota não é ajustável. Você não pode aumentá-lo usando Quotas de Serviço ou criando um caso em. AWS Support Se a política de chave estiver se aproximando do limite, considere o uso de concessões em vez de declarações de política. Concessões são particularmente úteis para permissões temporárias ou extremamente específicas.

Você usa um documento de política de chave sempre que cria ou altera uma política de chave usando a exibição padrão ou a exibição de política na AWS Management Console, ou na PutKeyPolicyoperação. Essa cota se aplica ao documento de política de chaves, mesmo se usar a visualização padrão no console do AWS KMS , no qual você não edita as instruções JSON diretamente.

Cota de recursos de armazenamento de chaves personalizado: 10

Você pode criar até 10 lojas de chaves personalizadas em Conta da AWS cada região. Se você tentar criar mais, a CreateCustomKeyStoreoperação falhará.

Essa cota se aplica ao número total de armazenamentos de chaves personalizados em cada conta e região, inclusive todos os armazenamentos de chaves do AWS CloudHSM e armazenamentos de chaves externas, independentemente do estado da conexão.

Rotação sob demanda: 10

Você pode realizar a rotação de chaves sob demanda no máximo 10 vezes por chave KMS. Se você tentar realizar mais rotações sob demanda, a RotateKeyOnDemandoperação falhará.

Esta cota não é ajustável. Você não pode aumentá-lo usando Quotas de Serviço ou criando um caso em. AWS Support Para evitar atingir a cota de rotação sob demanda, recomendamos usar a rotação automática de chaves sempre que possível.

Cotas de solicitações

AWS KMS estabelece cotas para o número de operações de API solicitadas em cada segundo. As cotas de solicitação diferem de acordo com a operação da API Região da AWS, a e outros fatores, como o tipo de chave KMS. Quando você excede uma cota de solicitação de API, AWS KMS limita a solicitação.

Todas as cotas de AWS KMS solicitação são ajustáveis, exceto a cota de solicitação do armazenamento de AWS CloudHSM chaves. Para solicitar um aumento da cota, consulte

Requesting a quota increase no Guia do usuário do Service Quotas. Para solicitar uma redução de cota, alterar uma cota que não está listada nas Cotas de Serviço ou alterar uma cota em uma área em que as Cotas de Região da AWS Serviço não estejam disponíveis, visite AWS Support o Centro e crie um caso. AWS KMS

Se você estiver excedendo a cota de solicitação para a GenerateDataKeyoperação, considere usar o recurso de armazenamento em cache da chave de dados do. AWS Encryption SDK A reutilização de chaves de dados pode reduzir a frequência de suas solicitações para o. AWS KMS

Além de solicitar cotas, AWS KMS usa cotas de recursos para garantir a capacidade de todos os usuários. Para obter detalhes, consulte Cotas de recurso.

Para visualizar as tendências em suas taxas de solicitação, use o console do Service Quotas. Você também pode criar um CloudWatch alarme da Amazon que o alerta quando sua taxa de solicitação atingir uma determinada porcentagem do valor da cota. Para obter detalhes, consulte Gerenciar suas taxas de solicitação de AWS KMS API usando Service Quotas e Amazon CloudWatch no Blog de AWS Segurança.

Tópicos

- Solicite cotas para cada operação de AWS KMS API
- Aplicar cotas de solicitações
- Cotas compartilhadas para operações de criptografia
- Solicitações de API dofeitas em seu nome
- Solicitações entre contas
- Cotas de solicitação de armazenamento de chaves personalizadas

Solicite cotas para cada operação de AWS KMS API

Esta tabela lista o código da cota de Service Quotas e o valor padrão para cada AWS KMS cota de solicitação. Todas as cotas de AWS KMS solicitação são ajustáveis, exceto a cota de solicitação do armazenamento de AWS CloudHSM chaves.

> **Note**
>
> Talvez seja necessário rolar horizontalmente ou verticalmente para ver todos os dados nessa tabela.

Nome da cota	Valor padrão (solicitações por segundo)

`Cryptographic operations (symmetric) request rate`
 	
Aplica-se a:
 	
• `Decrypt`
• `Encrypt`
• `GenerateDataKey`
• `GenerateDataKeyWithoutPlaintext`
• `GenerateMac`
• `GenerateRandom`
• `ReEncrypt`
• `VerifyMac`
	Essas cotas compartilhadas variam de acordo com o tipo Região da AWS e o tipo de chave KMS usada na solicitação. Cada cota é calculada separadamente.
	
	• 5.500 (compartilhado)
	• 10.000 (compartilhado) nas seguintes regiões:
	  • Leste dos EUA (Ohio), us-east-2
	  • Ásia-Pacífico (Singapura), ap-southeast-1
	  • Ásia-Pacífico (Sydney), ap-southeast-2
	  • Ásia-Pacífico (Tóquio), ap-northeast-1
	  • Europa (Frankfurt), eu-central-1
	  • Europa (Londres), eu-west-2
	• 50.000 (compartilhadas) nas seguintes regiões:
	  • Leste dos EUA (Norte da Virgínia), us-east-1
	  • Oeste dos EUA (Oregon), us-west-2
	  • Europa (Irlanda), eu-west-1

`Cryptographic operations (RSA) request rate` Aplica-se a: • `Decrypt` • `Encrypt` • `ReEncrypt` • `Sign` • `Verify`	500 (compartilhadas) para chaves do KMS RSA

Nome da cota	Valor padrão (solicitações por segundo)
`Cryptographic operations (ECC and SM2) request rate` Aplica-se a: • `Decrypt`— compatível somente com chaves KMS SM2 (somente regiões da China) • `Encrypt`— compatível somente com chaves KMS SM2 (somente regiões da China) • `ReEncrypt` — compatível somente com chaves KMS SM2 (somente regiões da China) • `Sign` • `Verify`	300 (compartilhadas) para chaves KMS de curva elíptica (ECC) e SM2 (somente regiões da China)
`Custom key store request quotas` Aplica-se a: • `Decrypt` • `Encrypt` • `GenerateDataKey` • `GenerateDataKeyWithoutPlaintext` • `GenerateRandom` • `ReEncrypt`	As cotas de solicitação de armazenamento de chaves personalizadas são calculadas separadamente para cada armazenamento de chaves personalizadas. • 1.800 (compartilhados) para cada armazenamento de AWS CloudHSM chaves • 1.800 (compartilhado) para cada armazenamento de chaves externas
`CancelKeyDeletion request rate`	5
`ConnectCustomKeyStore request rate`	5
`CreateAlias request rate`	5
`CreateCustomKeyStore request rate`	5

Nome da cota	Valor padrão (solicitações por segundo)
`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
`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` Aplica-se a: • `GenerateDataKeyPair` • `GenerateDataKeyPairWithoutPlaintext`	100

Nome da cota	Valor padrão (solicitações por segundo)
`GenerateDataKeyPair (ECC_NIST_P384) request rate` Aplica-se a: • `GenerateDataKeyPair` • `GenerateDataKeyPairWithoutPlaintext`	100
`GenerateDataKeyPair (ECC_NIST_P521) request rate` Aplica-se a: • `GenerateDataKeyPair` • `GenerateDataKeyPairWithoutPlaintext`	100
`GenerateDataKeyPair (ECC_SECG_P256K1) request rate` Aplica-se a: • `GenerateDataKeyPair` • `GenerateDataKeyPairWithoutPlaintext`	100
`GenerateDataKeyPair (RSA_2048) request rate` Aplica-se a: • `GenerateDataKeyPair` • `GenerateDataKeyPairWithoutPlaintext`	1

Nome da cota	Valor padrão (solicitações por segundo)
`GenerateDataKeyPair (RSA_3072) request rate` Aplica-se a: • `GenerateDataKeyPair` • `GenerateDataKeyPairWithoutPlaintext`	0,5 (1 em cada intervalo de 2 segundos)
`GenerateDataKeyPair (RSA_4096) request rate` Aplica-se a: • `GenerateDataKeyPair` • `GenerateDataKeyPairWithoutPlaintext`	0,1 (1 em cada intervalo de 10 segundos)
`GenerateDataKeyPair (SM2 – China Regions only) request rate` Aplica-se a: • `GenerateDataKeyPair` • `GenerateDataKeyPairWithoutPlaintext`	25
`GetKeyPolicy request rate`	1000
`GetKeyRotationStatus request rate`	1000
`GetParametersForImport request rate`	0,25 (1 em cada intervalo de 4 segundos)
`GetPublicKey request rate`	2000
`ImportKeyMaterial request rate`	5

Nome da cota	Valor padrão (solicitações por segundo)
`ListAliases request rate`	500
`ListGrants request rate`	100
`ListKeyPolicies request rate`	100
`ListKeys request rate`	500
`ListKeyRotations request rate`	100
`ListResourceTags request rate`	2000
`ListRetirableGrants request rate`	100
`PutKeyPolicy request rate`	15
`ReplicateKey request rate` Uma operação `ReplicateKey` conta como uma solicitação `ReplicateKey` na região da chave primária e duas solicitações `CreateKey` na região da réplica. Uma das solicitações `CreateKey` é uma simulação para detectar possíveis problemas antes de criar a chave.	5
`RetireGrant request rate`	30
`RevokeGrant request rate`	30
`RotateKeyOnDemand request rate`	5
`ScheduleKeyDeletion request rate`	15
`TagResource request rate`	10
`UntagResource request rate`	5
`UpdateAlias request rate`	5

Nome da cota	Valor padrão (solicitações por segundo)
`UpdateCustomKeyStore request rate`	5
`UpdateKeyDescription request rate`	5
`UpdatePrimaryRegion request rate` Uma operação `UpdatePrimaryRegion` conta como duas solicitações `UpdatePrimaryRegion` ; uma solicitação em cada uma das duas regiões afetadas.	5

Aplicar cotas de solicitações

Ao analisar as cotas de solicitações, tenha em mente as seguintes informações.

- Cotas de solicitações aplicam-se achaves gerenciadas pelo cliente e a Chaves gerenciadas pela AWS. O uso de Chaves pertencentes à AWSnão conta nas cotas de solicitação para você Conta da AWS, mesmo quando elas são usadas para proteger recursos em sua conta.
- Cotas de solicitações aplicam-se a solicitações enviadas a endpoints FIPS e não FIPS. Para obter uma lista de endpoints de AWS KMS serviço, consulte AWS Key Management Service endpoints e cotas no. Referência geral da AWS
- O controle de utilização é baseado em todas as solicitações em chaves do KMS de todos os tipos na região. Esse total inclui solicitações de todos os diretores do Conta da AWS, incluindo solicitações de AWS serviços em seu nome.
- Cada cota de solicitações é calculada de maneira independente. Por exemplo, as solicitações da CreateKeyoperação não têm efeito na cota de solicitações da CreateAliasoperação. Se as solicitações `CreateAlias` forem limitadas, as solicitações `CreateKey` ainda poderão ser concluídas com êxito.
- Embora as operações de criptografia compartilhem uma cota, a cota compartilhada é calculada independentemente das cotas de outras operações. Por exemplo, as chamadas para as operações Encrypt e Decrypt compartilham uma cota de solicitação, mas essa cota é independente da cota para operações de gerenciamento, como. EnableKey Por exemplo, na região Europa (Londres), é possível executar 10.000 operações de criptografia em chaves do KMS simétricas mais 5 operações `EnableKey` por segundo sem que haja limitação.

Cotas compartilhadas para operações de criptografia

AWS KMS operações criptográficas compartilham cotas de solicitação. É possível solicitar qualquer combinação de operações de criptografia compatíveis com a chave do KMS, para que o número total de operações de criptografia não exceda a cota de solicitações desse tipo de chave do KMS. As exceções são GenerateDataKeyPaire GenerateDataKeyPairWithoutPlaintext, que compartilham uma cota separada.

As cotas para diferentes tipos de chaves do KMS são calculadas de maneira independente. Cada cota se aplica a todas as solicitações dessas operações na região Conta da AWS e com o tipo de chave determinado em cada intervalo de um segundo.

- A taxa de solicitações de operações de criptografia (simétricas) é a cota de solicitações compartilhadas para operações de criptografia que usam chaves do KMS simétricas em uma conta e região. Essa cota se aplica a operações criptográficas com chaves de criptografia simétrica e chaves de Hash-based message authentication code (HMAC – Código de autenticação de mensagem por hash), que também são simétricas.

  Por exemplo, você pode estar usando chaves KMS simétricas em uma Região da AWS cota compartilhada de 10.000 solicitações por segundo. Quando você faz 7.000 GenerateDataKeysolicitações por segundo e 2.000 solicitações Decrypt por segundo, AWS KMS não restringe suas solicitações. No entanto, quando você faz 9.500 solicitações `GenerateDataKey` e 1.000 solicitações Encrypt por segundo, o AWS KMS limita as solicitações porque elas excedem a cota compartilhada.

  As operações criptográficas nas chaves do KMS de criptografia simétrica em um armazenamento de chaves personalizadas contam tanto para a taxa de solicitação de operações criptográficas (simétricas) da conta quanto para a cota de solicitação de armazenamento de chaves personalizadas para o armazenamento de chaves personalizadas.
- A taxa de solicitações de operações de criptografia (RSA) é a cota de solicitações compartilhadas de operações de criptografia que usam chaves do KMS assimétricas RSA.

  Por exemplo, com uma cota de solicitações de 500 operações por segundo, é possível fazer 200 solicitações Encrypt e 100 solicitações Decrypt com chaves do KMS RSA que podem criptografar e descriptografar, além de 50 solicitações Sign e 150 solicitações Verify com chaves do KMS RSA que podem assinar e verificar.
- A taxa de solicitações de operações de criptografia (ECC) é a cota de solicitações compartilhadas de operações de criptografia que usam chaves do KMS assimétricas de curva elíptica (ECC).

Por exemplo, com uma cota de solicitações de 300 operações por segundo, é possível fazer 100 solicitações Sign e 200 solicitações Verify com chaves do KMS RSA que podem assinar e verificar.

- A taxa de solicitações de operações de criptografia (SM - somente nas regiões da China) é a cota de solicitações compartilhada para operações criptográficas que usam chaves do KMS assimétricas SM.

  Por exemplo, com uma cota de solicitações de 300 operações por segundo, é possível fazer 100 solicitações Encrypt e 100 solicitações Decrypt com chaves do KMS SM2 que podem criptografar e descriptografar, mais de 50 solicitações Sign e 50 solicitações Verify com chaves do KMS SM2 que podem assinar e verificar.
- A cota de solicitação de armazenamento de chaves personalizadas corresponde à cota de solicitação compartilhada para operações criptográficas em chaves do KMS em um armazenamento de chaves personalizadas. Essa cota é calculada separadamente para cada armazenamento de chaves personalizado.

  As operações criptográficas nas chaves do KMS de criptografia simétrica em um armazenamento de chaves personalizadas contam tanto para a taxa de solicitação de operações criptográficas (simétricas) da conta quanto para a cota de solicitação de armazenamento de chaves personalizadas para o armazenamento de chaves personalizadas.

As cotas para diferentes tipos de chave também são calculadas de forma independente. Por exemplo, na região Ásia-Pacífico (Singapura), se usar chaves do KMS simétricas e assimétricas, você poderá fazer até 10.000 chamadas por segundo com chaves do KMS simétricas (incluindo chaves de HMAC) mais até 500 chamadas adicionais por segundo com suas chaves do KMS assimétricas RSA, mais até 300 solicitações adicionais por segundo com suas chaves do KMS baseadas em ECC.

Solicitações de API dofeitas em seu nome

Você pode fazer solicitações de API diretamente ou usando um AWS serviço integrado que faz solicitações de API AWS KMS em seu nome. A cota se aplica a ambos os tipos de solicitações.

Por exemplo, você pode armazenar dados no Amazon S3 usando a criptografia no lado do servidor com uma chave do KMS (SSE-KMS). Sempre que você carrega ou baixa um objeto do S3 criptografado com SSE-KMS, o Amazon S3 faz uma solicitação `GenerateDataKey` (para uploads) ou `Decrypt` (para downloads) em seu nome. AWS KMS Essas solicitações contam para sua cota, portanto, limita AWS KMS as solicitações se você exceder um total combinado de 5.500 (ou 10.000

ou 50.000, dependendo da sua Região da AWS) upload ou download por segundo de objetos do S3 criptografados com SSE-KMS.

Solicitações entre contas

Quando um aplicativo em um Conta da AWS usa uma chave KMS de propriedade de uma conta diferente, isso é conhecido como solicitação entre contas. Nas solicitações entre contas, o AWS KMS limita a conta que faz as solicitações, e não a conta que possui a chave do KMS. Por exemplo, se uma aplicação na conta A usar uma chave do KMS na conta B, o uso da chave do KMS será aplicado somente às cotas na conta A.

Cotas de solicitação de armazenamento de chaves personalizadas

AWS KMS mantém cotas de solicitação para operações criptográficas nas chaves KMS em um armazenamento de chaves personalizado. Essas cotas de solicitação são calculadas separadamente para cada armazenamento de chaves personalizadas.

Cota de solicitações do armazenamento de chaves personalizado	Valor padrão (solicitações por segundo) para cada armazenamento de chaves personalizadas	Ajustável
AWS CloudHSM cota de solicitação de armazenamento de chaves	1800	Não
Cota de solicitação de armazenamento de chaves externas	1800	Sim

> **Note**
>
> AWS KMS as cotas de solicitação de armazenamento de chaves personalizadas não aparecem no console Service Quotas. Não é possível visualizar ou gerenciar essas cotas usando as operações da API do Service Quotas. Para solicitar uma alteração em sua cota de solicitação de armazenamento de chaves externas, visite o AWS Support Center e crie um caso.

Se o AWS CloudHSM cluster associado a um armazenamento de AWS CloudHSM chaves estiver processando vários comandos, incluindo aqueles não relacionados ao armazenamento de chaves personalizadas, você poderá receber um AWS KMS `ThrottlingException` em uma lower-than-expected taxa. Se isso ocorrer, reduza sua taxa de solicitação AWS KMS, reduza a carga não relacionada ou use um AWS CloudHSM cluster dedicado para seu armazenamento de AWS CloudHSM chaves.
AWS KMS relata a limitação de solicitações externas de armazenamento de chaves na `ExternalKeyStoreThrottle` CloudWatch métrica. É possível usar essa métrica para visualizar padrões de controle de utilização, criar alarmes e ajustar a cota de solicitação de armazenamento de chaves externas.

Uma solicitação para uma operação criptográfica em uma chave do KMS em um armazenamento de chaves personalizadas é contabilizada para duas cotas:

- Cota de taxa de solicitação de operações criptográficas (simétricas) (por conta)

  As solicitações de operações criptográficas em chaves do KMS em um armazenamento de chaves personalizadas são contabilizadas na cota `Cryptographic operations (symmetric) request rate` para cada região e Conta da AWS . Por exemplo, no Leste dos EUA (Norte da Virgínia) (us-east-1), cada Conta da AWS pode ter até 50 mil solicitações por segundo em chaves do KMS de criptografia simétrica, incluindo solicitações que usam uma chave do KMS em um armazenamento de chaves personalizadas.
- Cota de solicitação de armazenamento de chaves personalizadas (por armazenamento de chaves personalizadas)

  As solicitações de operações criptográficas em chaves do KMS em um armazenamento de chaves personalizadas também são contabilizadas para `Custom key store request quota` de 1.800 operações por segundo. Essas cotas são calculadas separadamente para cada armazenamento de chaves personalizadas. Eles podem incluir solicitações de várias pessoas Contas da AWS que usam chaves KMS no armazenamento de chaves personalizadas.

Por exemplo, uma operação Encrypt em uma chave do KMS em um armazenamento de chaves personalizadas (de qualquer tipo) na região Leste dos EUA (Norte da Virgínia) (us-east-1) será contabilizada para a cota em nível de conta da `Cryptographic operations (symmetric) request rate` (50 mil solicitações por segundo) para sua conta e região, e para a `Custom key store request quota` (1.800 solicitações por segundo) para seu armazenamento de chaves

personalizadas. No entanto, uma solicitação para uma operação de gerenciamento PutKeyPolicy, como em uma chave KMS em um armazenamento de chaves personalizadas, se aplica somente à cota em nível de conta (15 solicitações por segundo).

Solicitações de AWS KMS limitação

Para garantir que AWS KMS possa fornecer respostas rápidas e confiáveis às solicitações de API de todos os clientes, ele limita as solicitações de API que excedem certos limites.

A limitação ocorre quando AWS KMS rejeita uma solicitação que, de outra forma, poderia ser válida e retorna um `ThrottlingException` erro como o seguinte.

```
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 as solicitações para as seguintes condições.

- A taxa de solicitações por segundo excede a cota de AWS KMS solicitações de uma conta e região.

  Por exemplo, se os usuários da sua conta enviarem 1.000 `DescribeKey` solicitações em um segundo, AWS KMS limitará todas as `DescribeKey` solicitações subsequentes nesse segundo.

  Para responder a um controle de utilização, use uma estratégia de recuo e repetição. Essa estratégia é implementada automaticamente para erros de HTTP 400 em alguns AWS SDKs.
- Uma taxa intermitente ou alta sustentada de solicitações para alterar o estado da mesma chave do KMS. Essa condição é muitas vezes conhecida como "tecla de atalho".

  Por exemplo, se um aplicativo em sua conta enviar uma série persistente de `DisableKey` solicitações `EnableKey` e solicitações para a mesma chave KMS, as solicitações serão AWS KMS limitadas. Essa limitação ocorre mesmo que as solicitações não excedam o limite de request-per-second solicitações para as operações `EnableKey` e. `DisableKey`

  Para responder ao controle de utilização, ajuste a lógica da aplicação para que ela faça apenas as solicitações necessárias ou consolide as solicitações de várias funções.
- As solicitações de operações em chaves KMS em um armazenamento de AWS CloudHSM chaves podem ser limitadas a uma lower-than-expected taxa quando o AWS CloudHSM cluster associado

ao armazenamento de AWS CloudHSM chaves está processando vários comandos, incluindo aqueles não relacionados ao armazenamento de chaves. AWS CloudHSM

(AWS KMS não limita mais as solicitações de operações em chaves KMS em um AWS CloudHSM armazenamento de chaves quando não há sessões PKCS #11 disponíveis para o cluster. AWS CloudHSM Em vez disso, ele lança um `KMSInternalException` e recomenda que você repita sua solicitação.)

Para visualizar as tendências em suas taxas de solicitação, use o console do Service Quotas. Você também pode criar um CloudWatch alarme da Amazon que o alerta quando sua taxa de solicitação atingir uma determinada porcentagem do valor da cota. Para obter detalhes, consulte Gerenciar suas taxas de solicitação de AWS KMS API usando Service Quotas e Amazon CloudWatch no Blog de AWS Segurança.

Todas as AWS KMS cotas são ajustáveis, exceto a cota de recursos do tamanho do documento de política principal, a cota de recursos de rotação sob demanda e a cota de solicitação do armazenamento de AWS CloudHSM chaves. Para solicitar um aumento da cota, consulte Requesting a quota increase no Guia do usuário do Service Quotas. Para solicitar uma redução de cota, alterar uma cota que não está listada nas Cotas de Serviço ou alterar uma cota em uma área em que as Cotas de Região da AWS Serviço não estejam disponíveis, visite AWS Support o Centro e crie um caso. AWS KMS

> **Note**
>
> AWS KMS as cotas de solicitação de armazenamento de chaves personalizadas não aparecem no console Service Quotas. Não é possível visualizar ou gerenciar essas cotas usando as operações da API do Service Quotas. Para solicitar uma alteração em sua cota de solicitação de armazenamento de chaves externas, visite o AWS Support Center e crie um caso.

Como os serviços da AWS, usam o AWS KMS

Muitos serviços da AWS usam o AWS KMS para oferecer suporte à criptografia de seus dados. Quando um serviço da AWS está integrado ao AWS KMS, é possível usar as AWS KMS keys na sua conta para proteger os dados que o serviço recebe, armazena ou gerencia para você. Para obter a lista completa de serviços da AWS que estão integrados ao AWS KMS, consulte Integração de serviços da AWS.

Os tópicos a seguir discutem em detalhes como determinados serviços usam o AWS KMS, incluindo as chaves do KMS com as quais são compatíveis, como eles gerenciam chaves de dados, as permissões de que precisam e como rastrear o uso das chaves do KMS de cada serviço em sua conta.

> **Important**
>
> Os serviços da AWS que são integrados ao AWS KMS usam exclusivamente chaves do KMS de criptografia simétrica para criptografar seus dados. Esses serviços não fornecem suporte para criptografia com chaves do KMS assimétricas. Para obter ajuda para determinar se uma chave do KMS é simétrica ou assimétrica, consulte Identificar chaves do KMS assimétricas.

Tópicos

- Como o AWS CloudTrail usa o AWS KMS
- Como o Amazon DynamoDB usa o AWS KMS
- Como o Amazon Elastic Block Store (Amazon EBS) usa o AWS KMS
- Como o Amazon Elastic Transcoder usa o AWS KMS
- Como o Amazon EMR usa o AWS KMS
- Como o AWS Nitro Enclaves usa o AWS KMS
- Como o Amazon Redshift usa o AWS KMS
- Como o Amazon Relational Database Service (Amazon RDS) usa o AWS KMS
- Como o AWS Secrets Manager usa o AWS KMS
- Como o Amazon Simple Email Service (Amazon SES) usa o AWS KMS
- Como o Amazon Simple Storage Service (Amazon S3) usa o AWS KMS
- Como o AWS Systems Manager Parameter Store usa o AWS KMS

- Como a Amazon WorkMail usa AWS KMS
- Como WorkSpaces usa AWS KMS

Como o AWS CloudTrail usa o AWS KMS

É possível usar o AWS CloudTrail para registrar chamadas à API da AWS e outras atividades da sua Conta da AWS e salvar as informações registradas nos arquivos de log em um bucket do Amazon Simple Storage Service (Amazon S3) de sua escolha. Por padrão, os arquivos de log colocados em seu bucket CloudTrail do S3 são criptografados usando criptografia do lado do servidor com chaves de criptografia gerenciadas pelo Amazon S3 (SSE-S3). Mas você pode optar por usar a criptografia do lado do servidor com uma chave do KMS (SSE-KMS). Para saber como criptografar seus arquivos de CloudTrail log comAWS KMS, consulte Criptografando arquivos de CloudTrail log com AWS KMS keys (SSE-KMS) no Guia do usuário. AWS CloudTrail

> **Important**
>
> O AWS CloudTrail e o Amazon S3 só oferece suporte a AWS KMS keys simétricas. Você não pode usar uma chave KMS assimétrica para criptografar seus registros. CloudTrail Para obter ajuda para determinar se uma chave do KMS é simétrica ou assimétrica, consulte Identificar chaves do KMS assimétricas.

Você não paga uma taxa de uso da chave ao CloudTrail ler ou gravar arquivos de log criptografados com uma chave SSE-KMS. No entanto, você paga uma taxa de uso da chave ao acessar arquivos de CloudTrail log criptografados com uma chave SSE-KMS. Para obter mais informações sobre a definição de preço do AWS KMS, consulte Definição de preço do AWS Key Management Service. Para obter informações sobre CloudTrail preços, consulte AWS CloudTrailpreços e gerenciamento de custos no Guia AWS CloudTrail do usuário.

Tópicos

- Entender quando sua chave do KMS é usada

Entender quando sua chave do KMS é usada

Criptografar arquivos de CloudTrail log com AWS KMS versões do recurso Amazon S3 chamado criptografia do lado do servidor com um (SSE-KMS). AWS KMS key Para saber mais sobre o SSE-

KMS, consulte Como o Amazon Simple Storage Service (Amazon S3) usa o AWS KMS neste guia ou Proteção de dados usando a criptografia no lado do servidor com chaves gerenciadas pelo KMS (SSE-KMS) no Guia do usuário do Amazon Simple Storage Service.

Quando você configura AWS CloudTrail para usar o SSE-KMS para criptografar seus arquivos de log, e o Amazon CloudTrail S3 os usa AWS KMS keys quando você executa determinadas ações com esses serviços. As seções a seguir explicam quando e como esses serviços podem usar a chave do KMS e fornecem informações adicionais que podem validar essa explicação.

Ações que fazem com CloudTrail que o Amazon S3 use sua chave KMS

- Você configura CloudTrail para criptografar arquivos de log com seu AWS KMS key
- CloudTrail coloca um arquivo de log em seu bucket do S3
- Um arquivo de log criptografado é recebido do seu bucket do S3

Você configura CloudTrail para criptografar arquivos de log com seu AWS KMS key

Quando você atualiza sua CloudTrail configuração para usar sua chave KMS, CloudTrail envia uma `GenerateDataKey`solicitação AWS KMS para verificar se a chave KMS existe e se CloudTrail tem permissão para usá-la para criptografia. CloudTrail não usa a chave de dados resultante.

A solicitação `GenerateDataKey` inclui as seguintes informações para o contexto de criptografia:

- O Amazon Resource Name (ARN) da trilha CloudTrail
- O ARN do bucket do S3 e o caminho em que os arquivos de CloudTrail log são entregues

A `GenerateDataKey` solicitação resulta em uma entrada em seus CloudTrail registros semelhante ao exemplo a seguir. Ao ver uma entrada de registro como essa, você pode determinar que CloudTrail (1) chamou a `GenerateDataKey` operação AWS KMS (2) (3) para uma trilha específica (4). AWS KMScriou a chave de dados em uma chave KMS específica (5).

> **Note**
>
> Talvez você precise rolar para a direita para ver algumas das legendas no seguinte exemplo de entrada de log.

