# Table of Contents

What is AWS Key Management Service? ................................................................. 1  
Concepts .................................................................................................................. 2  
  Customer Master Keys ......................................................................................... 2  
  Data Keys .......................................................................................................... 2  
  Envelope Encryption .......................................................................................... 3  
  Encryption Context .............................................................................................. 3  
  Key Policies ......................................................................................................... 4  
  Grants ................................................................................................................... 4  
  Grant Tokens ....................................................................................................... 4  
  Auditing CMK Usage .......................................................................................... 4  
  Key Management Infrastructure ......................................................................... 4  
Getting Started ..................................................................................................... 5  
  Creating Keys ........................................................................................................ 5  
    Creating CMKs (Console) .................................................................................. 5  
    Creating CMKs (API) ..................................................................................... 6  
  Viewing Keys ....................................................................................................... 7  
    Viewing CMKs (Console) ................................................................................ 7  
    Viewing CMKs (API) ..................................................................................... 9  
    Finding the Key ID and ARN ........................................................................... 10  
  Editing Keys ......................................................................................................... 11  
    Editing CMKs (console) .................................................................................. 12  
    Editing CMKs (API) ..................................................................................... 15  
  Tagging Keys ....................................................................................................... 16  
    Managing CMK Tags (Console) ..................................................................... 16  
    Managing CMK Tags (API) ........................................................................... 17  
  Enabling and Disabling Keys ............................................................................. 18  
    Enabling and Disabling CMKs (Console) ......................................................... 18  
    Enabling and Disabling CMKs (API) ............................................................... 19  
Authentication and Access Control ................................................................. 20  
  Authentication ..................................................................................................... 20  
  Access Control ................................................................................................. 21  
  Overview of Managing Access ......................................................................... 21  
    AWS KMS Resources and Operations ............................................................ 22  
    Managing Access to AWS KMS CMKs ............................................................ 22  
    Specifying Permissions in a Policy .................................................................. 23  
    Specifying Conditions in a Policy .................................................................. 24  
  Using Key Policies ............................................................................................... 24  
    Overview of Key Policies ................................................................................ 24  
    Default Key Policy ......................................................................................... 25  
    Example Key Policy ....................................................................................... 31  
    Modifying a Key Policy .................................................................................... 34  
    Keeping Key Policies Up to Date .................................................................... 38  
  Using IAM Policies ............................................................................................. 40  
    Overview of IAM Policies ............................................................................. 40  
    Permissions Required to Use the AWS KMS Console .................................... 41  
    AWS Managed (Predefined) Policies for AWS KMS ..................................... 41  
    Customer Managed Policy Examples ............................................................. 41  
AWS KMS API Permissions Reference ............................................................. 43  
  Using Policy Conditions ..................................................................................... 47  
    AWS Condition Keys ....................................................................................... 48  
    AWS KMS Condition Keys ............................................................................ 49  
  Using Grants ....................................................................................................... 57  
  Determining Access ......................................................................................... 57  
  Understanding Policy Evaluation ....................................................................... 58
Requests per second: varies ................................................................. 182
What is AWS Key Management Service?

AWS Key Management Service (AWS KMS) is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data. AWS KMS is integrated with other AWS services including Amazon Elastic Block Store (Amazon EBS), Amazon Simple Storage Service (Amazon S3), Amazon Redshift, Amazon Elastic Transcoder, Amazon WorkMail, Amazon Relational Database Service (Amazon RDS), and others to make it simple to encrypt your data with encryption keys that you manage. AWS KMS is also integrated with AWS CloudTrail to provide you with key usage logs to help meet your auditing, regulatory and compliance needs.

AWS KMS lets you create master keys that can never be exported from the service and which can be used to encrypt and decrypt data based on policies you define.

You can perform the following management actions on master keys by using AWS KMS:

- Create, describe, and list master keys
- Enable and disable master keys
- Set and retrieve master key usage policies (access control)
- Create, delete, list, and update aliases, which are friendly names that point to your master keys
- Delete master keys to complete the key lifecycle

With AWS KMS you can also perform the following cryptographic functions using master keys:

- Encrypt, decrypt, and re-encrypt data
- Generate data encryption keys that you can export from the service in plaintext or encrypted under a master key that doesn't leave the service
- Generate random numbers suitable for cryptographic applications

By using AWS KMS, you gain more control over access to data you encrypt. You can use the key management and cryptographic features directly in your applications or through AWS services that are integrated with AWS KMS. Whether you are writing applications for AWS or using AWS services, AWS KMS enables you to maintain control over who can use your master keys and gain access to your encrypted data.

AWS KMS is integrated with AWS CloudTrail, a service that delivers log files to an Amazon S3 bucket that you designate. By using CloudTrail you can monitor and investigate how and when your master keys have been used and by whom.

For a more detailed introduction to AWS KMS, see AWS KMS Concepts (p. 2).

To learn more about how AWS KMS uses cryptography and secures master keys, see the AWS Key Management Service Cryptographic Details whitepaper.

AWS KMS Pricing

As with other AWS products, there are no contracts or minimum commitments for using AWS KMS. For more information about AWS KMS pricing, see AWS Key Management Service Pricing.
AWS Key Management Service Concepts

Learn the basic terms and concepts in AWS Key Management Service (AWS KMS) and how they work together to help protect your data.

Topics
- Customer Master Keys (p. 2)
- Data Keys (p. 2)
- Envelope Encryption (p. 3)
- Encryption Context (p. 3)
- Key Policies (p. 4)
- Grants (p. 4)
- Grant Tokens (p. 4)
- Auditing CMK Usage (p. 4)
- Key Management Infrastructure (p. 4)

Customer Master Keys

The primary resources in AWS KMS are customer master keys (CMKs). CMKs are either customer managed or AWS managed. You can use either type of CMK to protect up to 4 kilobytes (4096 bytes) of data directly. Typically you use CMKs to protect data encryption keys (or data keys) which are then used to encrypt or decrypt larger amounts of data outside of the service. CMKs never leave AWS KMS unencrypted, but data keys can. AWS KMS does not store, manage, or track your data keys.

There is one AWS managed CMK for each service that is integrated with AWS KMS (p. 96). When you create an encrypted resource in these services, you can choose to protect that resource under the AWS managed CMK for that service. This CMK is unique to your AWS account and the AWS region in which it is used, and it protects the data keys used by the AWS services to protect your data.

Many of these services allow you to specify a customer managed CMK instead of the AWS managed CMK. This is useful when you need more granular control over the CMK. For example, when you use a customer managed CMK with these services you can enable automatic rotation (p. 64) of the CMK's key material every year. You cannot do this with an AWS managed CMK.

Data Keys

You use data keys to encrypt large data objects within your own application outside AWS KMS. When you make a GenerateDataKey API request, AWS KMS returns a plaintext copy of the data key and a ciphertext that contains the data key encrypted under the specified CMK. You use the plaintext data key in your application to encrypt data, and you typically store the encrypted data key alongside your encrypted data. Security best practices dictate that you should remove the plaintext data key from memory as soon as practical after use. To decrypt data in your application, you pass the encrypted data key with a Decrypt API request. AWS KMS uses your CMK to decrypt the data key into plaintext, and then returns it to you. You use the plaintext data key to decrypt your data and then remove the plaintext data key from memory as soon as practical after use.

Note
You can use AWS KMS to generate, encrypt, and decrypt data keys, but AWS KMS does not store, manage, or track your data keys. You must do this inside your application.
Envelope Encryption

AWS KMS uses envelope encryption to protect data. Envelope encryption is the practice of encrypting plaintext data with a unique data key, and then encrypting the data key with a key encryption key (KEK). You might choose to encrypt the KEK with another KEK, and so on, but eventually you must have a master key. The master key is an unencrypted (plaintext) key with which you can decrypt one or more other keys.