```
{
  "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 coloca um arquivo de log em seu bucket do S3

Cada vez que CloudTrail coloca um arquivo de log em seu bucket do S3, o Amazon S3 envia `GenerateDataKey`uma solicitação em nome AWS KMS de. CloudTrail Em resposta a essa solicitação, o AWS KMS gera uma chave de dados exclusiva e envia ao Amazon S3 duas cópias da chave de dados, uma em texto simples e uma criptografada com a chave do KMS especificada. O Amazon S3 usa a chave de dados de texto simples para criptografar o arquivo de CloudTrail log e, em seguida, remove a chave de dados de texto simples da memória assim que possível após o uso. O Amazon S3 armazena a chave de dados criptografada como metadados com o arquivo de log criptografado CloudTrail .

A solicitação `GenerateDataKey` inclui as seguintes informações para o contexto de criptografia:

- O Amazon Resource Name (ARN) da trilha CloudTrail
- O ARN do objeto S3 (o arquivo de log) CloudTrail

Cada `GenerateDataKey` solicitação resulta em uma entrada em seus CloudTrail registros semelhante ao exemplo a seguir. Ao ver uma entrada de registro como essa, você pode determinar que CloudTrail (1) chamou a `GenerateDataKey` operação AWS KMS (2) (3) para uma trilha específica (4) para proteger um arquivo de log específico (5).

AWS KMScriou a chave de dados sob a chave KMS especificada
(6),
mostrada duas vezes na mesma entrada de registro.

> **Note**
>
> Talvez você precise rolar para a direita para ver algumas das legendas no seguinte exemplo de entrada de log.

```
{
  "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"
}
```

Um arquivo de log criptografado é recebido do seu bucket do S3

Cada vez que você recebe um arquivo de CloudTrail log criptografado do seu bucket do S3, o Amazon S3 envia `Decrypt`uma solicitação em seu nome AWS KMS para descriptografar a chave de dados criptografada do arquivo de log. Em resposta a essa solicitação, o AWS KMS usa sua chave do KMS para descriptografar a chave de dados e depois envia a chave de dados de texto simples para o Amazon S3. O Amazon S3 usa a chave de dados de texto simples para descriptografar o arquivo de CloudTrail log e, em seguida, remove a chave de dados de texto sem formatação da memória assim que possível após o uso.

A solicitação `Decrypt` inclui as seguintes informações para o contexto de criptografia:

- O Amazon Resource Name (ARN) da trilha CloudTrail
- O ARN do objeto S3 (o arquivo de log) CloudTrail

Cada `Decrypt` solicitação resulta em uma entrada em seus CloudTrail registros semelhante ao exemplo a seguir. Ao obter uma entrada de log como esta, você pode determinar que um usuário em sua Conta da AWS (1) chamou a operação `Decrypt` (2) do AWS KMS (3) para uma trilha específica (4) e um arquivo de log específico (5). O AWS KMS descriptografou a chave de dados em uma chave do KMS específica (6).

> **Note**
>
> Talvez você precise rolar para a direita para ver algumas das legendas no seguinte exemplo de entrada de log.

```
{
  "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"
}
```

Como o Amazon DynamoDB usa o AWS KMS

O Amazon DynamoDB é um serviço de banco de dados NoSQL totalmente gerenciado e escalável. O DynamoDB integra-se ao AWS Key Management Service (AWS KMS) para comportar o recurso opcional de criptografia em repouso no lado do servidor.

Com a criptografia em repouso, o DynamoDB criptografa de forma transparente todos os dados do cliente em uma tabela do DynamoDB, incluindo sua chave primária e índices secundários locais e globais, sempre que a tabela é mantida no disco. (Se sua tabela tem uma chave de classificação, algumas dessas chaves que marcam os limites de intervalo são armazenadas em textos simples nos metadados da tabela.) Quando você acessa uma tabela criptografada, o DynamoDB descriptografa

os dados da tabela de maneira transparente. Você não precisa alterar suas aplicações para usar ou gerenciar tabelas criptografadas.

A criptografia em repouso protege o DynamoDB Streams, tabelas globais e backups sempre que esses objetos são salvos em uma mídia durável. As instruções sobre tabelas neste tópico também se aplicam a esses objetos.

Todas as tabelas do DynamoDB são criptografadas. Não há opção para habilitar ou desabilitar a criptografia para tabelas novas ou existentes. Por padrão, todas as tabelas são criptografadas sob uma Chave pertencente à AWS na conta de serviço do DynamoDB. No entanto, é possível selecionar uma opção para criptografar algumas ou todas as tabelas em uma chave gerenciada pelo cliente ou na Chave gerenciada pela AWS para o DynamoDB na sua conta.

Para obter detalhes sobre o suporte do Amazon DynamoDB para chaves do KMS, consulte Criptografia em repouso do DynamoDB no Guia do desenvolvedor do Amazon DynamoDB.

Como o Amazon Elastic Block Store (Amazon EBS) usa o AWS KMS

Este tópico discute em detalhes como o Amazon Elastic Block Store (Amazon EBS) usa o AWS KMS para criptografar volumes e snapshots. Para obter instruções básicas sobre a criptografia de volumes do Amazon EBS, consulte Criptografia do Amazon EBS.

Tópicos

- Criptografia de Amazon EBS
- Usar chaves do KMS e chaves de dados
- Contexto de criptografia do Amazon EBS
- Detectar falhas do Amazon EBS
- Como usar o AWS CloudFormation para criar volumes criptografados do Amazon EBS

Criptografia de Amazon EBS

Quando você anexa um volume do Amazon EBS criptografado a um tipo de instância do Amazon Elastic Compute Cloud (Amazon EC2) com suporte, os dados são armazenados em repouso no volume, E/S de disco e snapshots criados do volume são todos criptografados. A criptografia ocorre nos servidores que hospedam instâncias do Amazon EC2.

Esse recurso tem suporte em todos os tipos de volume do Amazon EBS. Você acessa os volumes criptografados da mesma forma que acessa outros volumes; a criptografia e a descriptografia são manipuladas de forma transparente e elas não exigem ações adicionais de você, sua instância do EC2 ou sua aplicação. Snapshots de volumes criptografados são criptografados automaticamente, e os volumes que são criados dos snapshots criptografados também são criptografados automaticamente.

O status da criptografia de um volume do EBS é determinado quando você cria o volume. Não é possível alterar o status de criptografia de um volume existente. No entanto, você pode migrar dados entre os volumes criptografados e não criptografados, e aplicar um novo status de criptografia enquanto copia um snapshot.

Por padrão, o Amazon EBS é compatível com criptografia opcional. É possível habilitar a criptografia automaticamente em todos os novos volumes do EBS e cópias de snapshots na Conta da AWS e região. Essa configuração não afeta volumes ou snapshots existentes. Para obter mais detalhes, consulte Criptografia por padrão no Manual do usuário do Amazon EC2 para instâncias Linux ou no Manual do usuário do Amazon EC2 para instâncias Windows.

Usar chaves do KMS e chaves de dados

Ao criar um volume do Amazon EBS criptografado, você especifica uma AWS KMS key. Por padrão, o Amazon EBS usa a Chave gerenciada pela AWS para o Amazon EBS na sua conta (`aws/ebs`). No entanto, você pode especificar uma chave gerenciada pelo cliente que você cria e gerencia.

Para usar uma chave gerenciada pelo cliente, você deve dar ao Amazon EBS a permissão para usar a chave do KMS em seu nome. Para obter uma lista de permissões necessárias, consulte Permissões para usuários do IAM, noManual do usuário do Amazon EC2 para instâncias Linux ou no Manual do usuário do Amazon EC2 para instâncias Windows.

> **Important**
>
> O Amazon EBS oferece suporte somente para chaves do KMS simétricas. Não é possível usar uma chave do KMS assimétrica para criptografar um volume do Amazon EBS. Para obter ajuda para determinar se uma chave do KMS é simétrica ou assimétrica, consulte Identificar chaves do KMS assimétricas.

Para cada volume, o Amazon EBS pede ao AWS KMS para gerar uma chave de dados exclusiva criptografada sob a chave do KMS que você especifica. O Amazon EBS armazena a chave de

dados criptografada com o volume. Em seguida, quando você anexa o volume a uma instância do Amazon EC2, o Amazon EBS chama o AWS KMS para descriptografar a chave de dados. O Amazon EBS usa a chave de dados em texto simples na memória do hipervisor para criptografar toda a E/S de disco no volume. Para obter mais detalhes, consulte Como funciona a criptografia do EBS, no Manual do usuário do Amazon EC2 para instâncias Linux ou no Manual do usuário do Amazon EC2 para instâncias Windows.

Contexto de criptografia do Amazon EBS

Em suas solicitações GenerateDataKeyWithoutPlaintexte Decrypt para, o AWS KMS Amazon EBS usa um contexto de criptografia com um par de nome-valor que identifica o volume ou o snapshot na solicitação. O nome no contexto de criptografia não varia.

Um contexto de criptografia é um conjunto de pares de chave-valor que contêm dados arbitrários não secretos. Quando você inclui um contexto de criptografia em uma solicitação para criptografar dados, o AWS KMS vincula de forma criptográfica o contexto de criptografia aos dados criptografados. Para descriptografar os dados, você deve passar o mesmo contexto de criptografia.

Para todos os volumes e para snapshots criptografados criados com a CreateSnapshotoperação do Amazon EBS, o Amazon EBS usa o ID do volume como valor do contexto de criptografia. No campo `requestParameters` de uma entrada de log do CloudTrail, o contexto de criptografia é parecido com o seguinte:

```
"encryptionContext": {
  "aws:ebs:id": "vol-0cfb133e847d28be9"
}
```

Para snapshots criptografados criados com a operação do Amazon CopySnapshotEC2, o Amazon EBS usa o ID do snapshot como valor de contexto de criptografia. No campo `requestParameters` de uma entrada de log do CloudTrail, o contexto de criptografia é parecido com o seguinte:

```
"encryptionContext": {
  "aws:ebs:id": "snap-069a655b568de654f"
}
```

Detectar falhas do Amazon EBS

Para criar um volume do EBS criptografado ou anexar o volume a uma instância do EC2, o Amazon EBS e a infraestrutura do Amazon EC2 devem poder usar a chave do KMS especificada para a

criptografia de volume do EBS. Quando a chave do KMS não pode ser utilizada, por exemplo, quando seu estado de chave não está `Enabled`, há falha na criação ou na anexação do volume.

Nesse caso, o Amazon EBS envia um evento para a Amazon EventBridge (antigo CloudWatch Events) para notificá-lo sobre a falha. Em EventBridge, você pode estabelecer regras que acionam ações automáticas em resposta a esses eventos. Para obter mais informações, consulte CloudWatch Eventos da Amazon para Amazon EBS no Guia do usuário do Amazon EC2 para instâncias Linux, especialmente nas seguintes seções:

- Chave de criptografia inválida em Anexar ou reanexar volume
- Chave de criptografia inválida em Criar volume

Para corrigir essas falhas, verifique se a chave do KMS especificada para criptografia do volume do EBS está habilitada. Para fazer isso, primeiro visualize a chave do KMS para determinar o estado atual da chave (a coluna Status no AWS Management Console). Veja as informações em um dos links a seguir:

- Se o estado da chave do KMS estiver desabilitado, habilite-o.
- Se o estado da chave do KMS for importação pendente, importe material de chave.
- Se o estado de chave da chave do KMS for exclusão pendente, cancele a exclusão da chave.

Como usar o AWS CloudFormation para criar volumes criptografados do Amazon EBS

Você pode usar o AWS CloudFormation para criar volumes criptografados do Amazon EBS. Para obter mais informações, consulte AWS::EC2::Volume no Guia de Usuário AWS CloudFormation.

Como o Amazon Elastic Transcoder usa o AWS KMS

Você pode usar o Amazon Elastic Transcoder para converter arquivos de mídia armazenados em um bucket do Amazon S3 em formatos exigidos pelos dispositivos de reprodução do consumidor. Ambos os arquivos de entrada e saída podem ser criptografados e descriptografados. As seções a seguir discutem como o AWS KMS é usado nos dois processos.

Tópicos

- Criptografia do arquivo de entrada

- Descriptografia do arquivo de entrada
- Criptografia do arquivo de saída
- Proteção de conteúdo HLS
- Contexto de criptografia do Elastic Transcoder

Criptografia do arquivo de entrada

Antes de usar o Elastic Transcoder, crie um bucket do Amazon S3 e carregue seu arquivo de mídia nele. Você pode criptografar o arquivo antes de enviá-lo usando a criptografia do cliente do AES ou após o upload usando a criptografia do servidor do Amazon S3.

Caso escolha a criptografia do cliente usando o AES, você será responsável por criptografar o arquivo antes de o carregar no Amazon S3 e deverá fornecer acesso para o Elastic Transcoder à chave de criptografia. Faça isso usando uma AWS KMS key simétrica do AWS KMS para proteger a chave de criptografia do AES usada para criptografar o arquivo de mídia.

Se escolher a criptografia no lado do servidor, você permitirá que o Amazon S3 criptografe e descriptografe todos os arquivos em seu nome. Você pode configurar o Amazon S3 para usar uma de três chaves de criptografia diferentes para proteger a chave de dados exclusiva usada para criptografar seu arquivo:

- Uma chave do Amazon S3, uma chave de criptografia que o Amazon S3 possui e gerencia. Ela não faz parte da sua Conta da AWS.
- A Chave gerenciada pela AWS para o Amazon S3, uma chave do KMS que faz parte da sua conta, mas é criada e gerenciada pela AWS.
- Qualquer chave gerenciada pelo cliente simétrica que você cria usando o AWS KMS

> **Important**
>
> Para criptografia do lado do cliente e no lado do servidor, o Elastic Transcoder oferece suporte somente a chaves do KMS simétricas. Não é possível usar uma chave do KMS assimétrica para criptografar os arquivos do Elastic Transcoder. Para obter ajuda para determinar se uma chave do KMS é simétrica ou assimétrica, consulte Identificar chaves do KMS assimétricas.

É possível habilitar a criptografia e especificar uma chave usando o console do Amazon S3 ou as APIs do Amazon S3 apropriadas. Para obter mais informações sobre como o Amazon S3 realiza a criptografia, consulte Proteção de dados usando criptografia no lado do servidor com chaves do KMS (SSE-KMS) no Guia do usuário do Amazon Simple Storage Service.

Ao proteger o arquivo de entrada usando a Chave gerenciada pela AWS para o Amazon S3 na sua conta ou uma chave gerenciada pelo cliente, o Amazon S3 e o AWS KMS interagem da seguinte maneira:

1. O Amazon S3 solicita uma chave de dados de texto simples e uma cópia da chave de dados criptografada na chave do KMS especificada.
2. O AWS KMS cria uma chave de dados, criptografa-a com a chave do KMS especificada e envia a chave de dados em texto não criptografada e a chave de dados criptografada ao Amazon S3.
3. O Amazon S3 usa a chave de dados de texto não criptografado para criptografar o arquivo de mídia e armazena o arquivo no bucket do Amazon S3 especificado.
4. O Amazon S3 armazena a chave de dados criptografada junto com o arquivo de mídia criptografado.

Descriptografia do arquivo de entrada

Se você optar pela criptografia do lado do servidor do Amazon S3 para criptografar o arquivo de entrada, o Elastic Transcoder não descriptografará o arquivo. Em vez disso, o Elastic Transcoder depende do Amazon S3 para executar a descriptografia de acordo com as configurações que você especifica ao criar um trabalho e um pipeline.

Está disponível a seguinte combinação de configurações:

Modo de criptografia	AWS KMSChave do	Significado
`S3`	Padrão	O Amazon S3 cria e gerencia as chaves usadas para criptografar e descriptografar o arquivo de mídia. O processo não é visível para o usuário.
`S3-AWS-KMS`	Padrão	Por padrão, o Amazon S3 usa uma chave de dados criptogra

Modo de criptografia	AWS KMSChave do	Significado
		fada pela Chave gerenciada pela AWS para o Amazon S3 na sua conta para criptografar o arquivo de mídia.
`S3-AWS-KMS`	Personalizar (com o ARN)	O Amazon S3 usa uma chave de dados criptografada pela chave gerenciada pelo cliente especificada para criptografar o arquivo de mídia.

Quando o `S3-AWS-KMS` está especificado, o Amazon S3 e o AWS KMS trabalham em conjunto da seguinte maneira para executar a descriptografia.

1. O Amazon S3 envia a chave de dados criptografada ao AWS KMS.
2. O AWS KMS descriptografa a chave de dados usando a chave do KMS apropriada e envia a chave de dados em texto simples de volta ao Amazon S3.
3. O Amazon S3 usa a chave de dados em texto simples para descriptografar o texto cifrado.

Quando você escolhe a criptografia do lado do cliente usando uma chave AES, o Elastic Transcoder recupera o arquivo criptografado do bucket do Amazon S3 e o descriptografa. O Elastic Transcoder usa a chave do KMS que você especificou quando criou o pipeline para descriptografar a chave AES e usa a chave AES para descriptografar o arquivo de mídia.

Criptografia do arquivo de saída

O Elastic Transcoder criptografa o arquivo de saída, dependendo de como você especifica as configurações de criptografia ao criar um trabalho e um pipeline. As seguintes opções estão disponíveis:

Modo de criptografia	AWS KMSChave do	Significado
`S3`	Padrão	O Amazon S3 cria e gerencia as chaves usadas para

Modo de criptografia	AWS KMSChave do	Significado
		criptografar o arquivo de saída.
S3-AWS-KMS	Padrão	O Amazon S3 usa uma chave de dados criada pelo AWS KMS e criptografada pela Chave gerenciada pela AWS para o Amazon S3 na sua conta.
S3-AWS-KMS	Personalizar (com o ARN)	O Amazon S3 usa uma chave de dados criptografada usando a chave gerenciad a pelo cliente especificada pelo ARN para criptografar o arquivo de mídia.
AES-	Padrão	O Elastic Transcoder usa a Chave gerenciada pela AWS para o Amazon S3 na sua conta para descriptografar a chave do AES fornecida por você e usa essa chave para criptografar o arquivo de saída.
AES-	Personalizar (com o ARN)	O Elastic Transcoder usa a chave gerenciada pelo cliente especificada pelo ARN para descriptografar a chave do AES fornecida por você e usa essa chave para criptografar o arquivo de saída.

Quando você especifica que a Chave gerenciada pela AWS para o Amazon S3 na sua conta ou uma chave gerenciada pelo cliente é usada para criptografar o arquivo de saída, o Amazon S3 e o AWS KMS interagem da seguinte maneira:

1. O Amazon S3 solicita uma chave de dados de texto simples e uma cópia da chave de dados criptografada na chave do KMS especificada.
2. O AWS KMS cria uma chave de dados, criptografa-a com a chave do KMS e envia a chave de dados em texto simples e a chave de dados criptografada ao Amazon S3.
3. O Amazon S3 criptografa a mídia usando a chave de dados e a armazena no bucket do Amazon S3 especificado.
4. O Amazon S3 armazena a chave de dados criptografada junto ao arquivo de mídia criptografado.

Quando você especifica que sua chave AES fornecida deve ser usada para criptografar o arquivo de saída, a chave AES deve ser criptografada usando uma chave do KMS no AWS KMS. O Elastic Transcoder, o AWS KMS e você interagem da seguinte maneira:

1. Você criptografa a chave AES chamando a operação Encrypt na API do AWS KMS. O AWS KMS criptografa a chave usando a chave do KMS especificada. Você especifica qual chave do KMS será usada ao criar o pipeline.
2. Você especifica o arquivo que contém a chave do AES criptografada ao criar o trabalho do Elastic Transcoder.
3. O Elastic Transcoder descriptografa a chave chamando a operação Decrypt na API do AWS KMS passando a chave criptografada como texto cifrado.
4. O Elastic Transcoder usa a chave AES descriptografada para criptografar o arquivo de mídia de saída e exclui da memória a chave AES descriptografada. Somente a cópia criptografada originalmente definida no trabalho é salva no disco.
5. Você pode fazer download do arquivo de saída criptografado e descriptografá-lo localmente usando a chave AES original que você definiu.

> **Important**
>
> AWSA nunca armazena suas chaves de criptografia privadas. Portanto, é importante que você gerencie as chaves com segurança. Se perdê-las, você não poderá descriptografar os seus dados.

Proteção de conteúdo HLS

HTTP Live Streaming (HLS) é um protocolo de transmiss~;ao adaptável. O Elastic Transcoder oferece suporte ao HLS, dividindo seu arquivo de entrada em pequenos arquivos individuais, chamados segmentos de mídia. Um conjunto de segmentos de mídia individuais correspondentes contêm o mesmo material codificado com diferentes taxas de bits, permitindo que o jogador selecione a transmissão que melhor se adapta à largura de banda disponível. O Elastic Transcoder também cria listas de reprodução que contêm metadados dos vários segmentos disponíveis para serem transmitidos.

Quando você habilita a proteção de conteúdo HLS, cada segmento de mídia é criptografado usando uma chave de criptografia do AES de 128 bits. Quando o conteúdo é visualizado, durante o processo de reprodução, o player faz download da chave e descriptografa os segmentos de mídia.

São usados dois tipos de chave: uma chave do KMS e uma chave de dados. Crie uma chave do KMS para criptografar e descriptografar a chave de dados. O Elastic Transcoder usa a chave de dados para criptografar e descriptografar segmentos de mídia. A chave de dados deve AES-128. Todas as variações e segmentos do mesmo conteúdo são criptografados usando a mesma chave de dados. Forneça uma chave de dados ou deixe que o Elastic Transcoder crie-a para você.

A chave do KMS pode ser usada para criptografar a chave de dados nos seguintes pontos:

- Se você fornecer sua própria chave de dados, deverá criptografá-la antes de passá-la para o Elastic Transcoder.
- Se você solicitar que o Elastic Transcoder gere a chave de dados, ele a criptografará para você.

A chave do KMS pode ser usada para descriptografar a chave de dados nos seguintes pontos:

- O Elastic Transcoder descriptografa a chave de dados fornecida quando precisa usá-la para criptografar o arquivo de saída ou descriptografar o arquivo de entrada.
- Você descriptografa uma chave de dados gerada pelo Elastic Transcoder e usa-a para descriptografar arquivos de saída.

Para obter mais informações, consulteProteção de conteúdo HLS, no Guia do desenvolvedor do Amazon Elastic Transcoder.

Contexto de criptografia do Elastic Transcoder

Um contexto de criptografia é um conjunto de pares de chave-valor que contêm dados arbitrários não secretos. Quando você inclui um contexto de criptografia em uma solicitação para criptografar dados, o AWS KMS vincula de forma criptográfica o contexto de criptografia aos dados criptografados. Para descriptografar os dados, você deve passar o mesmo contexto de criptografia.

O Elastic Transcoder usa o mesmo contexto de criptografia em todas as solicitações de API do AWS KMS para gerar chaves de dados, criptografar e descriptografar.

```
"service" : "elastictranscoder.amazonaws.com"
```

O contexto de criptografia é gravado CloudTrail nos registros para ajudar você a entender como uma determinada chave AWS KMS KMS foi usada. No `requestParameters` campo de um arquivo de CloudTrail log, o contexto de criptografia é semelhante ao seguinte:

```
"encryptionContext": {
  "service" : "elastictranscoder.amazonaws.com"
}
```

Para obter mais informações sobre como configurar trabalhos do Elastic Transcoder para usar uma das opções de criptografia com suporte, consulte Opções de criptografia dos dados, no Guia do desenvolvedor do Amazon Elastic Transcoder.

Como o Amazon EMR usa o AWS KMS

Ao usar um cluster do Amazon EMR, você pode configurá-lo para criptografar dados em repouso antes de salvá-los em um local de armazenamento persistente. Você pode criptografar dados em repouso no EMR File System (EMRFS), nos volumes de armazenamento de nós de cluster, ou em ambos. Para criptografar dados em repouso, use uma AWS KMS key. Os tópicos a seguir explicam como um cluster do Amazon EMR usa uma chave do KMS para criptografar dados em repouso.

> **Important**
>
> O Amazon EMR oferece suporte somente a chaves do KMS simétricas. Não é possível usar uma chave do KMS assimétrica para criptografar dados em repouso em um cluster do Amazon EMR. Para obter ajuda para determinar se uma chave do KMS é simétrica ou assimétrica, consulte Identificar chaves do KMS assimétricas.

Os clusters do Amazon EMR também criptografam dados em trânsito, o que significa que o cluster criptografa os dados antes de enviá-los por meio da rede. Não é possível usar uma chave do KMS para criptografar dados em trânsito. Para obter mais informações, consulte Criptografia de dados em trânsito, no Guia de gerenciamento do Amazon EMR.

Para obter mais informações sobre todas as opções de criptografia disponíveis no Amazon EMR, consulte Opções de criptografia, noGuia de gerenciamento do Amazon EMR.

Tópicos

- Criptografar dados no EMR File System (EMRFS)
- Criptografar dados nos volumes de armazenamento dos nós de cluster
- Contexto de criptografia

Criptografar dados no EMR File System (EMRFS)

Os clusters do Amazon EMR usam dois sistemas de arquivos distribuídos:

- O Hadoop Distributed File System (HDFS). A criptografia do HDFS não usa uma chave do KMS no AWS KMS.
- O EMR File System (EMRFS). O EMRFS é uma implementação do HDFS que permite que os clusters do Amazon EMR armazenem dados no Amazon Simple Storage Service (Amazon S3). O EMRFS oferece suporte a quatro opções de criptografia, duas das quais usam uma chave do KMS no AWS KMS. Para obter mais informações sobre todas as quatro opções de criptografia do EMRFS, consulte Opções de criptografia, no Guia de gerenciamento do Amazon EMR.

As duas opções de criptografia do EMRFS que usam uma chave do KMS usam os seguintes recursos de criptografia oferecidos pelo Amazon S3:

- Proteção de dados usando criptografia do servidor com AWS Key Management Service (SSE-KMS). O cluster do Amazon EMR envia dados ao Amazon S3. O Amazon S3 usa uma chave do KMS para criptografar os dados antes de enviá-los a um bucket do S3. Para obter mais informações sobre como isso funciona, consulte Processo para criptografar dados no EMRFS com o SSE-KMS.
- Proteger dados usando a criptografia no lado do cliente (CSE-KMS). Os dados em um Amazon EMR são criptografados sob um AWS KMS key antes de serem enviados ao Amazon S3 para

armazenamento. Para obter mais informações sobre como isso funciona, consulte Processo para criptografar dados no EMRFS com o CSE-KMS.

Ao configurar um cluster do Amazon EMR para criptografar dados no EMRFS com uma chave do KMS, escolha a chave do KMS que deseja que o Amazon S3 ou o cluster do Amazon EMR use. Com o SSE-KMS, é possível escolher a Chave gerenciada pela AWS para o Amazon S3 com o alias aws/s3 ou uma chave simétrica gerenciada pelo cliente criada por você. Com a criptografia no lado do cliente, é necessário escolher uma chave simétrica gerenciada pelo cliente criada por você. Ao escolher uma chave gerenciada pelo cliente, é necessário garantir que o cluster do Amazon EMR tenha permissão para usar a chave do KMS. Para obter mais informações, consulteUsar AWS KMS keys para criptografia, noGuia de gerenciamento do Amazon EMR.

Para a criptografia do lado do servidor e a criptografia do lado do cliente, a chave do KMS que você escolhe é a chave raiz em um fluxo de trabalho de criptografia de envelope. Os dados são criptografados com uma chave de dados exclusiva que é criptografada sob a chave do KMS no AWS KMS. Os dados criptografados e uma cópia criptografada de sua chave de dados são armazenados em conjunto como um único objeto criptografado em um bucket do S3. Para obter mais informações sobre como isso funciona, consulte os tópicos a seguir.

Tópicos

- Processo para criptografar dados no EMRFS com o SSE-KMS
- Processo para criptografar dados no EMRFS com o CSE-KMS

Processo para criptografar dados no EMRFS com o SSE-KMS

Quando você configura um cluster do Amazon EMR para usar o SSE-KMS, o processo de criptografia funciona da seguinte forma:

1. O cluster envia os dados ao Amazon S3 para armazenamento em um bucket do S3.
2. O Amazon S3 envia uma GenerateDataKeysolicitação paraAWS KMS, especificando o ID da chave KMS que você escolheu ao configurar o cluster para usar o SSE-KMS. A solicitação inclui o contexto de criptografia, para obter mais informações, consulte Contexto de criptografia.
3. O AWS KMS gera uma chave de criptografia dos dados exclusiva (chave de dados) e envia duas cópias dessa chave de dados ao Amazon S3. Uma cópia é não criptografada (texto simples), e a outra cópia é criptografada com a chave do KMS.

4. O Amazon S3 usa a chave de dados de texto não criptografado para criptografar os dados que ela recebeu na etapa 1 e remove a chave de dados de texto não criptografado da memória, assim que possível, após o uso.
5. O Amazon S3 armazena os dados criptografados e a cópia criptografada da chave de dados em conjunto como um único objeto criptografado em um bucket do S3.

O processo de descriptografia funciona desta forma:

1. O cluster solicita um objeto de dados criptografado de um bucket do S3.
2. O Amazon S3 extrai a chave de dados criptografada do objeto do S3 e, em seguida, envia a chave de dados criptografada ao AWS KMS com uma solicitação Decrypt. A solicitação inclui um contexto de criptografia.
3. O AWS KMS descriptografa a chave de dados criptografada usando a mesma chave do KMS que foi usada para criptografá-la e, em seguida, envia a chave de dados descriptografada (texto não criptografado) ao Amazon S3.
4. O Amazon S3 usa a chave de dados de texto não criptografado para descriptografar os dados criptografados e, em seguida, remove a chave de dados de texto não criptografado da memória, assim que possível, após o uso.
5. O Amazon S3 envia os dados descriptografados ao cluster.

Processo para criptografar dados no EMRFS com o CSE-KMS

Quando você configura um cluster do Amazon EMR para usar o CSE-KMS, o processo de criptografia funciona da seguinte forma:

1. Quando estiver pronto para armazenar dados no Amazon S3, o cluster envia uma GenerateDataKeysolicitação paraAWS KMS, especificando o ID da chave KMS que você escolheu ao configurar o cluster para usar o CSE-KMS. A solicitação inclui o contexto de criptografia, para obter mais informações, consulte Contexto de criptografia.
2. AWS KMSO gera uma chave de criptografia dos dados exclusiva (chave de dados) e envia duas cópias dessa chave de dados ao cluster. Uma cópia é não criptografada (texto simples), e a outra cópia é criptografada com a chave do KMS.
3. O cluster usa a chave de dados de texto simples para criptografar os dados e remove a chave de dados de texto simples da memória, assim que possível após o uso.

4. O cluster combina os dados criptografados e a cópia criptografada da chave de dados em conjunto em um único objeto criptografado.
5. O cluster envia o objeto criptografado para o Amazon S3 para armazenamento.

O processo de descriptografia funciona desta forma:

1. O cluster solicita o objeto de dados criptografado de um bucket do S3.
2. O Amazon S3 envia o objeto criptografado ao cluster.
3. O cluster extrai a chave de dados criptografada do objeto criptografado e envia a chave de dados criptografada ao AWS KMS com uma solicitação Decrypt. A solicitação inclui o contexto de criptografia.
4. O AWS KMS descriptografa a chave de dados criptografada usando a mesma chave do KMS que foi usada para criptografá-la e, em seguida, envia a chave de dados descriptografada (em texto simples) ao cluster.
5. O cluster usa a chave de dados de texto simples para descriptografar os dados criptografados e remove a chave de dados de texto simples da memória, assim que possível após o uso.

Criptografar dados nos volumes de armazenamento dos nós de cluster

Um cluster do Amazon EMR é um conjunto de instâncias do Amazon Elastic Compute Cloud (Amazon EC2). Cada instância no cluster é chamada de um nó de cluster ou nó. Cada nó pode ter dois tipos de volumes de armazenamento: volumes de armazenamento de instância e volumes do Amazon Elastic Block Store (Amazon EBS). Você pode configurar o cluster para usar Linux Unified Key Setup (LUKS) para criptografar ambos os tipos de volumes de armazenamento nos nós (mas não o volume de inicialização de cada nó). Isso é chamado de criptografia de disco local.

Ao habilitar a criptografia de disco local para um cluster, você pode optar por criptografar a chave LUKS com uma chave do KMS no AWS KMS. É necessário selecionar uma chave gerenciada pelo cliente criada por você. Não é possível usar uma Chave gerenciada pela AWS. Se você escolher uma chave gerenciada pelo cliente, será necessário garantir que o cluster do Amazon EMR tenha permissão para usar a chave do KMS. Para obter mais informações, consulteUsar AWS KMS keys para criptografia, noGuia de gerenciamento do Amazon EMR.

Quando você habilita a criptografia de disco local usando uma chave do KMS, o processo de criptografia funciona desta forma:

1. Quando cada nó do cluster é iniciado, ele envia uma GenerateDataKeysolicitação paraAWS KMS, especificando o ID da chave KMS que você escolheu ao habilitar a criptografia de disco local para o cluster.
2. AWS KMSO gera uma chave de criptografia dos dados exclusiva (chave de dados) e envia duas cópias dessa chave de dados ao nó. Uma cópia é não criptografada (texto simples), e a outra cópia é criptografada com a chave do KMS.
3. O nó usa uma versão codificada em base64 da chave de dados em texto simples como a senha que protege a chave LUKS. O nó salva a cópia criptografada da chave de dados em seu volume de inicialização.
4. Se o nó for reinicializado, ele enviará a chave de dados criptografada ao AWS KMS com uma solicitação Decrypt.
5. O AWS KMS descriptografa a chave de dados criptografada usando a mesma chave do KMS que foi usada para criptografá-la e, em seguida, envia a chave de dados descriptografada (em texto simples) ao nó.
6. O nó usa uma versão codificada em base64 da chave de dados de texto simples como a senha para desbloquear a chave LUKS.

Contexto de criptografia

Cada serviço da AWS integrado ao AWS KMS pode especificar um contexto de criptografia ao usar o AWS KMS para gerar chaves de dados ou para criptografar ou descriptografar dados. O contexto de criptografia são informações adicionais autenticadas que o AWS KMS usa para verificar a integridade dos dados. Quando um serviço especifica um contexto de criptografia para uma operação de criptografia, ele deve especificar o mesmo contexto de criptografia para a operação de descriptografia correspondente ou a descriptografia não terá êxito. O contexto de criptografia também é gravado em arquivos de log do AWS CloudTrail, o que pode ajudar você a entender por que uma determinada chave do KMS foi usada.

A seção a seguir explica o contexto de criptografia usado em cada cenário de criptografia do Amazon EMR que usa uma chave do KMS.

Contexto de criptografia para criptografia EMRFS com o SSE-KMS

Com o SSE-KMS, o cluster Amazon EMR; envia dados ao Amazon S3 e, em seguida, o Amazon S3 usa uma chave do KMS para criptografar esses dados antes de enviá-los a um bucket do S3. Nesse caso, o Amazon S3 usa o Amazon Resource Name (ARN) do objeto S3 como contexto de

criptografia com cada solicitação GenerateDataKeye Decrypt para a qual ele envia. AWS KMS O exemplo a seguir mostra uma representação JSON do contexto de criptografia usado pelo Amazon S3.

```
{ "aws:s3:arn" : "arn:aws:s3:::S3_bucket_name/S3_object_key" }
```

Contexto de criptografia para criptografia EMRFS com o CSE-KMS

Com o CSE-KMS, o cluster do Amazon EMR usa uma chave do KMS para criptografar os dados antes de os enviar ao Amazon S3 para armazenamento. Nesse caso, o cluster usa o Amazon Resource Name (ARN) da chave KMS como contexto de criptografia com cada solicitação GenerateDataKeye Decrypt para a qual ele envia. AWS KMS O exemplo a seguir mostra uma representação JSON do contexto de criptografia que o cluster usa.

```
{ "kms_cmk_id" : "arn:aws:kms:us-
east-2:111122223333:key/0987ab65-43cd-21ef-09ab-87654321cdef" }
```

Contexto de criptografia para criptografia de disco local com LUKS

Quando um cluster do Amazon EMR usa criptografia de disco local com LUKS, os nós do cluster não especificam o contexto de criptografia com as solicitações GenerateDataKeye Decrypt para as quais eles enviam. AWS KMS

Como o AWS Nitro Enclaves usa o AWS KMS

O AWS KMS é compatível com o atestado criptográfico para Nitro Enclaves da AWS. Os aplicativos que oferecem suporte a Nitro Enclaves da AWS chamam as seguintes operações criptográficas do AWS KMS com um documento de atestado assinado para o enclave. Essas APIs do AWS KMS verificam se o documento de atestado veio de um Nitro enclave. Em seguida, em vez de retornarem dados de texto não criptografado na resposta, essas APIs criptografam o texto sem formatação com a chave pública do documento de atestado e retornam um texto cifrado que pode ser descriptografado somente pela chave privada correspondente no enclave.

- Decrypt
- GenerateDataKey
- GenerateDataKeyPair
- GenerateRandom

A tabela a seguir mostra como a resposta às solicitações do Nitro enclave difere da resposta padrão para cada operação de API.

Operação do AWS KMS	Resposta padrão	Resposta para Nitro Enclaves da AWS
`Decrypt`	Retorna dados de texto simples	Retorna dados de texto simples criptografados pela chave pública do documento de atestado
`GenerateDataKey`	Retorna uma cópia em texto simples da chave de dados (Também retorna uma cópia da chave de dados criptografada por uma chave do KMS)	Retorna uma cópia da chave de dados criptografada pela chave pública do documento de atestado (Também retorna uma cópia da chave de dados criptografada por uma chave do KMS)
`GenerateDataKeyPair`	Retorna uma cópia em texto simples da chave privada (Também retorna a chave pública e uma cópia da chave privada criptografada por uma chave do KMS)	Retorna uma cópia da chave privada criptografada pela chave pública do documento de atestado (Também retorna a chave pública e uma cópia da chave privada criptografada por uma chave do KMS)
`GenerateRandom`	Retorna uma string de bytes aleatória	Retorna a string de bytes aleatória criptografada pela chave pública do documento de atestado

O AWS KMS oferece suporte a chaves de condição de política, que você pode usar para permitir ou negar operações de enclave em uma chave do AWS KMS com base no conteúdo do documento de

atestado. Também é possível monitorar solicitações do AWS KMS para seu enclave Nitro nos logs do AWS CloudTrail.

Tópicos

- Como chamar APIs do AWS KMS para um Nitro enclave
- Chaves de condição do AWS KMS para o AWS Nitro Enclaves
- Solicitações de monitoramento para Nitro enclaves

Como chamar APIs do AWS KMS para um Nitro enclave

Para chamar APIs do AWS KMS para um Nitro enclave, use o parâmetro `Recipient` na solicitação para fornecer o documento de atestado assinado para o enclave e o algoritmo de criptografia a ser usado com a chave pública do enclave. Quando uma solicitação inclui o parâmetro `Recipient` com um documento de atestado assinado, a resposta inclui um campo `CiphertextForRecipient` com o texto cifrado criptografado pela chave pública. O campo de texto simples é nulo ou vazio.

O parâmetro `Recipient` deve especificar um documento de atestado assinado de um Nitro enclave da AWS. O AWS KMS baseia-se na assinatura digital do documento de atestado do enclave para provar que a chave pública na solicitação veio de um enclave válido. Não é possível fornecer seu próprio certificado para assinar digitalmente o documento de atestado.

Para especificar o parâmetro `Recipient`, use o SDK de Nitro Enclaves da AWS ou qualquer SDK da AWS. O SDK de Nitro Enclaves da AWS, que é compatível somente em enclaves Nitro, adiciona automaticamente o parâmetro `Recipient` e seus valores a cada solicitação do AWS KMS. Para fazer solicitações de Nitro enclaves nos SDKs da AWS, você precisa especificar o parâmetro `Recipient` e seus valores. O suporte ao atestado criptográfico do Nitro enclave nos SDKs da AWS foi introduzido em março de 2023.

O AWS KMS oferece suporte a chaves de condição de política, que você pode usar para permitir ou negar operações de enclave em uma chave do AWS KMS com base no conteúdo do documento de atestado. Também é possível monitorar solicitações do AWS KMS para seu enclave Nitro nos logs do AWS CloudTrail.

Para obter informações detalhadas sobre o `Recipient` parâmetro e o campo de `CiphertextForRecipient` resposta da AWS, consulte os GenerateRandomtópicos Decrypt,, GenerateDataKey, e na Referência da AWS Key Management Service API GenerateDataKeyPair, no SDK do AWSNitro Enclaves ou em qualquer SDK. AWS Para obter informações sobre como

configurar seus dados e chaves de dados para criptografia, consulteUsar atestado criptográfico com o AWS KMS.

Chaves de condição do AWS KMS para o AWS Nitro Enclaves

É possível especificar as condições da chaves nas políticas de chave e nas políticas do IAM que controlam o acesso aos recursos do AWS KMS. Declarações de política que incluem uma chave de condição só são efetivas quando suas condições são satisfeitas.

AWS KMSfornece chaves de condição que limitam as permissões para as GenerateRandomoperações Decrypt, GenerateDataKey, GenerateDataKeyPair, e com base no conteúdo do documento de atestado assinado na solicitação. Essas chaves de condição funcionam somente quando uma solicitação para uma operação do AWS KMS inclui o parâmetro `Recipient` com um documento de atestado válido de um Nitro enclave da AWS. Para especificar o parâmetro `Recipient`, use o SDK de Nitro Enclaves da AWS ou qualquer SDK da AWS.

As chave de condição do AWS KMS específicas do enclave são válidas em declarações de políticas de chaves e declarações de políticas do IAM, mesmo que não apareçam no console do IAM ou na Referência de autorização de serviço do IAM.

kmRecipientAttestation: 384 ImageSha

Chaves de condição do AWS KMS	Tipo de condição	Tipo de valor	Operações de API	Tipo de política

`kms:RecipientAttestation:ImageSha384`	String	Valor único	`Decrypt`
			`GenerateDataKey`
			`GenerateDataKeyPair`
			`GenerateRandom`
				Políticas de chaves e políticas do IAM

A chave de condição `kms:RecipientAttestation:ImageSha384` controla o acesso a `Decrypt`, `GenerateDataKey`, `GenerateDataKeyPair` e `GenerateRandom` com uma chave do KMS

quando o resumo da imagem do documento de atestado assinado na solicitação corresponde ao valor na chave de condição. O valor `ImageSha384` corresponde a PCR0 no documento de atestado. Essa chave de condição só é efetiva quando o parâmetro `Recipient` na solicitação especifica um documento de atestação assinado para um Nitro Enclave da AWS.

Esse valor também está incluído em CloudTraileventos AWS KMS para solicitações de enclaves Nitro.

> **Note**
>
> Essa chave de condição é válida em declarações de políticas de chaves e declarações de políticas do IAM, mesmo que não apareça no console do IAM ou na Referência de autorização de serviço do IAM.

Por exemplo, a declaração de política chave a seguir permite que a `data-processing` função use a chave KMS para descriptografar, GenerateDataKey, GenerateDataKeyPaire operações. GenerateRandom A chave de condição `kms:RecipientAttestation:ImageSha384` permite as operações somente quando o valor de resumo da imagem (PCR0) do documento de atestado na solicitação corresponde ao valor de resumo da imagem na condição. Essa chave de condição só é efetiva quando o parâmetro `Recipient` na solicitação especifica um documento de atestação assinado para um Nitro Enclave da AWS.

Se a solicitação não incluir um documento de atestado válido de um Nitro Enclave AWS, a permissão será negada porque essa condição não está atendida.

```
{
  "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
    }
  }
}
```

km:: PCR RecipientAttestation <PCR_ID>

Chaves de condição do AWS KMS	Tipo de condição	Tipo de valor	Operações de API	Tipo de política

`kms:RecipientAttestation:PCR<PCR_ID>`	String	Valor único	`Decrypt`
			`GenerateDataKey`
			`GenerateDataKeyPair`
			`GenerateRandom`
				Políticas de chaves e políticas do IAM

A chave de condição `kms:RecipientAttestation:PCR<PCR_ID>` permite solicitações `Decrypt`, `GenerateDataKey`, `GenerateDataKeyPair` e `GenerateRandom` com uma chave do KMS somente quando os registros de configuração de plataforma (PCRs) do documento de atestado assinado na solicitação correspondem aos PCRs na chave de condição. Essa chave de condição só é efetiva quando o parâmetro `Recipient` na solicitação especifica um documento de atestação assinado de um AWS Nitro Enclave.

Esse valor também está incluído em CloudTraileventos que representam solicitações AWS KMS para enclaves Nitro.

> **Note**
>
> Essa chave de condição é válida em declarações de políticas de chaves e declarações de políticas do IAM, mesmo que não apareça no console do IAM ou na Referência de autorização de serviço do IAM.

Para especificar um valor de PCR, use o seguinte formato. Concatene o ID do PCR com o nome da chave da condição. O valor so PCR deve ser uma string hexadecimal minúscula de até 96 bytes.

```
"kms:RecipientAttestation:PCRPCR_ID": "PCR_value"
```

Por exemplo, a chave de condição a seguir especifica um valor específico para PCR1, que corresponde ao hash do kernel usado para o enclave e o processo de bootstrap.

```
kms:RecipientAttestation:PCR1:
 "0x1abcdef2abcdef3abcdef4abcdef5abcdef6abcdef7abcdef8abcdef9abcdef8abcdef7abcdef6abcdef5abcdef
```

Por exemplo, a instrução de política de chave a seguir permite que a função `data-processing` use a chave do KMS para a operação Decrypt.

A chave de condição `kms:RecipientAttestation:PCR` nessa instrução permite a operação somente quando o valor PCR1 no documento de atestado assinado na solicitação corresponde ao valor `kms:RecipientAttestation:PCR1` na condição. Use a política a`StringEqualsIgnoreCase` para exigir uma comparação sem distinção entre maiúsculas e minúsculas dos valores de PCR.

Se a solicitação não incluir um documento de atestado, a permissão será negada porque essa condição não foi atendida.

```
{
  "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
    }
  }
}
```

Solicitações de monitoramento para Nitro enclaves

Você pode usar seus AWS CloudTrail registros para monitorar as GenerateRandomoperações de descriptografia,, GenerateDataKeyGenerateDataKeyPair, e de um AWS enclave Nitro. Nessas entradas de log, o campo `additionalEventData` tem um campo `recipient` com o ID do módulo (`attestationDocumentModuleId`), o resumo da imagem (`attestationDocumentEnclaveImageDigest`) e os registros de configuração da plataforma (PCRs) do documento de atestado na solicitação. Esses campos são incluídos somente quando o parâmetro `Recipient` na solicitação especifica um documento de atestação assinado de um Nitro Enclave da AWS.

O ID do módulo é o ID do enclave do Nitro enclave. O resumo da imagem é o hash SHA384 da imagem do enclave. É possível usar o resumo da imagem e os valores de PCR em condições para políticas de chave e políticas do IAM. Para obter informações sobre os PCRs, consulte Onde obter as medidas de um enclave no Guia do usuário de Nitro Enclaves da AWS.