Envelope encryption offers several benefits:

- **Protecting data keys**
  
  When you encrypt a data key, you don’t have to worry about where to store the encrypted data key, because the security of that data key is inherently protected by encryption. You can safely store the encrypted data key alongside the encrypted data.

- **Encrypting the same data under multiple master keys**
  
  Encryption operations can be time consuming, particularly when the data being encrypted are large objects. Instead of reencrypting raw data multiple times with different keys, you can reencrypt only the data keys that protect the raw data.

- **Combining the strengths of multiple algorithms**
  
  In general, symmetric key algorithms are faster and produce smaller ciphertexts than public key algorithms, but public key algorithms provide inherent separation of roles and easier key management. You might want to combine the strengths of each.

The following image provides an overview of envelope encryption. In this scenario, the data key is encrypted with a single KEK, which is the master key. In AWS KMS, your CMK represents the master key.

![Envelope Encryption Diagram]

Encryption Context

All AWS KMS cryptographic operations accept an optional set of key–value pairs that can contain additional contextual information about the data. This set of key–value pairs is called encryption context. When encryption context is used with an encryption operation, the encryption context for the corresponding decryption operation must match for the decryption to succeed. Encryption context is not secret. Encryption context is logged, and you can use it for auditing and when controlling access to AWS KMS API operation. For more information, see Encryption Context (p. 175).
Key Policies

When you create a CMK, you choose who can manage or use that CMK. These permissions are contained in a document called the key policy. You can use the key policy to add, remove, or modify permissions at any time for a customer-managed CMK, but you cannot edit the key policy for an AWS-managed CMK. For more information, see Authentication and Access Control for AWS KMS (p. 20).

Grants

A grant is another mechanism for providing permissions, an alternative to the key policy. You can use grants to give long-term access that allows AWS principals to use your customer-managed CMKs. For more information, see Using Grants (p. 57).

Grant Tokens

When you create a grant, the permissions specified in the grant might not take effect immediately due to eventual consistency. If you need to mitigate the potential delay, use the grant token that you receive in the response to your CreateGrant API request. You can pass the grant token with some AWS KMS API requests to make the permissions in the grant take effect immediately. The following AWS KMS API operations accept grant tokens:

- CreateGrant
- Decrypt
- DescribeKey
- Encrypt
- GenerateDataKey
- GenerateDataKeyWithoutPlaintext
- ReEncrypt
- RetireGrant

A grant token is not a secret. The grant token contains information about who the grant is for and therefore who can use it to cause the grant's permissions to take effect more quickly.

Auditing CMK Usage

You can use AWS CloudTrail to audit key usage. CloudTrail creates log files that contain a history of AWS API calls and related events for your account. These log files include all AWS KMS API requests made with the AWS Management Console, AWS SDKs, and command line tools, as well as those made through integrated AWS services. You can use these log files to get information about when the CMK was used, the operation that was requested, the identity of the requester, the IP address that the request came from, and so on. For more information, see Logging AWS KMS API Calls (p. 136) and the AWS CloudTrail User Guide.

Key Management Infrastructure

A common practice in cryptography is to encrypt and decrypt with a publicly available and peer-reviewed algorithm such as AES (Advanced Encryption Standard) and a secret key. One of the main problems with cryptography is that it's very hard to keep a key secret. This is typically the job of a key management infrastructure (KMI). AWS KMS operates the KMI for you. AWS KMS creates and securely stores your master keys, called CMKs. For more information about how AWS KMS operates, see the AWS Key Management Service Cryptographic Details whitepaper.
Getting Started

You can use the IAM section of the AWS Management Console to create, view, edit, tag, enable, disable, and delete customer master keys (CMKs) in AWS Key Management Service (AWS KMS). For more information, see the following topics.

Topics
• Creating Keys (p. 5)
• Viewing Keys (p. 7)
• Editing Keys (p. 11)
• Tagging Keys (p. 16)
• Enabling and Disabling Keys (p. 18)

Creating Keys

You can use the IAM section of the AWS Management Console to create a customer master key (CMK). You can also use the CreateKey operation in the AWS Key Management Service (AWS KMS) API.