Esta seção mostra um exemplo de entrada de CloudTrail registro para cada uma das solicitações de enclave Nitro suportadas para. AWS KMS

Decrypt (para um enclave)

O exemplo a seguir mostra uma entrada de log do AWS CloudTrail para uma operação Decrypt para um Nitro Enclave da 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 (para um enclave)

O exemplo a seguir mostra uma entrada de AWS CloudTrail registro de uma GenerateDataKeyoperação para um 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 (para um enclave)

O exemplo a seguir mostra uma entrada de AWS CloudTrail registro de uma GenerateDataKeyPairoperação para um enclave AWS 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 (para um enclave)

O exemplo a seguir mostra uma entrada de AWS CloudTrail registro de uma GenerateRandomoperação para um 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"
}
```

Como o Amazon Redshift usa o AWS KMS

Este tópico discute como o Amazon Redshift usa o AWS KMS para criptografar dados.

Tópicos

- Criptografia do Amazon Redshift
- Contexto de criptografia

Criptografia do Amazon Redshift

Um data warehouse do Amazon Redshift é um conjunto de recursos de computação chamados nós, que são organizados em um grupo chamado cluster. Cada cluster executa um mecanismo do Amazon Redshift e contém um ou mais bancos de dados.

O Amazon Redshift usa para criptografia uma arquitetura de quatro níveis baseada em chaves. A arquitetura consiste em chaves de criptografia dos dados, uma chave de banco de dados, uma chave de cluster e uma chave raiz. Você pode usar uma AWS KMS key como chave raiz.

As chaves de criptografia dos dados criptografam blocos de dados do cluster. Cada bloco de dados recebe uma chave AES-256 gerada aleatoriamente. Essas chaves são criptografadas com a chave do banco de dados do cluster.

A chave do banco de dados criptografa as chaves de criptografia dos dados do cluster. A chave do banco de dados é uma chave AES-256 gerada aleatoriamente. Ela é armazenada em disco em uma rede separada do cluster do Amazon Redshift e passada para o cluster por meio de um canal seguro.

A chave do cluster criptografa a chave do banco de dados do cluster do Amazon Redshift. Você pode usar o AWS KMS, o AWS CloudHSM ou um módulo de segurança de hardware (HSM) externo para gerenciar a chave do cluster. Para obter mais detalhes, consulte a documentação de Criptografia de banco de dados do Amazon Redshift .

Para solicitar criptografia, marque a caixa apropriada no console do Amazon Redshift. Para especificar uma chave gerenciada pelo cliente, escolha uma na lista que aparece abaixo da caixa de

criptografia. Se você não especificar uma chave gerenciada pelo cliente, o Amazon Redshift usará a Chave gerenciada pela AWS na sua conta.

> **Important**
>
> O Amazon Redshift só é compatível com chaves do KMS de criptografia simétrica. Não é possível usar uma chave do KMS assimétrica em um fluxo de trabalho de criptografia do Amazon Redshift. Para obter ajuda para determinar se uma chave do KMS é simétrica ou assimétrica, consulte Identificar chaves do KMS assimétricas.

Contexto de criptografia

Cada serviço que é integrado ao AWS KMS especifica um contexto de criptografia ao solicitar chaves de dados, criptografia e descriptografia. O contexto de criptografia é dados autenticados adicionais (AAD) que o AWS KMS usa para verificar a integridade dos dados. Ou seja, quando um contexto de criptografia é especificado para uma operação de criptografia, o serviço também o especifica para a operação de descriptografia ou a descriptografia não terá êxito. O Amazon RedShift usa o ID do cluster e a hora de criação no contexto de criptografia. No `requestParameters` campo de um arquivo de CloudTrail log, o contexto de criptografia será semelhante a este.

```
"encryptionContext": {
    "aws:redshift:arn": "arn:aws:redshift:region:account_ID:cluster:cluster_name",
    "aws:redshift:createtime": "20150206T1832Z"
},
```

Você pode pesquisar o nome do cluster em seus CloudTrail registros para entender quais operações foram realizadas usando uma AWS KMS key (chave KMS). As operações incluem a criptografia e descriptografia do cluster e a geração de chaves de dados.

Como o Amazon Relational Database Service (Amazon RDS) usa o AWS KMS

Você pode usar o Amazon Relational Database Service (Amazon RDS) para configurar, operar e escalar um banco de dados relacional na nuvem. Você pode criptografar os recursos do Amazon RDS usando uma Chave gerenciada pela AWS ou uma chave gerenciada pelo cliente. 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.

Para obter informações detalhadas sobre como o Amazon RDS usa chaves do KMS para proteger seus recursos, consulte Criptografar recursos do Amazon RDS e Gerenciamento de chaves do AWS KMS no Guia do usuário do Amazon RDS.

Como o AWS Secrets Manager usa o AWS KMS

AWS Secrets Manager é um serviço da AWS que criptografa e armazena seus segredos e, de forma transparente, descriptografa e os devolve para você em texto simples. Ele é projetado especialmente para armazenar segredos de aplicação, como credenciais de login, que mudam periodicamente e não devem ser codificados ou armazenados em texto simples na aplicação. Em vez de credenciais codificadas ou pesquisas de tabela, a aplicação chama o Secrets Manager.

O Secrets Manager também oferece suporte a recursos que periodicamente giram os segredos associados aos bancos de dados usados com mais frequência. Ele sempre criptografa os segredos que acabaram de ser alternados antes de serem armazenados.

O Secrets Manager um valor de tag integra-se ao AWS Key Management Service (AWS KMS) para criptografar cada versão de cada segredo com uma chave de dados exclusiva protegida por uma AWS KMS key. Essa integração protege seus segredos em chaves de criptografia que nunca saem do AWS KMS sem estarem criptografadas. Ela também permite que você defina permissões personalizadas na chave do KMS e audite as operações que geram, criptografam e descriptografam as chaves de dados que protegem seus segredos.

Para obter informações sobre como o Secrets Manager usa chaves do KMS para proteger seus segredos, consulte Criptografar e descriptografar segredos, noManual do usuário do AWS Secrets Manager.

Como o Amazon Simple Email Service (Amazon SES) usa o AWS KMS

Você pode usar o Amazon Simple Email Service (Amazon SES) para receber e-mails e (opcionalmente) para criptografar as mensagens de e-email recebidas antes de armazená-las em um bucket do Amazon Simple Storage Service (Amazon S3) de sua escolha. Ao configurar o Amazon SES para criptografar mensagens de e-mail, você deve escolher a AWS KMS key do AWS KMS com a qual o Amazon SES criptografa as mensagens. É possível escolher a Chave gerenciada pela AWS

para o Amazon SES (seu alias é `aws/ses`), ou você pode escolher uma chave simétrica gerenciada pelo cliente criada no AWS KMS.

> **Important**
>
> O Amazon SES oferece suporte somente para chaves simétricas do KMS. Não é possível usar uma chave do KMS assimétrica para criptografar mensagens de e-mail do Amazon SES. Para obter ajuda para determinar se uma chave do KMS é simétrica ou assimétrica, consulte Identificar chaves do KMS assimétricas.

Para obter mais informações sobre o recebimento de e-mails usando o Amazon SES, acesse Receber e-mails no Amazon SES, no Guia do desenvolvedor do Amazon Simple Email Service.

Tópicos

- Visão geral da criptografia do Amazon SES usando o AWS KMS
- Contexto de criptografia do Amazon SES
- Conceder permissão ao Amazon SES para usar sua AWS KMS key
- Obter e descriptografar mensagens de e-mail

Visão geral da criptografia do Amazon SES usando o AWS KMS

Quando você configura o Amazon SES para receber e-mail e criptografar as mensagens de e-mail antes de salvá-las em seu bucket do S3, o processo funciona da seguinte forma:

1. Você cria uma regra de recebimento para o Amazon SES, especificando a ação do S3, um bucket do S3 para armazenamento e uma AWS KMS key para criptografia.
2. O Amazon SES recebe uma mensagem de e-mail que está em conformidade com a sua regra de recebimento.
3. O Amazon SES solicita uma chave de dados exclusiva criptografada com a chave do KMS que você especificou na regra de recebimento aplicável.
4. O AWS KMS cria uma nova chave de dados, criptografa-a com a chave do KMS especificada e envia as cópias de texto criptografado e não criptografado da chave de dados ao Amazon SES.
5. O Amazon SES usa a chave de dados de texto não criptografado para criptografar a mensagem de e-mail e remove a chave de dados de texto não criptografado da memória, assim que possível, após o uso.

6. O Amazon SES coloca a mensagem de e-mail criptografada e a chave de dados criptografada no bucket do S3 especificado. A chave de dados criptografada é armazenada como metadados com a mensagem de e-email criptografada.

Para realizar Step 3 por meio de Step 6, o Amazon SES usa o cliente de criptografia do Amazon S3 fornecido pelo AWS. Use o mesmo cliente para recuperar suas mensagens de e-mail criptografadas do Amazon S3 e as descriptografe. Para obter mais informações, consulte Obter e descriptografar mensagens de e-mail.

Contexto de criptografia do Amazon SES

Quando o Amazon SES solicita que uma chave de dados criptografe suas mensagens de e-mail recebidas (Step 3 no Visão geral da criptografia do Amazon SES usando o AWS KMS), ele inclui um contexto de criptografia na solicitação. O contexto de criptografia fornece dados autenticados adicionais (AAD) que o AWS KMS usa para garantir a integridade dos dados. O contexto de criptografia também é gravado em seus arquivos de log do AWS CloudTrail, o que pode ajudar você a entender por que uma determinada AWS KMS key (chave do KMS) foi usada. O Amazon SES usa o seguinte como contexto de criptografia:

- O ID da Conta da AWS na qual você configurou o Amazon SES para receber mensagens de e-mail
- O nome da regra do Amazon SES que invocou a ação do S3 na mensagem de e-mail
- O ID da mensagem do Amazon SES para a mensagem de e-mail

O exemplo a seguir mostra uma representação JSON do contexto de criptografia usado pelo Amazon SES:

```
{
  "aws:ses:source-account": "111122223333",
  "aws:ses:rule-name": "example-receipt-rule-name",
  "aws:ses:message-id": "d6iitobk75ur44p8kdnnp7g2n800"
}
```

Conceder permissão ao Amazon SES para usar sua AWS KMS key

Para criptografar suas mensagens de e-mail, você pode usar a Chave gerenciada pela AWS na sua conta para o Amazon SES (`aws/ses`) ou pode usar uma chave gerenciada pelo cliente criada por

você. O Amazon SES já tem permissão para usar a Chave gerenciada pela AWS em seu nome. No entanto, se você especificar uma chave gerenciada pelo cliente ao adicionar a ação do S3 à sua regra de recebimento do Amazon SES, será necessário conceder permissão ao Amazon SES para usar a chave do KMS com o objetivo de criptografar suas mensagens de e-mail.

Para conceder ao Amazon SES permissão para usar a sua chave gerenciada pelo cliente, adicione a seguinte instrução à política de chaves dessa chave do 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"}
  }
}
```

Substitua *ACCOUNT-ID-WITHOUT-HYPHENS* pelo ID de 12 dígitos da Conta da AWS na qual você configurou o Amazon SES para receber mensagens de e-mail. Essa instrução de política permite que o Amazon SES criptografe os dados com essa chave do KMS somente sob estas condições:

- O Amazon SES deve especificar `aws:ses:rule-name` e `aws:ses:message-id` no `EncryptionContext` de suas solicitações da API do AWS KMS.
- O Amazon SES deve especificar `EncryptionContext` no AWS KMS das solicitações de API do `aws:ses:source-account`, e o valor de Conta da AWS deve corresponder ao ID da `aws:ses:source-account` especificado na política de chaves.

Para obter mais informações sobre o contexto de criptografia usado pelo Amazon SES ao criptografar suas mensagens de e-mail, consulte Contexto de criptografia do Amazon SES. Para

obter informações gerais sobre como o AWS KMS usa o contexto de criptografia, consulte contexto de criptografia.

Obter e descriptografar mensagens de e-mail

O Amazon SES não tem permissão para descriptografar suas mensagens de e-mail criptografadas e não pode descriptografá-las para você. Você deve escrever o código para obter suas mensagens de e-mail do Amazon S3 e descriptografá-las. Para tornar isso mais fácil, use o cliente de criptografia do Amazon S3. Os AWS SDKs a seguir incluem o cliente de criptografia do Amazon S3:

- AWS SDK for Java – Consulte AmazonS3EncryptionClient e AmazonS3EncryptionClientV2 na Referência de APIs do AWS SDK for Java.
- AWS SDK for Ruby – Consulte Aws::S3::Encryption::Client na Referência de APIs do AWS SDK for Ruby.
- AWS SDK for .NET – Consulte AmazonS3EncryptionClient na Referência de APIs do AWS SDK for .NET.
- AWS SDK for Go – Consulte s3crypto na Referência de APIs do AWS SDK for Go.

O cliente de criptografia do Amazon S3 simplifica o trabalho de construção das solicitações necessárias para o Amazon S3 recuperar a mensagem de e-mail criptografada e o AWS KMS descriptografar a chave de dados criptografada da mensagem, e descriptografar a mensagem de e-mail. Por exemplo, para descriptografar com êxito a chave de dados criptografada, você deve passar o mesmo contexto de criptografia que o Amazon SES passou ao solicitar a chave de dados do AWS KMS (Step 3 na Visão geral da criptografia do Amazon SES usando o AWS KMS). O cliente de criptografia do Amazon S3 lida com isso, e muito mais das outras tarefas, para você.

Para o código de exemplo que usa o cliente de criptografia do Amazon S3 no AWS SDK for Java para fazer a descriptografia do lado do cliente, consulte o seguinte:

- Uso de uma chave do KMS armazenada no AWS KMS no Guia do usuário do Amazon Simple Storage Service.
- Criptografia do Amazon S3 com o AWS Key Management Service no blog de desenvolvedores da AWS.

Como o Amazon Simple Storage Service (Amazon S3) usa o AWS KMS

O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos que armazena dados como objetos em buckets. Os buckets e os objetos neles são privados e poderão ser acessados somente se você conceder explicitamente permissões de acesso.

O Amazon S3 integra-se ao AWS Key Management Service (AWS KMS) para fornecer criptografia no lado do servidor de objetos do Amazon S3. O Amazon S3 usa chaves do AWS KMS para criptografar seus objetos do Amazon S3. As chaves de criptografia que protegem seus objetos nunca saem do AWS KMS sem criptografia. Essa integração também permite que você defina permissões na chave do AWS KMS e audite as operações que geram, criptografam e descriptografam as chaves de dados que protegem seus segredos.

Para reduzir o volume de chamadas do Amazon S3 paraAWS KMS, use as chaves de bucket do Amazon S3, que são key-encryption-keys protegidas por chave KMS e reutilizadas por um tempo limitado no Amazon S3. Chaves de bucket podem AWS KMS reduzir os custos de solicitações do em até 99%. É possível configurar uma chave de bucket para todos os objetos em um bucket do Amazon S3 ou para um determinado objeto em um bucket do Amazon S3.

Para obter mais informações sobre como o Amazon S3 usa AWS KMS, consulte Proteger dados usando criptografia do lado do servidor com chaves do KMS (SSE-KMS) no Guia do usuário do Amazon S3.

Como o AWS Systems Manager Parameter Store usa o AWS KMS

Com o AWS Systems Manager Parameter Store, você pode criar parâmetros de string segura, que são parâmetros com um nome de parâmetro em texto simples e um valor de parâmetro criptografado. O Parameter Store usa o AWS KMS para criptografar e descriptografar os valores de parâmetros de parâmetros de string segura.

Com o Parameter Store, você pode criar, armazenar e gerenciar dados como parâmetros com valores. Você pode criar um parâmetro no Parameter Store e usá-lo em várias aplicações e serviços, de acordo com as políticas e as permissões que você define. Quando precisa alterar um valor de parâmetro, você altera uma instância, em vez de gerenciar uma alteração passível de erros em várias origens. O Parameter Store é compatível com uma estrutura hierárquica para nomes de parâmetros, de modo que você pode qualificar um parâmetro para usos específicos.

Para gerenciar dados confidenciais, crie parâmetros de string segura. O Parameter Store usa chaves do AWS KMS keys para criptografar os valores de parâmetros de string segura quando você os cria ou altera. Ele também usa chaves do KMS para descriptografar os valores do parâmetro quando você os acessa. Você pode usar a Chave gerenciada pela AWS criada pelo Parameter Store para sua conta ou especificar sua própria chave gerenciada pelo cliente.

> **Important**
>
> O Parameter Store apenas é compatível com chaves do KMS simétricas. Não é possível usar uma chave do KMS assimétrica para criptografar os parâmetros. Para obter ajuda para determinar se uma chave do KMS é simétrica ou assimétrica, consulte Identificar chaves do KMS assimétricas.

O repositório de parâmetros oferece suporte a dois níveis de parâmetros de string segura: padrão e avançado. Parâmetros padrão, que não podem exceder 4.096 bytes, são criptografados e descriptografados diretamente na chave do KMS especificada. Para criptografar e descriptografar parâmetros de string segura avançados, o Parameter Store usa a criptografia de envelope com o AWS Encryption SDK. Você pode converter um parâmetro de string segura padrão em um parâmetro avançado, mas não pode converter um parâmetro avançado em um padrão. Para obter mais informações sobre a diferença entre parâmetros de string segura padrão e avançados, consulte Sobre parâmetros avançados do Systems Manager, no Manual do usuário do AWS Systems Manager.

Tópicos

- Proteger parâmetros de string segura padrão
- Proteger parâmetros de string segura avançados
- Definir permissões para criptografar e descriptografar valores de parâmetro
- Contexto de criptografia do Parameter Store
- Solução de problemas com chaves do KMS no Parameter Store

Proteger parâmetros de string segura padrão

O Parameter Store não executa operações de criptografia. Em vez disso, ele se baseia no AWS KMS para criptografar e descriptografar valores de parâmetros de string segura. Quando você cria ou altera um valor de parâmetro de string segura padrão, o Parameter Store chama a operação do

AWS KMS Encrypt. Essa operação usa uma chave do KMS de criptografia simétrica diretamente para criptografar o valor do parâmetro em vez de usar a chave do KMS para gerar uma chave de dados.

Você pode selecionar a chave do KMS que o Parameter Store usa para criptografar o valor de parâmetro. Se você não especificar uma chave do KMS, o Parameter Store usará a Chave gerenciada pela AWS que o Systems Manager cria automaticamente na sua conta. Essa chave do KMS tem o alias `aws/ssm`.

Para ver a chave `aws/ssm` KMS padrão da sua conta, use a DescribeKeyoperação na AWS KMS API. O exemplo a seguir usa o comando `describe-key` na AWS Command Line Interface (AWS CLI) com o nome de alias `aws/ssm`.

```
aws kms describe-key --key-id alias/aws/ssm
```

Para criar um parâmetro de string seguro padrão, use a PutParameteroperação na API Systems Manager. Omita o parâmetro de `Tier` ou especifique um valor de `Standard`, que é o padrão. Inclua um parâmetro `Type` com um valor de `SecureString`. Para especificar uma chave do KMS, use o parâmetro `KeyId`. O padrão é a Chave gerenciada pela AWS para sua conta, `aws/ssm`.

Depois, o Parameter Store chama a operação `Encrypt` do AWS KMS com a chave do KMS e o valor do parâmetro em texto simples. O AWS KMS retorna o valor do parâmetro criptografado, que o Parameter Store armazena com o nome do parâmetro.

O exemplo a seguir usa o comando put-parameter do Systems Manager e seu parâmetro `--type` na AWS CLI para criar um parâmetro de string segura. Como o comando omite os parâmetros `--tier` e `--key-id` opcionais, o Parameter Store cria um parâmetro de string segura padrão e o criptografa com a Chave gerenciada pela AWS

```
aws ssm put-parameter --name MyParameter --value "secret_value" --type SecureString
```

O exemplo semelhante a seguir usa o parâmetro `--key-id` para especificar uma chave gerenciada pelo cliente. O exemplo usa um ID de chave do KMS para identificar a chave do KMS, mas você pode usar qualquer identificador de chave do KMS válido. Como o comando omite o parâmetro `Tier` (`--tier`), o cria um parâmetro de string segura padrão, e não um avançado.

```
aws ssm put-parameter --name param1 --value "secret" --type SecureString --key-id
 1234abcd-12ab-34cd-56ef-1234567890ab
```

Quando você obtém um parâmetro de string segura do Parameter Store, seu valor está criptografado. Para obter um parâmetro, use a GetParameter operação na API Systems Manager.

O exemplo a seguir usa o comando get-parameter do Systems Manager na AWS CLI para obter o parâmetro `MyParameter` no Parameter Store sem descriptografar seu valor.

```
$  aws ssm get-parameter --name MyParameter

{
    "Parameter": {
        "Type": "SecureString",
        "Name": "MyParameter",
        "Value":
 "AQECAHgnOkMROh5LaLXkA4j0+vYi6tmM17Lg/9E464VRo68cvwAAAG8wbQYJKoZIhvcNAQcGoGAwXgIBADBZBgkqhkiG9
    }
}
```

Para descriptografar o valor de parâmetro antes de retorná-lo, defina o parâmetro `WithDecryption` de `GetParameter` como `true`. Quando você usa `WithDecryption`, o Parameter Store chama a operação do AWS KMS Decrypt em seu nome para descriptografar o valor de parâmetro. Como resultado, a solicitação de `GetParameter` retorna o parâmetro com um valor de parâmetro de texto simples, como mostrado no exemplo a seguir.

```
$  aws ssm get-parameter --name MyParameter --with-decryption

{
    "Parameter": {
        "Type": "SecureString",
        "Name": "MyParameter",
        "Value": "secret_value"
    }
}
```

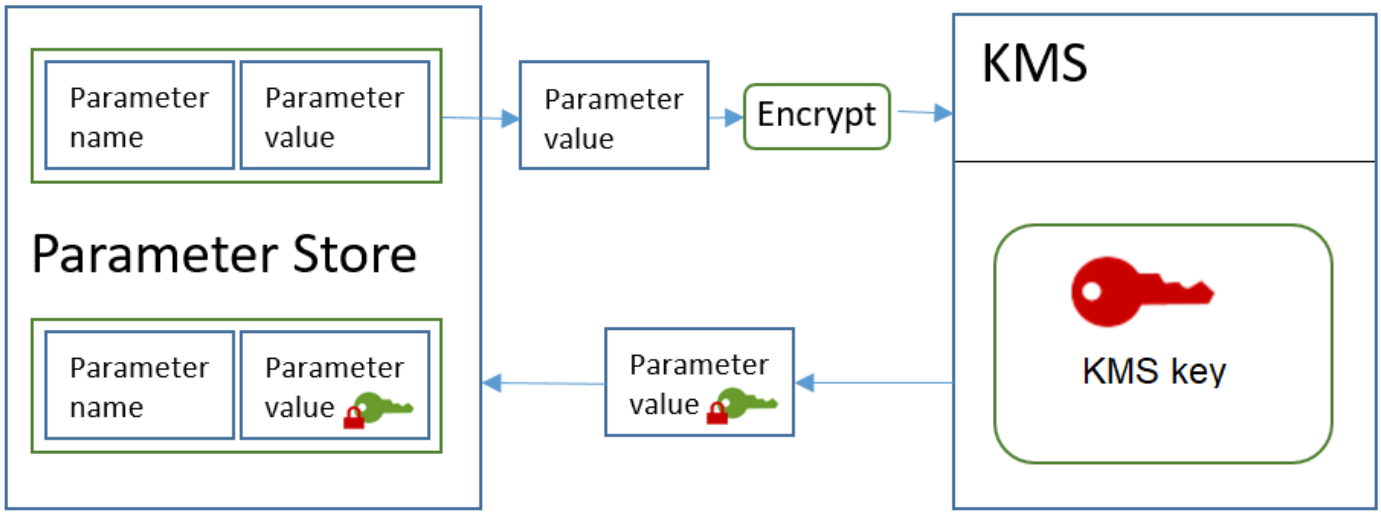
O fluxo de trabalho a seguir mostra como o Parameter Store usa uma chave do KMS para criptografar e descriptografar um parâmetro de string segura padrão.

Criptografar um parâmetro padrão

1. Quando você usa `PutParameter` para criar um parâmetro de string segura, o Parameter Store envia uma solicitação `Encrypt` ao AWS KMS. Essa solicitação inclui o valor do parâmetro em

texto simples e a chave do KMS que você escolheu e o contexto de criptografia do Parameter Store. Durante a transmissão ao AWS KMS, o valor em texto não criptografado no parâmetro de string segura é protegido pelo Transport Layer Security (TLS).

2. O AWS KMS criptografa o valor de parâmetro com a chave do KMS especificada e o contexto de criptografia. Ele retorna o texto cifrado ao Parameter Store, que armazena o nome de parâmetro e seu valor criptografado.



Descriptografar um parâmetro padrão

1. Quando você inclui o parâmetro `WithDecryption` em uma solicitação `GetParameter`, o Parameter Store envia uma solicitação `Decrypt` ao AWS KMS com o valor do parâmetro de string segura e o contexto de criptografia do Parameter Store.
2. O AWS KMS usa a mesma chave do KMS e o contexto de criptografia fornecido para descriptografar o valor criptografado. Ele retorna o valor do parâmetro em texto simples (descriptografado) ao Parameter Store. Durante a transmissão, os dados em texto simples são protegidos por TLS.
3. O Parameter Store retorna o valor do parâmetro em texto simples na resposta de `GetParameter`.

Proteger parâmetros de string segura avançados

Quando você usa `PutParameter` para criar um parâmetro de string segura avançado, o Parameter Store usa criptografia de envelope com o AWS Encryption SDK e uma AWS KMS key de criptografia simétrica para proteger o valor do parâmetro. Cada valor de parâmetro avançado é criptografado com uma chave de dados exclusiva, e a chave de dados é criptografada em uma chave do KMS. É

possível usar a Chave gerenciada pela AWS para a conta (`aws/ssm`) ou qualquer chave gerenciada pelo cliente.

O AWS Encryption SDK é uma biblioteca no lado do cliente de software livre que ajuda você a criptografar e descriptografar dados usando padrões do setor e práticas recomendadas. Ele é compatível com várias plataformas e várias linguagens de programação, incluindo uma interface de linha de comando. Você pode visualizar o código-fonte e contribuir para seu desenvolvimento em GitHub.

Para cada valor de parâmetro de cadeia de caracteres segura, o Parameter Store chama o AWS Encryption SDK para criptografar o valor do parâmetro usando uma chave de dados exclusiva que AWS KMS gera (GenerateDataKey). O AWS Encryption SDK retorna ao Parameter Store uma mensagem criptografada que inclui o valor de parâmetro criptografado e uma cópia criptografada da chave de dados exclusiva. O Parameter Store armazena toda a mensagem criptografada no valor do parâmetro de string segura. Quando você obtém um parâmetro de string segura avançado, o Parameter Store usa o AWS Encryption SDK para descriptografar o valor do parâmetro. Isso requer uma chamada para o AWS KMS descriptografar a chave de dados criptografada.

Para criar um parâmetro de string seguro avançado, use a PutParameteroperação na API Systems Manager. Defina o valor do parâmetro `Tier` como `Advanced`. Inclua um parâmetro `Type` com um valor de `SecureString`. Para especificar uma chave do KMS, use o parâmetro `KeyId`. O padrão é a Chave gerenciada pela AWS para sua conta, `aws/ssm`.

```
aws ssm put-parameter --name MyParameter --value "secret_value" --type SecureString --
tier Advanced
```

O exemplo semelhante a seguir usa o parâmetro `--key-id` para especificar uma chave gerenciada pelo cliente. O exemplo usa o Amazon Resource Name (ARN) da chave do KMS, mas você pode usar qualquer identificador válido de chave do KMS.

```
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 você obtém um parâmetro de string segura do Parameter Store, seu valor é a mensagem criptografada que é retornado pelo AWS Encryption SDK. Para obter um parâmetro, use a GetParameter operação na API Systems Manager.

O exemplo a seguir usa a operação `GetParameter` do Systems Manager para obter o parâmetro `MyParameter` no Parameter Store sem descriptografar seu valor.

```
$  aws ssm get-parameter --name MyParameter

{
    "Parameter": {
        "Type": "SecureString",
        "Name": "MyParameter",
        "Value":
 "AQECAHgnOkMROh5LaLXkA4j0+vYi6tmM17Lg/9E464VRo68cvwAAAG8wbQYJKoZIhvcNAQcGoGAwXgIBADBZBgkqhkiG9
    }
}
```

Para descriptografar o valor de parâmetro antes de retorná-lo, defina o parâmetro `WithDecryption` de `GetParameter` como `true`. Quando você usa `WithDecryption`, o Parameter Store chama a operação do AWS KMS Decrypt em seu nome para descriptografar o valor de parâmetro. Como resultado, a solicitação de `GetParameter` retorna o parâmetro com um valor de parâmetro de texto simples, como mostrado no exemplo a seguir.

```
$  aws ssm get-parameter --name MyParameter --with-decryption

{
    "Parameter": {
        "Type": "SecureString",
        "Name": "MyParameter",
        "Value": "secret_value"
    }
}
```

Você não pode converter um parâmetro de string segura avançado em um padrão, mas pode converter uma string segura padrão em uma avançada. Para converter um parâmetro de string segura padrão em uma string segura avançada, use a operação `PutParameter` com o parâmetro `Overwrite`. O `Type` deve ser `SecureString`, e o valor `Tier` deve ser `Advanced`. O parâmetro `KeyId`, que identifica uma chave gerenciada pelo cliente, é opcional. Se você omiti-lo, o Parameter Store usará a Chave gerenciada pela AWS da conta. É possível especificar qualquer chave do KMS que a entidade principal tenha permissão para usar, mesmo se você tiver usado uma chave do KMS diferente para criptografar o parâmetro padrão.

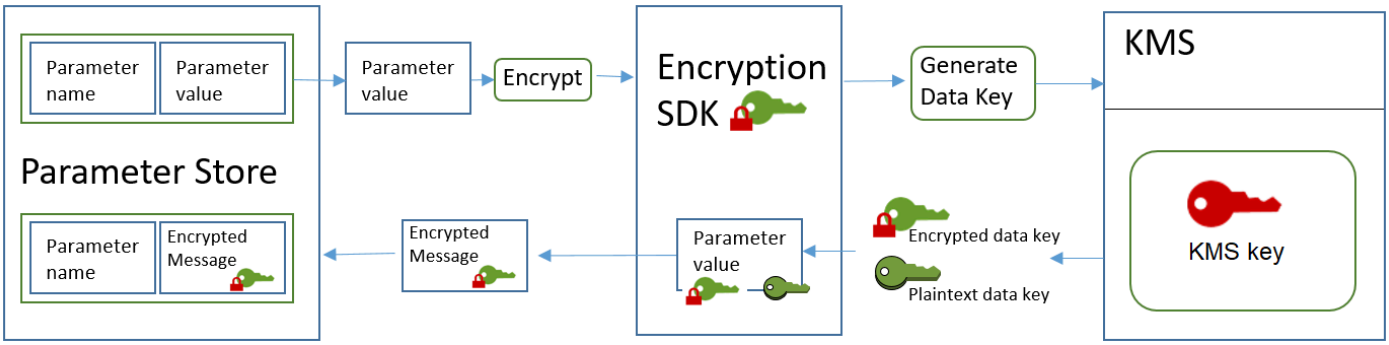
Quando você usa o parâmetro `Overwrite`, o Parameter Store usa o AWS Encryption SDK para criptografar o valor do parâmetro. Ele armazena a mensagem recém-criptografada no Parameter Store.

```
$ aws ssm put-parameter --name myStdParameter --value "secret_value"  --type
 SecureString --tier Advanced --key-id 1234abcd-12ab-34cd-56ef-1234567890ab --overwrite
```

O fluxo de trabalho a seguir mostra como o Parameter Store usa uma chave do KMS para criptografar e descriptografar um parâmetro de string segura avançado.

Criptografar um parâmetro avançado

1. Quando você usa o `PutParameter` para criar um parâmetro de string segura avançado, o Parameter Store usa o AWS Encryption SDK e o AWS KMS para criptografar o valor do parâmetro. O Parameter Store chama o AWS Encryption SDK com o valor do parâmetro, a chave do KMS que você especificou e a contexto de criptografia do Parameter Store.
2. O AWS Encryption SDK envia uma GenerateDataKeysolicitação AWS KMS com o identificador da chave KMS que você especificou e o contexto de criptografia do Parameter Store. AWS KMSretorna duas cópias da chave de dados exclusiva: uma em texto simples e outra criptografada sob a chave KMS. (O contexto de criptografia é usado ao criptografar a chave de dados.)
3. O AWS Encryption SDK usa a chave de dados em texto simples para criptografar valor de parâmetro. Ele retorna uma mensagem criptografada que inclui o valor do parâmetro criptografado, a chave de dados criptografada e outros dados, incluindo o contexto criptografia do Parameter Store.
4. O Parameter Store armazena a mensagem criptografada como o valor do parâmetro.



Descriptografar um parâmetro avançado

1. Você pode incluir o parâmetro `WithDecryption` em uma solicitação `GetParameter` para obter um parâmetro de string segura avançado. Quando você fizer isso, o Parameter Store repassará a mensagem criptografada do valor de parâmetro para um método de descriptografia do AWS Encryption SDK.
2. O AWS Encryption SDK chama a operação do AWS KMS Decrypt. Ele repassa a chave de dados criptografada e o contexto de criptografia do Parameter Store da mensagem criptografada.
3. O AWS KMS usa a chave do KMS e o contexto de criptografia do Parameter Store para descriptografar a chave de dados criptografada. Ele retorna a chave de dados de texto simples (descriptografada) ao AWS Encryption SDK.
4. O AWS Encryption SDK usa a chave de dados de texto simples para descriptografar o valor de parâmetro. Ele retorna o valor do parâmetro em texto simples ao Parameter Store.
5. O Parameter Store verifica o contexto de criptografia e retorna a você o valor de parâmetro em texto simples na resposta `GetParameter`.

Definir permissões para criptografar e descriptografar valores de parâmetro

Para criptografar um valor de parâmetro de string segura padrão, o usuário precisa da permissão `kms:Encrypt`. Para criptografar um valor de parâmetro de string segura avançado, o usuário precisa da permissão `kms:GenerateDataKey`. Para descriptografar qualquer tipo de valor de parâmetro de string segura, o usuário precisa da permissão `kms:Decrypt`.

Você pode usar políticas do IAM para permitir ou negar permissão para um usuário chamar as operações `PutParameter` e `GetParameter` do Systems Manager.

Além disso, se estiver usando chaves gerenciadas pelo cliente para criptografar seus valores de parâmetro de string segura, você poderá usar políticas do IAM e políticas de chaves para criptografar e descriptografar permissões. No entanto, você não pode estabelecer políticas de controle de acesso para a chave do KMS `aws/ssm` padrão. Para obter informações detalhadas sobre o como controlar o acesso a chaves gerenciadas pelo cliente, consulte Autenticação e controle de acesso para o AWS KMS.

O exemplo a seguir mostra uma política do IAM criada para parâmetros de string padrão. Ela permite que o usuário chame a operação `PutParameter` do Systems Manager em todos os parâmetros no caminho `FinancialParameters`. A política também permite que o usuário chame a operação do AWS KMS `Encrypt` em um exemplo de chave gerenciada pelo cliente.

```
{
    "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"
        }
    ]
}
```

O exemplo a seguir mostra uma política do IAM criada para parâmetros de string segura avançados. Ela permite que o usuário chame a operação `PutParameter` do Systems Manager em todos os parâmetros no caminho `ReservedParameters`. A política também permite que o usuário chame a operação do AWS KMS `GenerateDataKey` em um exemplo de chave gerenciada pelo cliente.

```
{
    "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"
        }
    ]
}
```

O último exemplo também mostra uma política do IAM que pode ser usada para parâmetros de string segura padrão ou avançados. Ela permite que o usuário chame as operações `GetParameter` do Systems Manager (e operações relacionadas) em todos os parâmetros no caminho de `ITParameters`. A política também permite que o usuário chame a operação do AWS KMS `Decrypt` em um exemplo de chave gerenciada pelo cliente.

```
{
    "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"
        }
    ]
}
```

Contexto de criptografia do Parameter Store

Um contexto de criptografia é um conjunto de pares de chave-valor que contêm dados arbitrários não secretos. Quando você inclui um contexto de criptografia em uma solicitação para criptografar dados, o AWS KMS vincula de forma criptográfica o contexto de criptografia aos dados criptografados. Para descriptografar os dados, você deve passar o mesmo contexto de criptografia.

Você também pode usar o contexto de criptografia para identificar uma operação de criptografia em registros de auditoria e logs. O contexto de criptografia aparece em texto simples em logs, como logs do AWS CloudTrail.

O AWS Encryption SDK também obtém um contexto de criptografia, embora lide com ele de maneira diferente. O Parameter Store fornece o contexto de criptografia para o método de criptografia. O AWS Encryption SDK vincula forma criptográfica o contexto de criptografia aos dados criptografados. Isso inclui o contexto de criptografia em texto simples no cabeçalho da mensagem criptografada retornada por ele. No entanto, ao contrário do AWS KMS, os métodos de descriptografia do AWS Encryption SDK não têm um contexto de criptografia como entrada. Em vez disso, quando ele descriptografa dados, o AWS Encryption SDKobtém o contexto de criptografia na mensagem criptografada. O Parameter Store verifica se o contexto de criptografia inclui o valor que ele espera antes de retornar o valor do parâmetro em texto simples para você.

O Parameter Store usa o seguinte contexto de criptografia em suas operações de criptografia:

- Chave: `PARAMETER_ARN`
- Valor: O Amazon Resource Name (ARN) do parâmetro que está sendo criptografado.

O formato do contexto de criptografia é o seguinte:

```
"PARAMETER_ARN":"arn:aws:ssm:<REGION_NAME>:<ACCOUNT_ID>:parameter/<parameter-name>"
```

Por exemplo, o Parameter Store inclui esse contexto de criptografia em chamadas para criptografar e descriptografar o parâmetro `MyParameter` em um exemplo de Conta da AWS e região.

```
"PARAMETER_ARN":"arn:aws:ssm:us-west-2:111122223333:parameter/MyParameter"
```

Se o parâmetro estiver em um caminho hierárquico do Parameter Store, o caminho e o nome são incluídos no contexto de criptografia. Por exemplo, esse contexto de criptografia é usado ao criptografar ou descriptografar o parâmetro `MyParameter` no caminho `/ReadableParameters` em um exemplo de Conta da AWS e região.

```
"PARAMETER_ARN":"arn:aws:ssm:us-west-2:111122223333:parameter/ReadableParameters/
MyParameter"
```

Você pode descriptografar um valor de parâmetro de string segura criptografado chamando a operação `Decrypt` do AWS KMS com o contexto de criptografia correto e o valor do parâmetro

criptografado que a operação `GetParameter` do Systems Manager retorna. No entanto, recomendamos que você descriptografe valores de parâmetros do Parameter Store usando a operação `GetParameter` com o parâmetro `WithDecryption`.

Você também pode incluir o contexto de criptografia em uma política do IAM. Por exemplo, você pode permitir que um usuário descriptografe apenas determinado valor de parâmetro ou conjunto de valores de parâmetro.

O exemplo a seguir de declaração de política do IAM permite que o usuário obtenha o valor do parâmetro `MyParameter` e descriptografe o valor usando a chave do KMS especificada. No entanto, as permissões são aplicáveis somente quando o contexto de criptografia corresponde à string especificada. Essas permissões não são aplicáveis a nenhum outro parâmetro ou chave do KMS, e ocorrerá falha na chamada para `GetParameter` se o contexto de criptografia não corresponder à string.

Antes de usar uma declaração de política como essa, substitua os ARNs de exemplo por valores válidos.

```
{
    "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"
                }
            }
        }
```

```
    ]
}
```

Solução de problemas com chaves do KMS no Parameter Store

Para executar qualquer operação em um parâmetro de string segura, o Parameter Store deve ser capaz de usar a chave do KMS do AWS KMS que você especifica para a operação desejada. A maioria das falhas do Parameter Store relacionadas a chaves do KMS é causada pelos seguintes problemas:

- As credenciais que uma aplicação está usando não têm permissão para executar a ação especificada na chave do KMS.

  Para corrigir este erro, execute a aplicação com credenciais diferentes ou revise a política da IAM ou de chaves que está impedindo a operação. Para obter ajuda com políticas do IAM e chaves do AWS KMS, consulte Autenticação e controle de acesso para o AWS KMS.
- A chave do KMS não foi encontrada.

  Isso geralmente acontece quando você usa um identificador incorreto para a chave do KMS. Encontre os identificadores corretos para a chave do KMS e tente o comando novamente.
- A chave do KMS não está habilitada. Quando isso ocorre, o Parameter Store retorna uma InvalidKeyIdexceção com uma mensagem de erro detalhada deAWS KMS. Se o estado da chave do KMS for `Disabled`, habilite-a. Se for `Pending Import`, conclua o procedimento de importação. Se o estado da chave for `Pending Deletion`, cancele a exclusão da chave ou use uma chave do KMS diferente.

  Para encontrar o estado de chave de uma chave do KMS no console do AWS KMS, na página Customer managed keys (Chaves gerenciadas pelo cliente) ou Chaves gerenciadas pela AWS, consulte a coluna Status. Para usar a AWS KMS API para encontrar o status de uma chave KMS, use a DescribeKeyoperação.

Como a Amazon WorkMail usa AWS KMS

Este tópico discute como a Amazon WorkMail usa AWS KMS para criptografar mensagens de e-mail.

Tópicos

- WorkMail Visão geral da Amazon

- WorkMail Criptografia da Amazon
- Autorizar o uso da chave do KMS
- Contexto WorkMail de criptografia da Amazon
- Monitorando a WorkMail interação da Amazon com AWS KMS

WorkMail Visão geral da Amazon

WorkMailA Amazon é um serviço de e-mail e calendário comercial seguro e gerenciado com suporte para clientes de e-mail móveis e desktop existentes. Você pode criar uma WorkMail organização da Amazon e atribuir a ela um ou mais domínios de e-mail de sua propriedade. Você pode criar caixas de correio para os usuários e grupos de distribuição de e-mail na organização.

A Amazon criptografa de WorkMail forma transparente todas as mensagens nas caixas de correio de todas as WorkMail organizações da Amazon antes que as mensagens sejam gravadas em disco e as descriptografa de forma transparente quando os usuários as acessam. Não há nenhuma opção para desabilitar a criptografia. Para proteger as chaves de criptografia que protegem as mensagens, a Amazon WorkMail está integrada com AWS Key Management Service (AWS KMS).

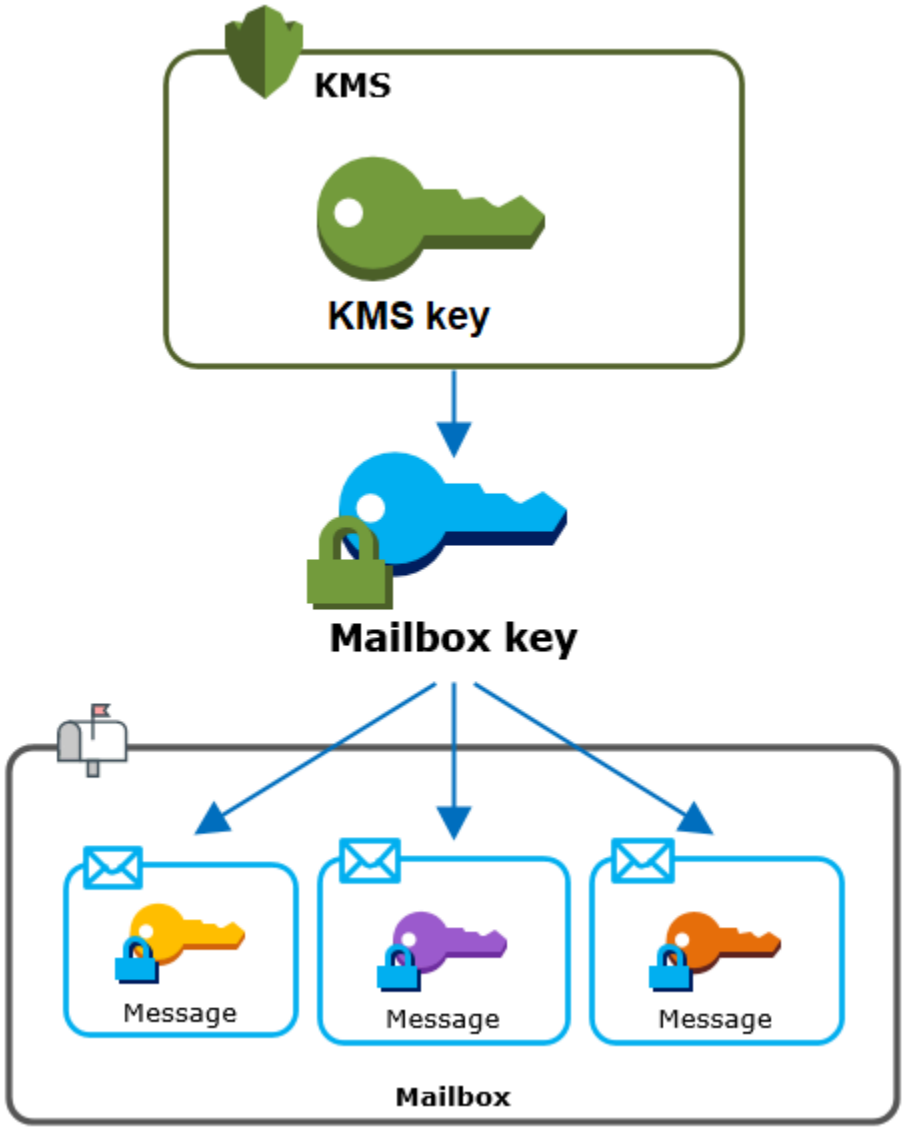
A Amazon WorkMail também oferece uma opção para permitir que os usuários enviem e-mails assinados ou criptografados. Este recurso de criptografia não usa o AWS KMS.

WorkMail Criptografia da Amazon

Na Amazon WorkMail, cada organização pode conter várias caixas de correio, uma para cada usuário na organização. Todas as mensagens, incluindo e-mail, calendário e itens são armazenados na caixa de correio do usuário.

Para proteger o conteúdo das caixas de correio em suas WorkMail organizações da Amazon, a Amazon WorkMail criptografa todas as mensagens da caixa de correio antes de serem gravadas no disco. Nenhuma informação fornecidas pelo cliente é armazenada em texto simples.

Cada mensagem é criptografada em uma chave de criptografia dos dados exclusiva. A chave da mensagem é protegida por uma chave de caixa de correio, que é uma chave exclusiva usada apenas para essa caixa de correio. A chave de caixa de correio é criptografada em uma AWS KMS key para a organização que nunca deixa o AWS KMS em estado sem criptografia. O diagrama a seguir mostra a relação das mensagens criptografadas, das chaves de mensagens criptografadas, da chave de caixa de correio criptografada e da chave do KMS para a organização no AWS KMS.



Uma chave do KMS para a organização

Ao criar uma WorkMail organização da Amazon, você pode selecionar uma AWS KMS key para a organização. Essa chave do KMS protege todas as chaves de caixa de correio nessa organização.

Se você usar o procedimento de configuração rápida para criar sua organização, a Amazon WorkMail usará o Chave gerenciada pela AWSfor Amazon WorkMail (`aws/workmail`) em seuConta da AWS. Se você usar a Configuração padrão, poderá selecionar a chave Chave gerenciada pela AWS para a Amazon WorkMail ou uma chave gerenciada pelo cliente que você possui e gerencia. É possível selecionar a mesma chave do KMS ou uma chave do KMS diferente para cada uma das suas organizações, mas não é possível alterar a chave do KMS depois de selecioná-la.

> **Important**
>
> A Amazon WorkMail suporta somente chaves KMS de criptografia simétrica. Você não pode usar uma chave KMS assimétrica para criptografar dados na Amazon. WorkMail Para obter ajuda para determinar se uma chave do KMS é simétrica ou assimétrica, consulte Identificar chaves do KMS assimétricas.

Para localizar a chave do KMS da sua organização, use a entrada de log do AWS CloudTrail que registra chamadas para o AWS KMS.

Uma chave de criptografia exclusiva para cada caixa de correio

Quando você cria uma nova caixa de correio, a Amazon WorkMail gera uma chave de criptografia simétrica exclusiva do Advanced Encryption Standard (AES) de 256 bits para a caixa de correio, conhecida como chave de caixa de correio, fora dela. AWS KMS A Amazon WorkMail usa a chave da caixa de correio para proteger as chaves de criptografia de cada mensagem na caixa de correio.

Para proteger a chave da caixa de correio, a Amazon WorkMail liga AWS KMS para criptografar a chave da caixa de correio sob a chave KMS da organização. Ele armazena a chave de caixa de correio criptografada nos metadados da caixa de correio.

> **Note**
>
> A Amazon WorkMail usa uma chave de criptografia de caixa de correio simétrica para proteger as chaves das mensagens. Anteriormente, a Amazon WorkMail protegia cada caixa de correio com um par de chaves assimétrico. Ele usava a chave pública para criptografar cada chave de mensagem e a chave privada para descriptografá-la. A chave de caixa correio privada era protegida pela chave do KMS para a organização. As caixas de correio existentes ainda podem usar um par de chaves de caixa de correio assimétricas. Essa alteração não afeta a segurança da caixa de correio ou suas mensagens.

Uma chave de criptografia exclusiva para cada mensagem

Quando uma mensagem é adicionada à caixa de correio, a Amazon WorkMail gera uma chave de criptografia simétrica AES exclusiva de 256 bits para a mensagem externa. AWS KMS Ele usa essa chave de mensagem para criptografar a mensagem. A Amazon WorkMail criptografa a chave da

mensagem sob a chave da caixa de correio e armazena a chave da mensagem criptografada com a mensagem. Em seguida, ele criptografa a chave de caixa de correio na chave do KMS para a organização.

Criar uma caixa de correio

Quando a Amazon WorkMail cria uma nova caixa de correio, ela usa o seguinte processo para preparar a caixa de correio para armazenar mensagens criptografadas.

- WorkMail A Amazon gera uma chave de criptografia simétrica AES exclusiva de 256 bits para a caixa de correio externa. AWS KMS
- A Amazon WorkMail chama a operação AWS KMS Encrypt. Ela é transmitida na chave de caixa de correio e no identificador da AWS KMS key para a organização. O AWS KMS retorna um texto cifrado da chave de caixa de correio criptografada na chave do KMS.
- A Amazon WorkMail armazena a chave criptografada da caixa de correio com os metadados da caixa de correio.

Criptografar uma mensagem de caixa de correio

Para criptografar uma mensagem, a Amazon WorkMail usa o seguinte processo.

1. WorkMail A Amazon gera uma chave simétrica AES exclusiva de 256 bits para a mensagem. Ele usa a chave de dados de texto simples e o algoritmo AES (Advanced Encryption Standard) para criptografar a mensagem fora do AWS KMS.
2. Para proteger a chave da mensagem sob a chave da caixa de correio, a Amazon WorkMail precisa descriptografar a chave da caixa de correio, que é sempre armazenada em seu formato criptografado.

   A Amazon WorkMail chama a operação AWS KMS Decrypt e passa a chave criptografada da caixa de correio. AWS KMSusa a chave KMS da organização para descriptografar a chave da caixa de correio e retorna a chave da caixa de correio em texto simples para a Amazon. WorkMail
3. A Amazon WorkMail usa a chave da caixa de correio de texto simples e o algoritmo Advanced Encryption Standard (AES) para criptografar a chave da mensagem fora dela. AWS KMS
4. A Amazon WorkMail armazena a chave da mensagem criptografada nos metadados da mensagem criptografada para que esteja disponível para descriptografá-la.

Descriptografar uma mensagem de caixa de correio

Para descriptografar uma mensagem, a Amazon WorkMail usa o seguinte processo.

1. A Amazon WorkMail chama a operação AWS KMS Decrypt e passa a chave criptografada da caixa de correio. AWS KMSusa a chave KMS da organização para descriptografar a chave da caixa de correio e retorna a chave da caixa de correio em texto simples para a Amazon. WorkMail
2. A Amazon WorkMail usa a chave da caixa de correio de texto simples e o algoritmo Advanced Encryption Standard (AES) para descriptografar a chave da mensagem criptografada fora dela. AWS KMS
3. A Amazon WorkMail usa a chave da mensagem de texto simples para descriptografar a mensagem criptografada.

Armazenar chaves de caixa de correio em cache

Para melhorar o desempenho e minimizar as chamadas paraAWS KMS, a Amazon armazena em WorkMail cache cada chave de caixa de correio de texto simples de cada cliente localmente por até um minuto. No final do período de cache, a chave de caixa de correio é removida. Se a chave da caixa de correio desse cliente for necessária durante o período de armazenamento em cache, a Amazon WorkMail poderá obtê-la do cache em vez de ligar. AWS KMS A chave de caixa de correio está protegida no cache e nunca é gravada em disco em texto simples.

Autorizar o uso da chave do KMS

Quando a Amazon WorkMail usa um AWS KMS key em operações criptográficas, ela age em nome do administrador da caixa de correio.

Para usar a AWS KMS key para um segredo em seu nome, o administrador deve ter as permissões a seguir. Você pode especificar essas permissões necessárias em uma política do IAM ou uma política de chaves.

- `kms:Encrypt`
- `kms:Decrypt`
- `kms:CreateGrant`

Para permitir que a chave KMS seja usada somente para solicitações originadas na Amazon WorkMail, você pode usar a chave de ViaService condição kms: com o valor. `workmail.<region>.amazonaws.com`

Você também pode usar as chaves ou valores no contexto de criptografia como uma condição para usar a chave do KMS para operações de criptografia. Por exemplo, você pode usar um operador de condição de string em um documento do IAM ou de uma política de chaves, ou usar uma restrição de concessão em uma concessão.

Política de chaves para as Chave gerenciada pela AWS

A política de chaves do Chave gerenciada pela AWS for Amazon WorkMail dá aos usuários permissão para usar a chave KMS para operações específicas somente quando a Amazon WorkMail faz a solicitação em nome do usuário. A política de chaves não permite que os usuários utilizem a chave do KMS diretamente.

Essa política de chaves, como as políticas de todas as Chaves gerenciadas pela AWS, é estabelecida pelo serviço. Não é possível alterar a política de chaves, mas é possível visualizá-la a qualquer momento. Para obter mais detalhes, consulte Visualizar uma política de chaves.

As declarações de política na política de chaves têm os seguintes efeitos:

- Permita que os usuários da conta e da região usem a chave KMS para operações criptográficas e criem concessões, mas somente quando a solicitação vier da Amazon WorkMail em seu nome. A chave de condição `kms:ViaService` impõe essa restrição.
- Permite que a Conta da AWS crie políticas do IAM que permitem que os usuários visualizem as propriedades da chave do KMS e revoguem concessões.

A seguir está uma política fundamental para um exemplo Chave gerenciada pela AWS para a 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" : "*"
  } ]
}
```

Usando subsídios para autorizar a Amazon WorkMail

Além das principais políticas, a Amazon WorkMail usa concessões para adicionar permissões à chave KMS para cada organização. Para ver as concessões na chave KMS em sua conta, use a ListGrantsoperação.