Topics
• Creating CMKs (Console) (p. 5)
• Creating CMKs (API) (p. 6)

Creating CMKs (Console)

You can use the AWS Management Console to create customer master keys (CMKs).

To create a new CMK (console)

1. Sign in to the AWS Management Console and open the AWS Identity and Access Management (IAM) console at https://console.aws.amazon.com/iam/.
2. In the left navigation pane, choose Encryption keys.
3. For Region, choose the appropriate AWS Region. Do not use the region selector in the navigation bar (top right corner).
4. Choose Create key.
5. Type an alias for the CMK. An alias cannot begin with aws. Aliases that begin with aws are reserved by Amazon Web Services to represent AWS-managed CMKs in your account.

   An alias is a display name that you can use to identify the CMK. We recommend that you choose an alias that indicates the type of data you plan to protect or the application you plan to use with the CMK.

6. (Optional) Type a description for the CMK.

   We recommend that you choose a description that explains the type of data you plan to protect or the application you plan to use with the CMK.

7. Choose Next Step.
8. (Optional) Type a tag key and an optional tag value. To add more than one tag to the CMK, choose Add tag.
9. Choose Next Step.
10. Select which IAM users and roles can administer the CMK.

   **Note**
   The AWS account (root user) has full permissions by default. As a result, any IAM users and roles whose attached policies allow the appropriate permissions can also administer the CMK.

11. (Optional) To prevent the IAM users and roles that you chose in the previous step from deleting this CMK, clear the box at the bottom of the page for Allow key administrators to delete this key.
12. Choose Next Step.
13. Select which IAM users and roles can use the CMK to encrypt and decrypt data with the AWS KMS API.

   **Note**
   The AWS account (root user) has full permissions by default. As a result, any IAM users and roles whose attached policies allow the appropriate permissions can also use the CMK.

14. (Optional) You can use the controls at the bottom of the page to specify other AWS accounts that can use this CMK to encrypt and decrypt data. To do so, choose Add an External Account and then type the intended AWS account ID. Repeat as necessary to add more than one external account.

   **Note**
   Administrators of the external accounts must also allow access to the CMK by creating IAM policies for their users. For more information, see Allowing External AWS Accounts to Access a CMK (p. 37).

15. Choose Next Step.
16. Choose Finish to create the CMK.

   **Tip**
   To refer to your new CMK programmatically and in command line interface operations, you need a key ID or key ARN.
   The key ID is displayed in the Encryption keys section of the IAM console. To find the key ARN, in the Encryption keys section, choose the region, and then choose the CMK alias. You can also find the CMK ID and ARN by using the ListKeys operation in the AWS KMS API. For details, see Finding the Key ID and ARN (p. 10).

### Creating CMKs (API)

The `CreateKey` operation creates a new AWS KMS customer master key (CMK). These examples use the AWS Command Line Interface (AWS CLI), but you can use any supported programming language.

This operation has no required parameters. However, if you are creating a key with no key material, the `Origin` parameter is required. You might also want to use the `Policy` parameter to specify a key policy. You can change the key policy (`PutKeyPolicy`) and add optional elements, such as a `description` and `tags` at any time.

The following is an example of a call to the `CreateKey` operation with no parameters.

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

If you do not specify a key policy for your new CMK, the default key policy (p. 25) that CreateKey applies is different from the default key policy that the console applies when you use it to create a new CMK.

For example, this call to the GetKeyPolicy operation returns the key policy that CreateKey applies. It gives the AWS account root user access to the CMK and allows it to create AWS Identity and Access Management (IAM) policies for the CMK. For detailed information about IAM policies and key policies for CMKs, see Authentication and Access Control for AWS KMS (p. 20)

```
$ 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": "*"
        }
    ]
}
```

Viewing Keys

You can use the Encryption keys section of the AWS Management Console to view customer master keys (CMKs), including CMKs that you manage and CMKs that are managed by AWS. You can also use the operations in the AWS Key Management Service (AWS KMS) API, such as ListKeys and DescribeKey, to view CMKs.