A Amazon WorkMail usa concessões para adicionar as seguintes permissões à chave KMS da organização.

- Adicione a `kms:Encrypt` permissão para permitir que a Amazon criptografe WorkMail a chave da caixa de correio.
- Adicione a `kms:Decrypt` permissão para permitir que a Amazon use WorkMail a chave KMS para descriptografar a chave da caixa de correio. A Amazon WorkMail exige essa permissão em uma concessão porque a solicitação para ler mensagens da caixa de correio usa o contexto de segurança do usuário que está lendo a mensagem. A solicitação não usa as credenciais da Conta da AWS. WorkMail A Amazon cria essa concessão quando você seleciona uma chave KMS para a organização.

Para criar as doações, a Amazon WorkMail liga CreateGrantem nome do usuário que criou a organização. A permissão para criar a concessão vem de política de chaves. Essa política permite

que os usuários da conta `CreateGrant` solicitem a chave KMS da organização quando a Amazon WorkMail faz a solicitação em nome de um usuário autorizado.

A política de chaves também permite que a conta raiz revogue a concessão na Chave gerenciada pela AWS. No entanto, se você revogar a concessão, a Amazon WorkMail não poderá decifrar os dados criptografados em suas caixas de correio.

Contexto WorkMail de criptografia da Amazon

Um contexto de criptografia é um conjunto de pares de chave-valor que contêm dados arbitrários não secretos. Quando você inclui um contexto de criptografia em uma solicitação para criptografar dados, o AWS KMS vincula de forma criptográfica o contexto de criptografia aos dados criptografados. Para descriptografar os dados, você deve passar o mesmo contexto de criptografia.

A Amazon WorkMail usa o mesmo formato de contexto de criptografia em todas as operações AWS KMS criptográficas. É possível usar o contexto de criptografia para identificar uma operação criptográfica em logs e registros de auditoria, como o AWS CloudTrail, e como uma condição para a autorização em políticas e concessões.

Em suas solicitações de criptografia e descriptografia, a AWS KMS Amazon WorkMail usa um contexto de criptografia em que a chave está `aws:workmail:arn` e o valor é o Amazon Resource Name (ARN) da organização.

```
"aws:workmail:arn":"arn:aws:workmail:region:account ID:organization/organization ID"
```

Por exemplo, o seguinte contexto de criptografia inclui um ARN da organização de exemplo na região Leste dos EUA (Ohio) (`us-east-2`)

```
"aws:workmail:arn":"arn:aws:workmail:us-east-2:111122223333:organization/
m-68755160c4cb4e29a2b2f8fb58f359d7"
```

Monitorando a WorkMail interação da Amazon com AWS KMS

Você pode usar o AWS CloudTrail Amazon CloudWatch Logs para rastrear as solicitações que a Amazon WorkMail envia AWS KMS em seu nome.

Encrypt

Quando você cria uma nova caixa de correio, a Amazon WorkMail gera uma chave de caixa de correio e liga AWS KMS para criptografar a chave da caixa de correio. WorkMail A Amazon

envia uma solicitação Encrypt AWS KMS com a chave da caixa de correio em texto simples e um identificador para a chave KMS da organização Amazon. WorkMail

O evento que registra a operação `Encrypt` é semelhante ao evento de exemplo a seguir. O usuário é o WorkMail serviço da Amazon. Os parâmetros incluem o ID da chave KMS (`keyId`) e o contexto de criptografia da WorkMail organização Amazon. A Amazon WorkMail também passa a chave da caixa de correio, mas isso não é registrado no 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 você adiciona, visualiza ou exclui uma mensagem da caixa de correio, a Amazon WorkMail pede AWS KMS para descriptografar a chave da caixa de correio. WorkMail A Amazon envia uma solicitação Decrypt AWS KMS com a chave criptografada da caixa de correio e um identificador para a chave KMS da organização Amazon. WorkMail

O evento que registra a operação `Decrypt` é semelhante ao evento de exemplo a seguir. O usuário é o WorkMail serviço da Amazon. Os parâmetros incluem a chave criptografada da caixa de correio (como um blob de texto cifrado), que não é registrada no log, e o contexto de criptografia da organização Amazon. WorkMail AWS KMSderiva o ID da chave KMS do texto cifrado.

```
{
    "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"
}
```

Como WorkSpaces usa AWS KMS

Você pode usar WorkSpacespara provisionar um desktop (a WorkSpace) baseado em nuvem para cada um dos seus usuários finais. Ao iniciar um novo WorkSpace, você pode optar por criptografar seus volumes e decidir quais usar AWS KMS keypara a criptografia. Você pode escolher o Chave gerenciada pela AWSformulário WorkSpaces (aws/workspaces) ou uma chave simétrica gerenciada pelo cliente.

> **Important**
>
> WorkSpaces suporta somente chaves KMS de criptografia simétrica. Você não pode usar uma chave KMS assimétrica para criptografar os volumes em um. WorkSpaces Para obter ajuda para determinar se uma chave do KMS é simétrica ou assimétrica, consulte Identificar chaves do KMS assimétricas.

Para obter mais informações sobre a criação WorkSpaces com volumes criptografados, acesse Encrypt a WorkSpace no Amazon WorkSpaces Administration Guide.

Tópicos

- Visão geral da WorkSpaces criptografia usando AWS KMS
- WorkSpaces contexto de criptografia
- Dar WorkSpaces permissão para usar uma chave KMS em seu nome

Visão geral da WorkSpaces criptografia usando AWS KMS

Quando você cria WorkSpaces com volumes criptografados, WorkSpaces usa o Amazon Elastic Block Store (Amazon EBS) para criar e gerenciar esses volumes. Ambos os serviços usam sua AWS KMS key para trabalhar com os volumes criptografados. Para obter mais informações sobre criptografia de volume do EBS, consulte a documentação a seguir:

- Como o Amazon Elastic Block Store (Amazon EBS) usa o AWS KMS neste guia
- Criptografia do Amazon EBS, noManual do usuário do Amazon EC2 para instâncias Windows

Quando você inicia WorkSpaces com volumes criptografados, o end-to-end processo funciona assim:

1. Você especifica a chave KMS a ser usada para criptografia, bem como o usuário e o diretório WorkSpace do KMS. Essa ação cria uma concessão que permite WorkSpaces usar sua chave KMS somente para isso, ou WorkSpace seja, somente para a WorkSpace associada ao usuário e diretório especificados.
2. WorkSpaces cria um volume do EBS criptografado para o WorkSpace e especifica a chave KMS a ser usada, bem como o usuário e o diretório do volume (as mesmas informações que você especificou em). Step 1 Essa ação cria uma concessão que permite que o Amazon EBS use sua chave KMS somente para essa chave WorkSpace e para o volume, ou seja, somente para o WorkSpace associado ao usuário e diretório especificados e somente para o volume especificado.
3. O Amazon EBS solicita uma chave de dados de volume que é criptografada sob sua chave KMS e especifica o ID WorkSpace do usuário `Sid` e do diretório, bem como o ID do volume como contexto de criptografia.
4. O AWS KMS cria uma nova chave de dados, criptografa essa chave com sua chave do KMS e, em seguida, envia a chave de dados criptografada ao Amazon EBS.
5. WorkSpaces usa o Amazon EBS para anexar o volume criptografado ao seu WorkSpace. O Amazon EBS envia a chave de dados criptografada para AWS KMS com uma `Decrypt`solicitação e especifica a WorkSpace do usuário`Sid`, seu ID de diretório e o ID do volume, que é usado como contexto de criptografia.
6. O AWS KMS usa sua chave do KMS para descriptografar a chave de dados e, em seguida, envia a chave de dados em texto simples ao Amazon EBS.
7. O Amazon EBS usa a chave de dados em texto simples para criptografar todos os dados enviados e recebidos do volume criptografado. O Amazon EBS mantém a chave de dados de texto simples na memória enquanto o volume estiver conectado ao. WorkSpace
8. O Amazon EBS armazena a chave de dados criptografada (recebida emStep 4) com os metadados do volume para uso futuro, caso você reinicie ou reconstrua o. WorkSpace
9. Quando você usa o AWS Management Console para remover uma WorkSpace (ou usa a `TerminateWorkspaces`ação na WorkSpaces API), WorkSpaces o Amazon EBS retira as concessões que permitiram que eles usassem sua chave KMS para isso. WorkSpace

WorkSpaces contexto de criptografia

WorkSpaces não usa seu AWS KMS key diretamente para operações criptográficas (como `Encrypt`,, `Decrypt`, etc.) `GenerateDataKey`, o que significa que WorkSpaces não envia solicitações AWS KMS que incluam um contexto de criptografia. No entanto, quando o Amazon EBS solicita uma chave de dados criptografada para os seus volumes criptografados WorkSpaces (Step 3noVisão geral da WorkSpaces criptografia usando AWS KMS) e quando solicita uma cópia em texto simples dessa chave de dados (Step 5), ele inclui o contexto de criptografia na solicitação. O contexto de criptografia fornece dados autenticados adicionais (AAD) que o AWS KMS usa para garantir a integridade dos dados. O contexto de criptografia também é gravado em seus arquivos de log do AWS CloudTrail, o que pode ajudar você a entender por que uma determinada AWS KMS key foi usada. O Amazon EBS usa o seguinte como contexto de criptografia:

- O `sid` do AWS Directory Service usuário que está associado ao WorkSpace
- O ID do AWS Directory Service diretório associado ao WorkSpace
- O ID do volume criptografado

O exemplo a seguir mostra uma representação JSON do contexto de criptografia usado pelo Amazon EBS:

```
{
  "aws:workspaces:sid-directoryid":
 "[S-1-5-21-277731876-1789304096-451871588-1107]@[d-1234abcd01]",
  "aws:ebs:id": "vol-1234abcd"
}
```

Dar WorkSpaces permissão para usar uma chave KMS em seu nome

Você pode proteger os dados do seu espaço de trabalho sob o Chave gerenciada pela AWS WorkSpaces formulário (aws/workspaces) ou uma chave gerenciada pelo cliente. Se você usar uma chave gerenciada pelo cliente, precisará dar WorkSpaces permissão para usar a chave KMS em nome dos administradores da WorkSpaces sua conta. O Chave gerenciada pela AWS formulário WorkSpaces tem as permissões necessárias por padrão.

Para preparar sua chave gerenciada pelo cliente para uso com WorkSpaces, use o procedimento a seguir.

1. Adicione os WorkSpaces administradores à lista de usuários-chave na política de chaves da chave KMS
2. Conceda aos WorkSpaces administradores permissões adicionais com uma política do IAM

WorkSpaces os administradores também precisam de permissão para usar WorkSpaces. Para obter mais informações sobre essas permissões, acesse Controlando o acesso aos WorkSpaces recursos no Amazon WorkSpaces Administration Guide.

Parte 1: Adicionando WorkSpaces administradores aos principais usuários de uma chave KMS

Para dar aos WorkSpaces administradores as permissões de que eles precisam, você pode usar a AWS Management Console ou a AWS KMS API.

Para adicionar WorkSpaces administradores como usuários-chave de uma chave KMS (console)

1. Faça login no AWS Management Console e abra o console do AWS Key Management Service (AWS KMS) em https://console.aws.amazon.com/kms.
2. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.
3. No painel de navegação, escolha Customer managed keys (Chaves gerenciadas pelo cliente).
4. Escolha o ID de chave ou alias da sua chave gerenciada pelo cliente preferida
5. Selecione a guia Key policy (Política de chaves). Em Key users (Usuários de chaves), escolhaAdd (Adicionar).
6. Na lista de usuários e funções do IAM, selecione os usuários e funções que correspondem aos seus WorkSpaces administradores e, em seguida, escolha Anexar.

Para adicionar WorkSpaces administradores como usuários-chave de uma chave KMS (API) AWS KMS

1. Use a GetKeyPolicyoperação para obter a política de chaves existente e, em seguida, salve o documento de política em um arquivo.
2. Abra o documento de política no editor de texto de sua preferência. Adicione os usuários e funções do IAM que correspondem aos seus WorkSpaces administradores às declarações de política que dão permissão aos principais usuários. Salve o arquivo.
3. Use a PutKeyPolicyoperação para aplicar a política de chaves à chave KMS.

Parte 2: Conceder WorkSpaces permissões extras aos administradores

Se você estiver usando uma chave gerenciada pelo cliente para proteger seus WorkSpaces dados, além das permissões na seção de usuários-chave da política de chaves padrão, WorkSpaces os administradores precisam de permissão para criar concessões na chave KMS. Além disso, se usarem o AWS Management Consolepara criar WorkSpaces com volumes criptografados, os WorkSpaces administradores precisarão de permissão para listar aliases e chaves de lista. Para obter mais informações sobre como criar e editar políticas de usuário do IAM, consulte Políticas gerenciadas e em linha, no Manual do usuário do IAM.

Para conceder essas permissões aos seus WorkSpaces administradores, use uma política do IAM. Adicione uma declaração de política semelhante ao exemplo a seguir à política do IAM para cada WorkSpaces administrador. Substitua o ARN da chave do KMS de exemplo (*arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab*) por um válido. Se seus WorkSpaces administradores usam somente a WorkSpaces API (não o console), você pode omitir a segunda declaração de política com as permissões `"kms:ListAliases"` e. `"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": "*"
    }
  ]
}
```

Programação da API do AWS KMS

Você pode usar a API AWS KMS para criar e gerenciar chaves KMS e recursos especiais, como armazenamentos de chaves personalizados e usar chaves do KMS em operações criptográficas. Para obter mais informações, consulte a Referência da API do AWS Key Management Service.

O código de exemplo nos tópicos a seguir mostra como usar os AWS SDKs para chamar a API do AWS KMS.

Para obter informações sobre como usar o console do AWS KMS para executar algumas dessas tarefas, consulte Gerenciar chaves do .

Tópicos

- Criar um cliente
- Trabalhar com chaves
- Trabalhar com aliases
- Criptografar e descriptografar chaves de dados
- Trabalhar com políticas de chaves
- Trabalhar com concessões
- Como testar suas chamadas de API do AWS KMS
- Consistência eventual do AWS KMS

Criar um cliente

Para usar o AWS SDK for Java, the AWS SDK for .NET, the AWS SDK for Python (Boto3), the AWS SDK for RubyAWS SDK for PHP, the ou o AWSSDK do Node.js para JavaScript escrever código que usa a API AWS Key Management Service (AWS KMS), comece criando um AWS KMS cliente.

O objeto do cliente que você cria é usado no código de exemplo nos tópicos a seguir.

Java

Para criar um cliente do AWS KMS em Java, use o compilador de cliente.

```
AWSKMS kmsClient = AWSKMSClientBuilder.standard().build();
```

Para obter mais informações sobre como usar o criador do cliente Java, consulte os seguintes recursos.

- Fluent Client Builders no Blog de desenvolvedores da AWS
- Como criar clientes de serviço, no Guia do desenvolvedor do AWS SDK for Java
- AWSKMSClientBuilder na Referência de API do 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

Para criar um cliente do AWS KMS no PHP, use um objeto de cliente do AWS KMS e especifique a versão `2014-11-01`. Para obter mais informações, consulte a Classe KMSClient, na Referência de APIs do 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();
```

Trabalhar com chaves

Os exemplos neste tópico usam a API do AWS KMS para criar, visualizar, habilitar e desabilitar AWS KMS AWS KMS keys e para gerar chaves de dados.

Tópicos

- Criar uma chave do KMS
- Gerar uma chave de dados
- Como visualizar um AWS KMS key
- Obter IDs e ARNs de chaves do KMS
- Habilitar o AWS KMS keys
- Desabilitar as AWS KMS key

Criar uma chave do KMS

Para criar uma AWS KMS key(chave KMS), use a CreateKeyoperação. Os exemplos nesta seção criam uma chave do KMS de criptografia simétrica. O parâmetro `Description` usado nesses exemplos é opcional.

Em linguagens que exigem um objeto cliente, esses exemplos usam o objeto cliente do AWS KMS criado em Criar um cliente.

Para obter ajuda com a criação de chaves do KMS no console do AWS KMS, consulte Criar chaves.

Java

Para obter detalhes, consulte o Método createKey, na Referência de APIs do 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#

Para obter detalhes, consulte o Método CreateKey no 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

Para obter detalhes, consulte o Método `create_key` no AWS SDK for Python (Boto3).

```
# Create a KMS key

desc = 'Key for protecting critical data'

response = kms_client.create_key(
    Description=desc
)
```

Ruby

Para obter detalhes, consulte o método de instância `create_key` no AWS SDK for Ruby.

```
# Create a KMS key

desc = 'Key for protecting critical data'

response = kmsClient.create_key({
  description: desc
})
```

PHP

Para obter detalhes, consulte o Método CreateKey no AWS SDK for PHP.

```
// Create a KMS key
//
$desc = "Key for protecting critical data";

$result = $KmsClient->createKey([
```

```
    'Description' => $desc
]);
```

Node.js

Para obter detalhes, consulte a propriedade createKey no SDK JavaScript em AWS Node.js.

```
// Create a KMS key
//
const Description = 'Key for protecting critical data';

kmsClient.createKey({ Description }, (err, data) => {
  ...
});
```

PowerShell

Para criar uma chave KMS PowerShell, use o KmsKey cmdlet New-.

```
# Create a KMS key

$desc = 'Key for protecting critical data'
New-KmsKey -Description $desc
```

Para usar os AWS KMS PowerShell cmdlets, instale o AWS.Tools.KeyManagementServicemódulo. Para obter mais informações, consulte o AWS Tools for Windows PowerShellGuia do Usuário.

Gerar uma chave de dados

Para gerar uma chave de dados simétrica, use a GenerateDataKeyoperação. Essa operação retorna uma chave de dados de texto simples e uma cópia dessa chave de dados criptografada com a chave do KMS de criptografia simétrica que você especifica. É necessário especificar um `KeySpec` ou `NumberOfBytes` (mas não ambos) em cada comando.

Para obter ajuda para usar a chave de dados para criptografar dados, consulte o AWS Encryption SDK. Você também pode usar a chave de dados em operações de Hash-based message authentication code (HMAC – Código de autenticação de mensagem por hash).

Em linguagens que exigem um objeto cliente, esses exemplos usam o objeto cliente do AWS KMS criado em Criar um cliente.

Java

Para obter detalhes, consulte o generateDataKey método na Referência AWS SDK for Java da API.

```
// 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#

Para obter detalhes, consulte o Método GenerateDataKey no 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

Para obter detalhes, consulte o Método `generate_data_key` no 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

Para obter detalhes, consulte o método de instância `generate_data_key` no 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

Para obter detalhes, consulte o Método GenerateDataKey no 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

Para obter detalhes, consulte a generateDataKey propriedade no AWSSDK JavaScript em 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

Para gerar uma chave de dados simétrica, use o cmdlet New-KMS DataKey.

Na saída, a chave de texto simples (na `Plaintext` propriedade) e a chave criptografada (na `CiphertextBlob` propriedade) são MemoryStreamobjetos. Para convertê-los em cadeias de caracteres, use os métodos da `MemoryStream` classe ou um cmdlet ou função que

converta `MemoryStream` objetos em cadeias de caracteres, como as funções ConvertFrom-MemoryStream e ConvertFrom-Base64 no módulo 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
```

Para usar os AWS KMS PowerShell cmdlets, instale o AWS.Tools.KeyManagementServicemódulo. Para obter mais informações, consulte o AWS Tools for Windows PowerShellGuia do Usuário.

Como visualizar um AWS KMS key

Para obter informações detalhadas sobre umAWS KMS key, incluindo o ARN da chave KMS e o estado da chave, use DescribeKeya operação.

`DescribeKey` não recebe aliases. Para obter aliases, use a ListAliasesoperação. Para ver exemplos, consulte Trabalhar com aliases.

Em linguagens que exigem um objeto cliente, esses exemplos usam o objeto cliente do AWS KMS criado em Criar um cliente.

Para obter ajuda com a visualização de chaves do KMS no console do AWS KMS, consulte Visualizar chaves.

Java

Para obter detalhes, consulte o Método describeKey, na Referência de APIs do 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#

Para obter detalhes, consulte o Método DescribeKey no 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

Para obter detalhes, consulte o Método `describe_key` no 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

Para obter detalhes, consulte o método de instância `describe_key` no 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

Para obter detalhes, consulte o Método DescribeKey no 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

Para obter detalhes, consulte a propriedade describeKey no SDK JavaScript em 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

Para obter informações detalhadas sobre uma chave KMS, use o KmsKey cmdlet Get-.

```
# 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
```

Para usar os AWS KMS PowerShell cmdlets, instale o AWS.Tools.KeyManagementServicemódulo. Para obter mais informações, consulte o AWS Tools for Windows PowerShellGuia do Usuário.

Obter IDs e ARNs de chaves do KMS

Para obter os IDs das chaves e os ARNs das chaves doAWS KMS keys, use a ListKeysoperação. Esses exemplos usam o parâmetro `Limit` opcional, que define o número máximo de chaves do KMS retornadas em cada chamada. Para obter ajuda para identificar uma chave do KMS em uma operação do AWS KMS, consulte Identificadores-chave () KeyId.

Em linguagens que exigem um objeto cliente, esses exemplos usam o objeto cliente do AWS KMS criado em Criar um cliente.

Para obter ajuda sobre como localizar IDs e ARNs de chaves no console do AWS KMS, consulte Como encontrar o ID e o ARN da chave.

Java

Para obter detalhes, consulte o Método listKeys, na Referência de APIs do 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#

Para obter detalhes, consulte o Método ListKeys no 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

Para obter detalhes, consulte o Método `list_keys` no AWS SDK for Python (Boto3).

```
# List KMS keys in this account

response = kms_client.list_keys(
    Limit=10
)
```

Ruby

Para obter detalhes, consulte o método de instância `list_keys` no AWS SDK for Ruby.

```
# List KMS keys in this account

response = kmsClient.list_keys({
  limit: 10
})
```

PHP

Para obter detalhes, consulte o Método ListKeys no AWS SDK for PHP.

```
// List KMS keys in this account
//
$limit = 10;

$result = $KmsClient->listKeys([
    'Limit' => $limit,
]);
```

Node.js

Para obter detalhes, consulte a propriedade listKeys no AWSSDK em Node.js. JavaScript

```
// List KMS keys in this account
//
const Limit = 10;
kmsClient.listKeys({ Limit }, (err, data) => {
  ...
});
```

PowerShell

Para obter o ID e o ARN da chave de todas as chaves KMS na conta e na região, use o cmdlet Get -. KmsKeyList

Para limitar o número de objetos de saída, este exemplo usa o cmdlet Select-Object em vez do parâmetro `Limit`, que está defasado nos cmdlets da lista. Para obter ajuda com a saída da paginação no AWS Tools for PowerShell, consulte Paginação de saída com o AWS Tools for PowerShell.

```
# List KMS keys in this account

$limit = 10
Get-KmsKeyList | Select-Object -First $limit
```

Para usar os AWS KMS PowerShell cmdlets, instale o AWS.Tools. KeyManagementServicemódulo. Para obter mais informações, consulte o AWS Tools for Windows PowerShellGuia do Usuário.

Habilitar o AWS KMS keys

Para habilitar um desativadoAWS KMS key, use a EnableKeyoperação.

Em linguagens que exigem um objeto cliente, esses exemplos usam o objeto cliente do AWS KMS criado em Criar um cliente.

Para obter ajuda sobre como habilitar e desabilitar chaves do KMS no console do AWS KMS, consulte Habilitar e desabilitar chaves.

Java

Para obter detalhes sobre a implementação de Java, consulte o Método enableKey, na Referência de APIs do 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#

Para obter detalhes, consulte o Método EnableKey no 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

Para obter detalhes, consulte o Método `enable_key` no 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

Para obter detalhes, consulte o método de instância `enable_key` no 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

Para obter detalhes, consulte o Método EnableKey no 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

Para obter detalhes, consulte a propriedade enableKey no SDK JavaScript em 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

Para habilitar uma chave KMS, use o KmsKey cmdlet Enable-.

```
# 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
```

Para usar os AWS KMS PowerShell cmdlets, instale o AWS.Tools.KeyManagementServicemódulo. Para obter mais informações, consulte o AWS Tools for Windows PowerShellGuia do Usuário.

Desabilitar as AWS KMS key

Para desativar uma chave KMS, use a DisableKeyoperação. A desabilitação de uma chave do KMS impede que ela seja usada em operações de criptografia.

Em linguagens que exigem um objeto cliente, esses exemplos usam o objeto cliente do AWS KMS criado em Criar um cliente.

Para obter ajuda sobre como habilitar e desabilitar chaves do KMS no console do AWS KMS, consulte Habilitar e desabilitar chaves.

Java

Para obter detalhes, consulte o Método disableKey, na Referência de APIs do 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#

Para obter detalhes, consulte o Método DisableKey no 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

Para obter detalhes, consulte o Método `disable_key` no 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

Para obter detalhes, consulte o método de instância `disable_key` no 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

Para obter detalhes, consulte o Método DisableKey no 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

Para obter detalhes, consulte a propriedade disableKey no SDK JavaScript em 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

Para desativar uma chave KMS, use o KmsKey cmdlet Disable-.

```
# 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
```

Para usar os AWS KMS PowerShell cmdlets, instale o AWS.Tools.KeyManagementServicemódulo. Para obter mais informações, consulte o Guia do usuário da AWS Tools for Windows PowerShell.

Trabalhar com aliases

Os exemplos neste tópico usam a API do AWS KMS para criar, visualizar, atualizar e excluir aliases. Para obter mais informações sobre aliases, consulte the section called “Usar aliases”.

Tópicos

- Criar um alias
- Listar aliases
- Atualizar um alias
- Excluir um alias

Criar um alias

Quando você cria uma AWS KMS key no AWS Management Console, é necessário criar um alias para ela. No entanto, a CreateKeyoperação que cria uma chave KMS não cria um alias.

Para criar um alias, use a CreateAliasoperação. O alias deve ser exclusivo na conta e na região. Você não pode criar um alias que comece com `aws/`. O prefixo `aws/` é reservado pela Amazon Web Services para Chaves gerenciadas pela AWS.

Em linguagens que exigem um objeto cliente, esses exemplos usam o objeto cliente do AWS KMS criado em Criar um cliente.

Java

Para obter detalhes, consulte o Método createAlias na Referência de APIs do 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#

Para obter detalhes, consulte o Método CreateAlias no 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

Para obter detalhes, consulte o Método `create_alias` no 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

Para obter detalhes, consulte o método de instância `create_alias` no 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

Para obter detalhes, consulte o Método CreateAlias no 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

Para obter detalhes, consulte a propriedade createAlias no SDK em 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

Para criar um alias, use o cmdlet New-KMSAlias. O nome do alias diferencia maiúsculas de minúsculas.

```
# 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
```

Para usar os AWS KMS PowerShell cmdlets, instale o AWS.Tools.KeyManagementServicemódulo. Para obter mais informações, consulte o AWS Tools for Windows PowerShellGuia do Usuário.

Listar aliases

Para listar aliases na conta e na região, use a ListAliasesoperação.

Por padrão, o comando ListAliases gera todos os aliases na conta e na região. Isso inclui aliases que você criou e associou às suas chaves gerenciadas pelo cliente e aliases que a AWS criou e associou às suas Chaves gerenciadas pela AWS. A resposta também pode incluir aliases sem campo `TargetKeyId`. Estes são aliases predefinidos criados pela AWS, mas que ainda não estão associados a uma chave do KMS.

Em linguagens que exigem um objeto cliente, esses exemplos usam o objeto cliente do AWS KMS criado em Criar um cliente.

Java

Para obter detalhes sobre a implementação de Java, consulte o Método listAliases na Referência de APIs do AWS SDK for Java.

```
// List the aliases in this Conta da AWS
//
Integer limit = 10;

ListAliasesRequest req = new ListAliasesRequest().withLimit(limit);
ListAliasesResult result = kmsClient.listAliases(req);
```

C#

Para obter detalhes, consulte o Método ListAliases no AWS SDK for .NET.

```
// List the aliases in this Conta da AWS
//
int limit = 10;

ListAliasesRequest listAliasesRequest = new ListAliasesRequest()
```

```
{
    Limit = limit
};
ListAliasesResponse listAliasesResponse = kmsClient.ListAliases(listAliasesRequest);
```

Python

Para obter detalhes, consulte o Método `list_aliases` no AWS SDK for Python (Boto3).

```
# List the aliases in this Conta da AWS

response = kms_client.list_aliases(
    Limit=10
)
```

Ruby

Para obter detalhes, consulte o método de instância `list_aliases` no AWS SDK for Ruby.

```
# List the aliases in this Conta da AWS

response = kmsClient.list_aliases({
  limit: 10
})
```

PHP

Para obter detalhes, consulte o Método List Aliases no AWS SDK for PHP.

```
// List the aliases in this Conta da AWS
//
$limit = 10;

$result = $KmsClient->listAliases([
    'Limit' => $limit,
]);
```

Node.js

Para obter detalhes, consulte a propriedade listAliases no SDK JavaScript em AWS Node.js.

```
// List the aliases in this Conta da AWS
```

```
//
const Limit = 10;
kmsClient.listAliases({ Limit }, (err, data) => {
  ...
});
```

PowerShell

Para listar os aliases na conta e na região, use o cmdlet Get-KMS AliasList.

Para limitar o número de objetos de saída, este exemplo usa o cmdlet Select-Object em vez do parâmetro `Limit`, que está defasado nos cmdlets da lista. Para obter ajuda com a saída da paginação no AWS Tools for PowerShell, consulte Paginação de saída com o AWS Tools for PowerShell.

```
# List the aliases in this Conta da AWS
$limit = 10

$result = Get-KMSAliasList | Select-Object -First $limit
```

Para usar os AWS KMS PowerShell cmdlets, instale o AWS.Tools. KeyManagementServicemódulo. Para obter mais informações, consulte o AWS Tools for Windows PowerShellGuia do Usuário.

Para relacionar apenas os aliases que estão associados a uma determinada chave do KMS, use o parâmetro `KeyId`. Seu valor pode ser o ID da chave ou i ARN de chave de qualquer chave do KMS na região. Você não pode especificar um nome de alias ou ARN de alias.

Java

Para obter detalhes sobre a implementação de Java, consulte o Método listAliases na Referência de APIs do 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#

Para obter detalhes, consulte o Método ListAliases no 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

Para obter detalhes, consulte o Método `list_aliases` no 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

Para obter detalhes, consulte o método de instância `list_aliases` no 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

Para obter detalhes, consulte o Método List Aliases no 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

Para obter detalhes, consulte a propriedade listAliases no SDK JavaScript em 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

Para listar os aliases de uma chave KMS, use o `KeyId` parâmetro do cmdlet AliasListGet-KMS.

```
# 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
```

Para usar os AWS KMS PowerShell cmdlets, instale o AWS.Tools.KeyManagementServicemódulo. Para obter mais informações, consulte o AWS Tools for Windows PowerShellGuia do Usuário.

Atualizar um alias

Para associar um alias existente a uma chave KMS diferente, use a UpdateAliasoperação.

Em linguagens que exigem um objeto cliente, esses exemplos usam o objeto cliente do AWS KMS criado em Criar um cliente.

Java

Para obter detalhes sobre a implementação de Java, consulte o Método updateAlias no Referência de APIs do 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#

Para obter detalhes, consulte o Método UpdateAlias no 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

Para obter detalhes, consulte o Método `update_alias` no 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

Para obter detalhes, consulte o método de instância `update_alias` no 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

Para obter detalhes, consulte o Método UpdateAlias no 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

Para obter detalhes, consulte a propriedade updateAlias no SDK em 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

Para alterar a chave do KMS associada a um alias, use o cmdlet Update-KMSAlias. O nome do alias diferencia maiúsculas de minúsculas.

O cmdlet `Update-KMSAlias` não retorna nenhuma saída. Para verificar se o comando funcionou, use o 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
```

Para usar os AWS KMS PowerShell cmdlets, instale o AWS.Tools.KeyManagementServicemódulo. Para obter mais informações, consulte o AWS Tools for Windows PowerShellGuia do Usuário.

Excluir um alias

Para excluir um alias, use a DeleteAliasoperação. A exclusão de um alias não afeta a chave do KMS associada.

Em linguagens que exigem um objeto cliente, esses exemplos usam o objeto cliente do AWS KMS criado em Criar um cliente.

Java

Para obter detalhes, consulte o Método deleteAlias, na Referência de APIs do 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#

Para obter detalhes, consulte o Método DeleteAlias no 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

Para obter detalhes, consulte o Método `delete_alias` no 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

Para obter detalhes, consulte o método de instância `delete_alias` no AWS SDK for Ruby.

```
# Delete an alias for a KMS key

alias_name = 'alias/projectKey1'

response = kmsClient.delete_alias({
  alias_name: alias_name
})
```

PHP

Para obter detalhes, consulte o Método DeleteAlias no AWS SDK for PHP.

```
// Delete an alias for a KMS key
//
$aliasName = "alias/projectKey1";

$result = $KmsClient->deleteAlias([
    'AliasName' => $aliasName,
]);
```

Node.js

Para obter detalhes, consulte a propriedade DeleteAlias) no SDK para Node.js. AWS JavaScript

```
// Delete an alias for a KMS key
//
```

```
const AliasName = 'alias/projectKey1';
kmsClient.deleteAlias({ AliasName }, (err, data) => {
  ...
});
```

PowerShell

Para excluir um alias, use o cmdlet Remove-KMSAlias. O nome do alias diferencia maiúsculas de minúsculas.

Como esse cmdlet exclui permanentemente o alias, PowerShell solicita que você confirme o comando. O `ConfirmImpact` é `High`, portanto, não é possível usar um `ConfirmPreference` para suprimir esse prompt. Se for necessário suprimir o prompt de confirmação, adicione o parâmetro `Confirm` comum com um valor `$false`, por exemplo, `-Confirm:$false`.

O cmdlet `Remove-KMSAlias` não retorna nenhuma saída. Para verificar se o comando foi efetivo, use o cmdlet Get-KMS AliasList.

```
# Delete an alias for a KMS key

$aliasName = 'alias/projectKey1'
Remove-KMSAlias -AliasName $aliasName
```

Para usar os AWS KMS PowerShell cmdlets, instale o AWS.Tools. KeyManagementServicemódulo. Para obter mais informações, consulte o Guia do usuário da AWS Tools for Windows PowerShell.

Criptografar e descriptografar chaves de dados

Os exemplos neste tópico usam as ReEncryptoperações Encrypt, Decrypt e na API. AWS KMS

Essas operações são projetadas para criptografar e descriptografar chaves de dados. Elas usam uma AWS KMS keys nas operações de criptografia e não podem aceitar mais de 4 KB (4.096 bytes) de dados. Embora você possa usá-las para criptografar pequenas quantidades de dados, como uma senha ou chave RSA, elas não serão projetadas para criptografar dados de aplicações.

Para criptografar dados de aplicações, use os recursos de criptografia no lado do servidor de um serviço da AWS ou uma biblioteca de criptografia de cliente, como a AWS Encryption SDK ou o Cliente de criptografia do Amazon S3.

Tópicos

- Criptografar uma chave de dados
- Descriptografia de uma chave de dados
- Criptografar novamente uma chave de dados em uma AWS KMS key

Criptografar uma chave de dados

A operação Encrypt é projetada para criptografar chaves de dados, mas não é frequentemente usada. As GenerateDataKeyWithoutPlaintextoperações GenerateDataKeye retornam chaves de dados criptografadas. Você pode usar essa método quando está movendo dados criptografados para uma região diferente e deseja criptografar sua chave de dados com uma chave KMS na nova região.

Em linguagens que exigem um objeto cliente, esses exemplos usam o objeto cliente do AWS KMS criado em Criar um cliente.

Java

Para detalhes, consulte o Método encrypt, na Referência de APIs do 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#

Para obter detalhes, consulte o Método Encrypt no 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

Para obter detalhes, consulte o Método encrypt no 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

Para obter detalhes, consulte o método de instância encrypt no 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

Para obter detalhes, consulte o Método Encrypt no 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

Para obter detalhes, consulte a propriedade encrypt no AWS SDK JavaScript em 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

Para criptografar uma chave de dados em uma chave do KMS, use o cmdlet Invoke-KMSEncrypt. Ele retorna o texto cifrado como um `MemoryStream` (System.io). MemoryStream) objeto. É possível usar o objeto `MemoryStream` como entrada para o cmdlet Invoke-KMSDecrypt.

O AWS KMS também retorna chaves de dados como objetos `MemoryStream`. Neste exemplo, para simular uma chave de dados de texto simples, criamos uma matriz de bytes e a gravamos em um objeto `MemoryStream`.

Observe que o parâmetro `Plaintext` de `Invoke-KMSEncrypt` utiliza uma matriz de bytes (`byte[]`). Ele não requer um objeto `MemoryStream`. A partir da AWSPowerShell versão 4.0, os parâmetros em todos os AWSPowerShell módulos que usam matrizes de bytes e `MemoryStream` objetos aceitam matrizes de bytes, objetos, strings, `MemoryStream` matrizes de strings e (System.io). `FileInfo` FileInfo) objetos. É possível passar qualquer um desses tipos para `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
```

Para usar os AWS KMS PowerShell cmdlets, instale o AWS.Tools. KeyManagementServicemódulo. Para obter mais informações, consulte o Manual do usuário do AWS Tools for Windows PowerShell.

Descriptografia de uma chave de dados

Para descriptografar uma chave de dados, use a operação Decrypt.

O `ciphertextBlob` que você especificar deve ser o valor do `CiphertextBlob` campo de uma resposta GenerateDataKey, GenerateDataKeyWithoutPlaintext, ou Criptografar, ou o `PrivateKeyCiphertextBlob` campo de uma GenerateDataKeyPairWithoutPlaintextresposta GenerateDataKeyPairou. Também é possível usar a operação `Decrypt` para descriptografar dados criptografados fora do AWS KMS pela chave pública em uma chave do KMS assimétrica.

O parâmetro `KeyId` não é necessário ao descriptografar com chaves do KMS de criptografia simétrica. O AWS KMS pode obter a chave do KMS que foi usada para criptografar os dados diretamente dos metadados no blob de texto cifrado. Porém, sempre é uma prática recomendada especificar a chave do KMS que você está usando. Essa prática garante que você use a chave do KMS desejada e impede que você descriptografe um texto cifrado acidentalmente usando uma chave do KMS em que você não confia.

Em linguagens que exigem um objeto cliente, esses exemplos usam o objeto cliente do AWS KMS criado em Criar um cliente.

Java

Para obter detalhes, consulte o Método decrypt, na Referência de APIs do 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#

Para obter detalhes, consulte o Método Decrypt no 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

Para obter detalhes, consulte o Método decrypt no 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

Para obter detalhes, consulte o método de instância decrypt no 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

Para obter detalhes, consulte o Método Decrypt no 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

Para obter detalhes, consulte a propriedade decrypt no AWSSDK em 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

Para descriptografar uma chave de dados, use o cmdlet Invoke-KMSEncrypt.

Esse cmdlet retorna o texto simples como um (System.IO). `MemoryStream` MemoryStream) objeto. Para convertê-lo em uma matriz de bytes, use cmdlets ou funções que convertem objetos `MemoryStream` em matrizes de bytes, como as funções no módulo Converter.

Como esse exemplo usa o texto cifrado por um cmdlet de criptografia do AWS KMS retornado, ele usa um objeto `MemoryStream` para o valor do parâmetro `CiphertextBlob`. No entanto, o parâmetro `CiphertextBlob` de `Invoke-KMSDecrypt` utiliza uma matriz de bytes (`byte[]`). Ele não requer um objeto `MemoryStream`. A partir da AWSPowerShell versão 4.0, os parâmetros em todos os AWSPowerShell módulos que usam matrizes de bytes e `MemoryStream` objetos aceitam matrizes de bytes, objetos, strings, `MemoryStream` matrizes de strings e (System.io). `FileInfo` FileInfo) objetos. É possível passar qualquer um desses tipos para `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
```

Para usar os AWS KMS PowerShell cmdlets, instale o AWS.Tools. KeyManagementServicemódulo. Para obter mais informações, consulte o AWS Tools for Windows PowerShellGuia do Usuário.

Criptografar novamente uma chave de dados em uma AWS KMS key

Para descriptografar uma chave de dados criptografada e, em seguida, recriptografar imediatamente a chave de dados em outraAWS KMS key, use a operação. ReEncrypt As operações são realizadas inteiramente no lado servidor dentro do AWS KMS, para nunca exporem o texto não criptografado fora do AWS KMS.

O `ciphertextBlob` que você especificar deve ser o valor do `CiphertextBlob` campo de uma resposta GenerateDataKey, GenerateDataKeyWithoutPlaintext, ou Criptografar, ou o

`PrivateKeyCiphertextBlob` campo de uma GenerateDataKeyPairWithoutPlaintextresposta GenerateDataKeyPairou. Também é possível usar a operação `ReEncrypt` para recriptografar dados criptografados fora do AWS KMS pela chave pública em uma chave do KMS assimétrica.

O parâmetro `SourceKeyId` não é necessário ao recriptografar com chaves do KMS de criptografia simétrica. O AWS KMS pode obter a chave do KMS que foi usada para criptografar os dados diretamente dos metadados no blob de texto cifrado. Porém, sempre é uma prática recomendada especificar a chave do KMS que você está usando. Essa prática garante que você use a chave do KMS desejada e impede que você descriptografe um texto cifrado acidentalmente usando uma chave do KMS em que você não confia.

Em linguagens que exigem um objeto cliente, esses exemplos usam o objeto cliente do AWS KMS criado em Criar um cliente.

Java

Para detalhes, consulte o Método reEncrypt, na Referência de APIs do 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#

Para obter detalhes, consulte o Método ReEncrypt no 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

Para obter detalhes, consulte o Método `re_encrypt` no 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

Para obter detalhes, consulte o método de instância `re_encrypt` no 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

Para obter detalhes, consulte o Método ReEncrypt no 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

Para obter detalhes, consulte a propriedade reEncrypt no SDK JavaScript em 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

Para recriptografar um texto cifrado com a mesma chave KMS ou com uma chave KMS diferente, use o cmdlet Invoke-KMS. ReEncrypt

Como esse exemplo usa o texto cifrado por um cmdlet de criptografia do AWS KMS retornado, ele usa um objeto `MemoryStream` para o valor do parâmetro `CiphertextBlob`. No entanto, o parâmetro `CiphertextBlob` de `Invoke-KMSReEncrypt` utiliza uma matriz de bytes (`byte[]`). Ele não requer um objeto `MemoryStream`. A partir da AWSPowerShell versão 4.0, os parâmetros em todos os AWSPowerShell módulos que usam matrizes de bytes e `MemoryStream` objetos aceitam matrizes de bytes, objetos, strings, `MemoryStream` matrizes de strings e (System.io). `FileInfo` FileInfo) objetos. É possível passar qualquer um desses tipos para `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
```

Para usar os AWS KMS PowerShell cmdlets, instale o AWS.Tools.KeyManagementServicemódulo. Para obter mais informações, consulte o Guia do usuário da AWS Tools for Windows PowerShell.

Trabalhar com políticas de chaves

Os exemplos deste tópico usam a API do AWS KMS para visualizar e alterar políticas de chaves do AWS KMS keys.

Para obter detalhes sobre como usar políticas de chaves, políticas do IAM e concessões para gerenciar o acesso às suas chaves do KMS, consulte Autenticação e controle de acesso para o AWS KMS. Para ajuda sobre como escrever e formatar um documento de política JSON, consulte aReferência a políticas JSON do IAM, no Manual do usuário do IAM.

Tópicos

- Listar nomes de política de chaves
- Obter uma política de chaves
- Definir uma política de chaves

Listar nomes de política de chaves

Para obter os nomes das principais políticas de umAWS KMS key, use a ListKeyPoliciesoperação. O único nome de política de chaves que ela retorna é padrão.

Em linguagens que exigem um objeto cliente, esses exemplos usam o objeto cliente do AWS KMS criado em Criar um cliente.

Java

Para obter detalhes sobre a implementação do Java, consulte o listKeyPolicies método na Referência AWS SDK for Java da API.

```
// 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#

Para obter detalhes, consulte o Método ListKeyPolicies no 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

Para obter detalhes, consulte o Método `list_key_policies` no 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

Para obter detalhes, consulte o método de instância `list_key_policies` no 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

Para obter detalhes, consulte o Método ListKeyPolicies no 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

Para obter detalhes, consulte a listKeyPolicies propriedade no AWSSDK JavaScript em 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

Para listar o nome da política de chaves padrão, use o cmdlet Get-KMS KeyPolicyList.

```
# 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
```

Para usar os AWS KMS PowerShell cmdlets, instale o AWS.Tools.KeyManagementServicemódulo. Para obter mais informações, consulte o AWS Tools for Windows PowerShellGuia do Usuário.

Obter uma política de chaves

Para obter a política de chaves para umAWS KMS key, use a GetKeyPolicyoperação.

GetKeyPolicy requer um nome de política. O único nome de política válido é padrão.

Em linguagens que exigem um objeto cliente, esses exemplos usam o objeto cliente do AWS KMS criado em Criar um cliente.

Java

Para obter detalhes, consulte o getKeyPolicy método na Referência AWS SDK for Java da API.

```
// 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#

Para obter detalhes, consulte o Método GetKeyPolicy no 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

Para obter detalhes, consulte o Método `get_key_policy` no 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

Para obter detalhes, consulte o método de instância `get_key_policy` no 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

Para obter detalhes, consulte o Método GetKeyPolicy no 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

Para obter detalhes, consulte a getKeyPolicy propriedade no AWSSDK JavaScript em 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

Para obter a política de chaves para uma chave KMS, use o cmdlet KeyPolicyGet-KMS. Esse cmdlet retorna a política de chaves como uma string (System.String) que você pode usar em um comando KeyPolicyWrite-KMS (). `PutKeyPolicy` Para converter as políticas na string JSON em `PSCustomObject` objetos, use o cmdlet ConvertFrom-JSON.

```
# 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
```

Para usar os AWS KMS PowerShell cmdlets, instale o AWS.Tools.KeyManagementServicemódulo. Para obter mais informações, consulte o AWS Tools for Windows PowerShellGuia do Usuário.

Definir uma política de chaves

Para criar ou substituir a política de chaves de uma chave KMS, use a PutKeyPolicyoperação.

`PutKeyPolicy` exige um nome de política. O único nome de política válido é padrão.

Em linguagens que exigem um objeto cliente, esses exemplos usam o objeto cliente do AWS KMS criado em Criar um cliente.

Java

Para obter detalhes, consulte o putKeyPolicy método na Referência AWS SDK for Java da API.

```
// 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#

Para obter detalhes, consulte o Método PutKeyPolicy no 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

Para obter detalhes, consulte o Método put_key_policy no 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

Para obter detalhes, consulte o método de instância put_key_policy no 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

Para obter detalhes, consulte o Método PutKeyPolicy no 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

Para obter detalhes, consulte a putKeyPolicy propriedade no AWSSDK JavaScript em 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

Para definir uma política de chaves para uma chave KMS, use o cmdlet KeyPolicyWrite-KMS. Este cmdlet não retorna nenhuma saída. Para verificar se o comando foi efetivo, use o cmdlet Get-KMS KeyPolicy.

O parâmetro `Policy` utiliza uma string. Coloque a string entre aspas simples para torná-la uma string literal. Não é necessário usar caracteres de continuação ou caracteres de escape na string literal.

```
# 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
```

Para usar os AWS KMS PowerShell cmdlets, instale o AWS.Tools.KeyManagementServicemódulo. Para obter mais informações, consulte o Guia do usuário da AWS Tools for Windows PowerShell.

Trabalhar com concessões

Os exemplos deste tópico usam a API do AWS KMS para criar, visualizar, retirar e revogar concessões em AWS KMS keys. Para obter mais detalhes sobre como usar concessões no AWS KMS, consulte Concessões no AWS KMS.

Tópicos

- Criar uma concessão
- Visualizar uma concessão
- Remover uma concessão

- Revogar uma concessão

Criar uma concessão

Para criar uma concessão para umAWS KMS key, use a CreateGrantoperação. A resposta inclui apenas o ID de concessão e o token de concessão. Para obter informações detalhadas sobre a concessão, use a ListGrantsoperação, conforme mostrado emVisualizar uma concessão.

Esses exemplos criam uma concessão que permite que os usuários que podem assumir a `ExampleKeyUser` função chamem a GenerateDataKeyoperação na chave KMS identificada pelo `KeyId` parâmetro.

Em linguagens que exigem um objeto cliente, esses exemplos usam o objeto cliente do AWS KMS criado em Criar um cliente.

Java

Para obter detalhes, consulte o Método createGrant, na Referência de APIs do 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#

Para obter detalhes, consulte o Método CreateGrant no 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

Para obter detalhes, consulte o Método `create_grant` no 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

Para obter detalhes, consulte o método de instância `create_grant` no 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

Para obter detalhes, consulte o Método CreateGrant no 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

Para obter detalhes, consulte a propriedade createGrant no SDK JavaScript em 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

Para criar uma concessão, use o 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
```

Para usar os AWS KMS PowerShell cmdlets, instale o AWS.Tools.KeyManagementServicemódulo. Para obter mais informações, consulte o AWS Tools for Windows PowerShellGuia do Usuário.

Visualizar uma concessão

Para obter informações detalhadas sobre as concessões em uma chave KMS, use a ListGrantsoperação.

> **Note**
>
> O campo `GranteePrincipal` na resposta `ListGrants` geralmente contém o principal favorecido da concessão. No entanto, quando a entidade principal receptora na concessão é um serviço da AWS, o campo `GranteePrincipal` contém a entidade principal de serviço, que pode representar várias entidades principais entidade receptoras de concessão diferentes.

Em linguagens que exigem um objeto cliente, esses exemplos usam o objeto cliente do AWS KMS criado em Criar um cliente.

Esses exemplos usam o parâmetro `Limits` opcional, que determina o número de concessões que a operação retorna.

Java

Para obter detalhes sobre a implementação de Java, consulte o Método listGrants, na Referência de APIs do 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#

Para obter detalhes, consulte o Método ListGrants no 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

Para obter detalhes, consulte o Método `list_grants` no 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

Para obter detalhes, consulte o método de instância `list_grants` no 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

Para obter detalhes, consulte o Método ListGrants no 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

Para obter detalhes, consulte a propriedade listGrants no AWSSDK em Node.js. JavaScript

```
// 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

Para ver os detalhes de todas as AWS KMS concessões de uma chave KMS, use o cmdlet GrantListGet-KMS.

Para limitar o número de objetos de saída, este exemplo usa o cmdlet Select-Object em vez do parâmetro `Limit`, que está defasado nos cmdlets da lista. Para obter ajuda com a saída da paginação no AWS Tools for PowerShell, consulte Paginação de saída com o 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
```

Para usar os AWS KMS PowerShell cmdlets, instale o AWS.Tools.KeyManagementServicemódulo. Para obter mais informações, consulte o AWS Tools for Windows PowerShellGuia do Usuário.

Você deve especificar a chave do KMS em todas as operações `ListGrants`. No entanto, você pode filtrar ainda mais a lista de concessões especificando o ID de concessão ou a entidade principal receptora da concessão. Os exemplos a seguir obtêm apenas as concessões para uma chave do KMS e que a função `test-engineer` é a entidade principal receptora da concessão.

Java

Para obter detalhes sobre a implementação de Java, consulte o Método listGrants, na Referência de APIs do 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#

Para obter detalhes, consulte o Método ListGrants no 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

Para obter detalhes, consulte o Método `list_grants` no 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

Para obter detalhes, consulte o método de instância `list_grants` no 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

Para obter detalhes, consulte o Método ListGrants no 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

Para obter detalhes, consulte a propriedade listGrants no AWSSDK em Node.js. JavaScript

```
// 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

Para ver os detalhes de todas as AWS KMS concessões de uma chave KMS, use o cmdlet GrantListGet-KMS.

```
# 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
```

Para usar os AWS KMS PowerShell cmdlets, instale o AWS.Tools. KeyManagementServicemódulo. Para obter mais informações, consulte o AWS Tools for Windows PowerShellGuia do Usuário.

Remover uma concessão

Para retirar uma concessão para uma chave KMS, use a RetireGrantoperação. Você deve remover uma concessão para limpá-la depois de terminar de usá-la.

Para retirar uma concessão, forneça o token da concessão ou o ID de concessão e o ID da chave do KMS. Para essa operação, o ID da chave do KMS deve ser o Amazon Resource Name (ARN) da chave do KMS. O token de concessão é retornado pela CreateGrantoperação. O ID da concessão é retornado pelas ListGrantsoperações CreateGrant e.

RetireGrant não retorna uma resposta. Para verificar se foi eficaz, use a ListGrantsoperação.

Em linguagens que exigem um objeto cliente, esses exemplos usam o objeto cliente do AWS KMS criado em Criar um cliente.

Java

Para obter detalhes, consulte o Método retireGrant, na Referência de APIs do AWS SDK for Java.

```
// Retire a grant
//
String grantToken = Place your grant token here;

RetireGrantRequest req = new RetireGrantRequest().withGrantToken(grantToken);
```

```
kmsClient.retireGrant(req);
```

C#

Para obter detalhes, consulte o Método RetireGrant no AWS SDK for .NET.

```
// Retire a grant
//
String grantToken = "Place your grant token here";

RetireGrantRequest retireGrantRequest = new RetireGrantRequest()
{
    GrantToken = grantToken
};
kmsClient.RetireGrant(retireGrantRequest);
```

Python

Para obter detalhes, consulte o Método `retire_grant` no AWS SDK for Python (Boto3).

```
# Retire a grant

grant_token = Place your grant token here

response = kms_client.retire_grant(
    GrantToken=grant_token
)
```

Ruby

Para obter detalhes, consulte o método de instância `retire_grant` no AWS SDK for Ruby.

```
# Retire a grant

grant_token = Place your grant token here

response = kmsClient.retire_grant({
  grant_token: grant_token
})
```

PHP

Para obter detalhes, consulte o Método RetireGrant no AWS SDK for PHP.

```
// Retire a grant
//
$grantToken = 'Place your grant token here';

$result = $KmsClient->retireGrant([
    'GrantToken' => $grantToken,
]);
```

Node.js

Para obter detalhes, consulte a propriedade retireGrant no SDK JavaScript em AWS Node.js.

```
// Retire a grant
//
const GrantToken = 'Place your grant token here';
kmsClient.retireGrant({ GrantToken }, (err, data) => {
  ...
});
```

PowerShell

Para retirar uma concessão, use o cmdlet Disable-KMSGrant. Para obter o token de concessão, use o cmdlet New-KMSGrant. O parâmetro `GrantToken` usa uma string, portanto, não é necessário converter a saída retornada pelo cmdlet Read-Host.

```
# Retire a grant

$grantToken = Read-Host -Message Place your grant token here
Disable-KMSGrant -GrantToken $grantToken
```

Para usar os AWS KMS PowerShell cmdlets, instale o AWS.Tools.KeyManagementServicemódulo. Para obter mais informações, consulte o AWS Tools for Windows PowerShellGuia do Usuário.

Revogar uma concessão

Para revogar uma concessão para uma chave KMS, use a RevokeGrantoperação. Você pode revogar uma concessão para negar explicitamente as operações que dependem dela.

Em linguagens que exigem um objeto cliente, esses exemplos usam o objeto cliente do AWS KMS criado em Criar um cliente.

Java

Para obter detalhes, consulte o Método revokeGrant, na Referência de APIs do 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#

Para obter detalhes, consulte o Método RevokeGrant no 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);
```

Para usar os AWS KMS PowerShell cmdlets, instale o AWS.Tools.KeyManagementServicemódulo. Para obter mais informações, consulte o AWS Tools for Windows PowerShellGuia do Usuário.

Python

Para obter detalhes, consulte o Método `revoke_grant` no 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

Para obter detalhes, consulte o método de instância `revoke_grant` no 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

Para obter detalhes, consulte o Método RevokeGrant no 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

Para obter detalhes, consulte a propriedade revokeGrant no SDK JavaScript em AWS Node.js.

```
// 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

Para revogar uma concessão, use o 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
```

Para usar os AWS KMS PowerShell cmdlets, instale o AWS.Tools.KeyManagementServicemódulo. Para obter mais informações, consulte o Guia do usuário da AWS Tools for Windows PowerShell.

Como testar suas chamadas de API do AWS KMS

Para usar o AWS KMS, você deve ter credenciais que a AWS possa usar para autenticar suas solicitações de API. As credenciais devem incluir permissões para acessar chaves KMS e aliases. As permissões são determinadas pelas política de chave, políticas do IAM, concessões e controles de acesso entre contas. Além de controlar o acesso às chaves KMS, é possível controlar o acesso ao seu CloudHSM e aos seus repositórios de chaves personalizados.

É possível especificar o parâmetro da API `DryRun` para verificar se você tem as permissões necessárias para usar as chaves do AWS KMS. Também é possível usar `DryRun` para verificar se os parâmetros de solicitação em uma chamada de API do AWS KMS estão especificados corretamente.

Tópicos

- Qual é o DryRun parâmetro?
- Especificando DryRun com a API

Qual é o DryRun parâmetro?

`DryRun` é um parâmetro de API opcional que você especifica para verificar se as chamadas da API do AWS KMS serão bem-sucedidas. Use `DryRun` para testar sua chamada de API, antes de realmente fazer a chamada para o AWS KMS. É possível verificar o seguinte:

- Que você tem as permissões necessárias para usar as chaves do AWS KMS.
- Que você especificou os parâmetros na chamada corretamente.

AWS KMS oferece suporte ao uso do parâmetro `DryRun` em determinadas ações da API:

- CreateGrant
- Decrypt

- Encrypt
- GenerateDataKey
- GenerateDataKeyPair
- GenerateDataKeyPairWithoutPlaintext
- GenerateDataKeyWithoutPlaintext
- GenerateMac
- ReEncrypt
- RetireGrant
- RevokeGrant
- Sign
- Verificar
- VerifyMac

O uso do parâmetro `DryRun` incorrerá em cobranças e será cobrado como uma solicitação de API padrão. Para obter mais informações sobre os preços do AWS KMS, consulte Definição de preço do AWS Key Management Service.

Todas as solicitações de API que usam o parâmetro `DryRun` se aplicam à cota de solicitações da API e podem resultar em uma exceção de controle de utilização se você exceder a cota de solicitação da API. Por exemplo, chamar Decrypt com `DryRun` ou sem `DryRun` conta na mesma cota de operações criptográficas. Para saber mais, consulte Solicitações de AWS KMS limitação.

Toda chamada para uma operação de API do AWS KMS é capturada como um evento e gravada em um log do AWS CloudTrail. A saída de qualquer operação que especifique o `DryRun` parâmetro aparece no seu CloudTrail registro. Para ter mais informações, consulte Registrando chamadas de AWS KMS API com AWS CloudTrail.

Especificando DryRun com a API

Para usar `DryRun`, especifique o parâmetro `–dry-run` nos comandos AWS CLI e chamadas de API do AWS KMS compatíveis com o parâmetro. Ao fazer isso, o AWS KMS verificará se sua chamada será bem-sucedida. As chamadas do AWS KMS que usam `DryRun` sempre falharão e retornarão uma mensagem com informações sobre o motivo pelo qual a chamada falhou. A mensagem pode incluir as seguintes exceções:

- `DryRunOperationException` - A solicitação seria bem-sucedida se `DryRun` não estivesse especificada.
- `ValidationException` - A solicitação falhou devido à especificação de um parâmetro de API incorreto.
- `AccessDeniedException` - Você não tem permissões para realizar a ação de API especificada no recurso KMS.

Por exemplo, o comando a seguir usa a CreateGrantoperação e cria uma concessão que permite que os usuários autorizados a assumir a `keyUserRole` função chamem a operação Decrypt em uma chave KMS simétrica especificada. O parâmetro `DryRun` está especificado.

```
$  aws kms create-grant \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --grantee-principal arn:aws:iam::111122223333:role/keyUserRole \
    --operations Decrypt \
    --dry-run
```

Consistência eventual do AWS KMS

A API do AWS KMS segue um modelo de consistência eventual devido à natureza distribuída do sistema. Como resultado, as alterações nos recursos do AWS KMS poderão não ser imediatamente visíveis para os comandos subsequentes que forem executados.

Quando você realiza chamadas da API do AWS KMS, pode haver um breve atraso antes que a alteração esteja disponível em todo o AWS KMS. Normalmente, a alteração leva menos de alguns segundos para se propagar por todo o sistema, mas, em alguns casos, pode levar vários minutos. Você poderá receber erros inesperados, como `NotFoundException` ou `InvalidStateException`, durante esse período. Por exemplo, o AWS KMS pode retornar um `NotFoundException` se você chamar `GetParametersForImport` imediatamente após chamar `CreateKey`.

Recomendamos que você configure uma estratégia de repetição em seus clientes do AWS KMS para repetir automaticamente as operações após um breve período de espera. Para obter mais informações, consulte Comportamento de repetição nos SDKs AWS e no Guia de referência de ferramentas.

Para chamadas de API relacionadas a concessões, é possível usar um token de concessão para evitar possíveis atrasos e usar as permissões em uma concessão imediatamente. Para obter informações, consulte Eventual consistency (for grants) (Consistência eventual (para concessões)).

Referências

As referências a seguir fornecem informações úteis sobre o uso e o gerenciamento de chaves do KMS.

- Referência do tipo de chave. Lista o tipo de chave do KMS que oferece suporte a cada operação da API do AWS KMS.

  Para encontrar: posso habilitar e desabilitar uma chave do KMS de assinatura RSA?

- Tabela de estados de chaves. Mostra como o estado da chave de uma chave do KMS afeta seu uso em operações de API do AWS KMS.

  Para encontrar: posso alterar o alias de uma chave do KMS cuja exclusão está pendente?

- Referência de permissões da API do AWS KMS. Fornece informações sobre as permissões necessárias para cada operação da API do AWS KMS.

  Para descobrir: Posso GetKeyPolicyusar uma chave em uma AWS conta diferente? Posso conceder a permissão `kms:Decrypt` em uma política do IAM?

  - ViaService referência. Lista os serviços da AWS que oferecem suporte à chave de condição `kms:ViaService`.

    Para descobrir: Posso usar a chave de `kms:ViaService` condição para permitir uma permissão somente quando ela vem da Amazon ElastiCache? E o Amazon Neptune?

- Definição de preço do AWS KMS Lista e explica o preço das chaves do KMS.

  Para encontrar: quanto custa para usar minhas chaves assimétricas?

- Cotas de solicitações do AWS KMS. Lista as cotas por segundo para solicitações de API do AWS KMS em cada conta e região.

  Para encontrar: quantas solicitações Decrypt posso executar em cada segundo? Quantas solicitações Decrypt posso executar em chaves do KMS no meu armazenamento de chaves personalizado?

- Cotas de recursos do AWS KMS. Lista as cotas nos recursos da AWS KMS.

  Para encontrar: quantas chaves KMS posso ter em cada região da minha conta? Quantos aliases posso ter em cada chave do KMS?

- Serviços da AWS integrados ao AWS KMS. Lista os serviços da AWS que usam chaves do KMS para proteger os recursos que eles criam, armazenam e gerenciam.

  Para encontrar: o Amazon Connect usa chaves do KMS para proteger meus recursos do Connect?

Histórico do documento

Este tópico descreve atualizações importantes no Guia do desenvolvedor do AWS Key Management Service .

Tópicos

- Atualizações recentes
- Atualizações anteriores

Atualizações recentes

A tabela a seguir descreve alterações significativas nesta documentação desde janeiro de 2018. Além das principais alterações listadas aqui, também atualizamos a documentação com frequência para melhorar as descrições e os exemplos e abordar os comentários que você nos envia. Para ser notificado sobre alterações significativas, inscreva-se no feed RSS.

Talvez seja necessário rolar horizontalmente ou verticalmente para ver todos os dados nessa tabela.

Alteração	Descrição	Data
Atualizações na rotação de chaves	Foi adicionado suporte para períodos de rotação personalizados para rotações automáticas de chaves, rotações de chaves sob demanda e visibilidade das rotações de materiais-chave.	12 de abril de 2024
Atualizações da política gerenciada	Novas permissões adicionadas permitem AWS KMS monitorar as alterações na VPC que contém seu AWS CloudHSM cluster para que AWS KMS possa fornecer mensagens de erro claras em caso de falhas. `AWSKeyMan`	10 de novembro de 2023

	`agementServiceCust omKeyStoresService RolePolicy`	
Atualização de recurso	Foi adicionado suporte para o parâmetro da API `DryRun`.	5 de julho de 2023
Atualização de recurso	Foi adicionado suporte para importar material de chaves para todos os tipos de AWS KMS chaves, exceto lojas de chaves personalizadas.	5 de junho de 2023
Atualização de recurso	Atualizações nas AWS KMS APIs para Nitro Enclaves	10 de março de 2023
Atualização de recurso	O algoritmo de `RSAES_PKCS1_V1_5` empacotamento está obsoleto. AWS KMS encerrará todo o suporte até 1º de outubro de 2023, de acordo com as diretrizes de gerenciamento de chaves criptográficas do Instituto Nacional de Padrões e Tecnologia (NIST). Recomendamos que você comece a usar um algoritmo de empacotamento diferente imediatamente.	28 de fevereiro de 2023
Atualização de recurso	Foi adicionado suporte para armazenamentos externos de chaves, um recurso que permite proteger seus AWS recursos usando chaves criptográficas externas. AWS	29 de novembro de 2022

Alteração de cota	Aumentamos a cota de AWS KMS keys recursos para 100.000 chaves KMS em cada conta e região.	8 de julho de 2022
Atualização de recursos	Foi adicionado suporte para chaves HMAC KMS em mais Regiões da AWS	8 de julho de 2022
Novo tópico	O AWS Key Management Service tópico Resiliência foi adicionado ao capítulo Segurança do Guia do AWS KMS Desenvolvedor.	14 de junho de 2022
Novo atributo	Foi adicionado suporte para AWS KMS chaves e operações de API que geram e verificam códigos HMAC.	19 de abril de 2022
Alteração na documentação	Substituição da condição chave mestra do cliente (CMK) porAWS KMS key e chave do KMS.	30 de agosto de 2021
Novo recurso	Suporte adicionado para chaves de várias regiões, um conjunto de chaves do KMS interoperáveis em regiões diferentes que têm o mesmo ID de chave e material de chave. É possível usar chaves de várias regiões para criptografar dados em uma região e descriptografar dados em uma região diferente.	8 de junho de 2021

Novo recurso	Suporte adicionado para controle de acesso baseado em atributos (ABAC). Você pode usar tags e aliases para controlar o acesso ao seu AWS KMS keys.	17 de dezembro de 2020
Novo recurso	Adicionado suporte para políticas de endpoint da VPC.	9 de julho de 2020
Novo conteúdo	Explica as propriedades de segurança do AWS KMS.	18 de junho de 2020
Novo recurso	Foi adicionado suporte para chaves de dados assimétricas AWS KMS keys e assimétri cas.	25 de novembro de 2019
Recurso atualizado	Você pode ver a política de chaves do Chaves gerenciad as pela AWS no AWS KMS console. Esse recurso costumava ser limitado a chaves gerenciadas pelo cliente.	15 de novembro de 2019
Novo recurso	Explica como usar algoritmos de troca de chave pós-quânt ica híbrida no TLS para suas chamadas para o AWS KMS.	4 de novembro de 2019
Alteração de cota	Aumento das cotas de recursos para algumas APIs que gerenciam chaves do KMS.	18 de setembro de 2019

Alteração de cota	Alteradas as cotas de recursos para chaves do KMS, aliases e concessões por chave do KMS.	27 de março de 2019
Alteração de cota	Alterada a cota de solicitações compartilhadas por segundo para operações de criptografia que usam AWS KMS keys em um armazenamento de chaves personalizado.	7 de março de 2019
Novo recurso	Explica como criar e gerenciar armazenamentos de chaves AWS KMS personalizadas. Cada armazenamento de chaves é apoiado por um AWS CloudHSM cluster que você possui e controla.	26 de novembro de 2018
Novo console	Explica como usar o novo AWS KMS console, que é independente do console do IAM. O console original e as instruções para usá-lo permanecerão disponíveis por um breve período para que você tenha tempo para se familiarizar com o novo console.	7 de novembro de 2018
Alteração de cota	Alterou a cota de solicitações compartilhadas para uso de AWS KMS keys.	21 de agosto de 2018

Novo conteúdo	Explica como AWS Secrets Manager usa AWS KMS chaves para criptografar o valor secreto em um segredo.	13 de julho de 2018
Novo conteúdo	Explica como o DynamoDB usa o AWS KMS AWS KMS keys para dar suporte à opção de criptografia no lado do servidor.	23 de maio de 2018
Novo recurso	Explica como usar um endpoint privado em sua VPC para se conectar diretamente AWS KMS, em vez de se conectar pela Internet.	22 de janeiro de 2018

Atualizações anteriores

A tabela a seguir descreve as mudanças importantes no Guia do AWS Key Management Service desenvolvedor antes de 2018.

Talvez seja necessário rolar horizontalmente ou verticalmente para ver todos os dados nessa tabela.

Alteração	Descrição	Data
Novo conteúdo	Documentação adicionada sobre Marcar chaves com tags.	15 de fevereiro de 2017
Novo conteúdo	Documentação adicionada sobre Como monitorar o AWS KMS keys e Monitoramento com a Amazon CloudWatch.	31 de agosto de 2016

Alteração	Descrição	Data
Novo conteúdo	Documentação adicionada sobre Material de chave importado.	11 de agosto de 2016
Novo conteúdo	Adicionada a seguinte documentação: Políticas do IAM, Referência de permissões e Chaves de condição.	5 de julho de 2016
Atualizar	Partes da documentação atualizadas no capítulo Autenticação e controle de acesso.	5 de julho de 2016
Atualizar	Atualizada a página Cotas para refletir as novas cotas padrão.	31 de maio de 2016
Atualizar	Atualização da página Cotas para refletir novas cotas padrão e atualização da documentação sobre o token de concessão para aumentar a clareza e a precisão.	11 de abril de 2016
Novo conteúdo	Documentação adicionada sobre Permitir que diversas entidades principais do IAM acessem uma chave do KMS e Usar a condição de endereço IP.	17 de fevereiro de 2016

Alteração	Descrição	Data
Atualizar	Atualizadas as páginas Políticas-chave em AWS KMS e Alterar uma política de chaves para aumentar a clareza e a precisão.	17 de fevereiro de 2016
Atualizar	Atualizada a página de tópicos Gerenciar chaves do para aumentar a clareza.	5 de janeiro de 2016
Novo conteúdo	Documentação adicionada sobre Como o AWS CloudTrail usa o AWS KMS.	18 de novembro de 2015
Novo conteúdo	Adicionadas instruções para Alterar uma política de chaves.	18 de novembro de 2015
Atualizar	Documentação sobre Como o Amazon Relational Database Service (Amazon RDS) usa o AWS KMS atualizada.	18 de novembro de 2015
Novo conteúdo	Documentação adicionada sobre Como WorkSpaces usa AWS KMS.	6 de novembro de 2015
Atualizar	Atualizada a página Políticas -chave em AWS KMS para aumentar a clareza.	22 de outubro de 2015

Alteração	Descrição	Data
Novo conteúdo	Documentação adicionada sobre Excluir AWS KMS keys, inclusive a documentação de suporte sobre Criar um alarme e Determinar a utilização anterior de uma chave do KMS.	15 de outubro de 2015
Novo conteúdo	Documentação adicionada sobre Determinar acesso a AWS KMS keys.	15 de outubro de 2015
Novo conteúdo	Documentação adicionada sobre Principais estados das AWS KMS chaves.	15 de outubro de 2015
Novo conteúdo	Documentação adicionada sobre Como o Amazon Simple Email Service (Amazon SES) usa o AWS KMS.	1º de outubro de 2015
Atualizar	Atualização da página Cotas para explicar as novas cotas de solicitações.	31 de agosto de 2015
Novo conteúdo	Foram adicionadas informações sobre as cobranças de uso AWS KMS. Consulte Definição de preço do AWS KMS.	14 de agosto de 2015
Novo conteúdo	Foram adicionadas cotas de solicitação ao AWS KMS Cotas.	11 de junho de 2015

Alteração	Descrição	Data
Novo conteúdo	Adicionado um novo exemplo de código Java que demonstra o uso da operação `UpdateAlias` . Consulte Atualizar um alias.	1º de junho de 2015
Atualizar	A tabela de regiões do AWS Key Management Service foi movida para a Referência geral da AWS.	29 de maio de 2015
Novo conteúdo	Documentação adicionada sobre Como o Amazon EMR usa o AWS KMS.	28 de janeiro de 2015
Novo conteúdo	Documentação adicionad a sobre Como a Amazon WorkMail usa AWS KMS.	28 de janeiro de 2015
Novo conteúdo	Documentação adicionad a sobre Como o Amazon Relational Database Service (Amazon RDS) usa o AWS KMS.	6 de janeiro de 2015
Novo conteúdo	Documentação adicionada sobre Como o Amazon Elastic Transcoder usa o AWS KMS.	24 de novembro de 2014
Novo guia	Introdução do Guia do desenvolvedor do AWS Key Management Service .	12 de novembro de 2014

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.