Topics
- Viewing CMKs (Console) (p. 7)
- Viewing CMKs (API) (p. 9)
- Finding the Key ID and ARN (p. 10)

Viewing CMKs (Console)

You can see a list of your customer managed keys in the AWS Management Console.

To view your CMKs (console)

1. Sign in to the AWS Management Console and open the AWS Identity and Access Management (IAM) console at https://console.aws.amazon.com/iam/.

Viewing CMKs (Console)
2. In the left navigation pane, choose **Encryption keys**.
3. For **Region**, choose the appropriate AWS Region. Do not use the region selector in the navigation bar (top right corner).

The console shows all the CMKs in your AWS account in the chosen region, including customer-managed and AWS managed CMKs. The page displays the alias, key ID, status, and creation date for each CMK.

**To show additional columns in the list of CMKs**

1. Choose the settings button ( ) in the upper-right corner of the page.
2. Select the check boxes for the additional columns to show, and then choose **Close**.

**To show detailed information about the CMK**

The details include the Amazon Resource Name (ARN), description, key policy, tags, and key rotation settings of the CMK.

- Choose the alias of the CMK.

If the CMK does not have an alias, choose the empty cell in the **Alias** column, as shown in the following image.

**To find CMKs**

You can use the **Filter** box to find CMKs based on their aliases.

- In the **Filter** box, type all or part of the alias name of a CMK. Only the CMKs with alias names that match the filter appear.
You can use the AWS Key Management Service (AWS KMS) API to view your CMKs. This section demonstrates several operations that return details about existing CMKs. The examples use the AWS Command Line Interface (AWS CLI), but you can use any supported programming language.

Topics
- ListKeys: Get the ID and ARN of All CMKs (p. 9)
- DescribeKey: Get Detailed Information About a CMK (p. 10)
- GetKeyPolicy: Get the Key Policy Attached to a CMK (p. 10)

ListKeys: Get the ID and ARN of All CMKs

The ListKeys operation returns the ID and Amazon Resource Name (ARN) of all CMKs in the account and region. To see the aliases and key IDs of your CMKs that have aliases, use the ListAliases operation.

For example, this call to the ListKeys operation returns the ID and ARN of each CMK in this fictitious account.

```
$ 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-2:0987dcba-09fe-87dc-65ba-ab0987654321",
      "KeyId": "0987dcba-09fe-87dc-65ba-ab0987654321"
    },
    {
      "KeyArn": "arn:aws:kms:us-east-2:1234abcd-12ab-34cd-56ef-1234567890ab",
      "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    }
  ]
}
```
DescribeKey: Get Detailed Information About a CMK

The DescribeKey operation returns details about the specified CMK. To identify the CMK, use its key ID, key ARN, alias name, or alias ARN.

For example, this call to DescribeKey returns information about an existing CMK. The fields in the response vary with the key state and the key origin.

```bash
$ 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,
        "KeyUsage": "ENCRYPT_DECRYPT",
        "KeyState": "Enabled",
        "CreationDate": 1499988169.234,
        "Arn": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "AWSAccountId": "111122223333"
    }
}
```

GetKeyPolicy: Get the Key Policy Attached to a CMK

The GetKeyPolicy operation gets the key policy that is attached to the CMK. To identify the CMK, use its key ID or key ARN. You must also specify the policy name, which is always default. (If your output is difficult to read, add the --output text option to your command.)

```bash
$ 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" : "*"
    } ]
}
```

Finding the Key ID and ARN

To identify your AWS KMS CMKs in programs, scripts, and command line interface (CLI) commands, you use the ID of the CMK or its Amazon Resource Name (ARN). Some API operations also let you use the CMK alias.

To find the CMK ID and ARN (console)

2. For **Region**, choose the appropriate AWS region. Do not use the region selector in the navigation bar (top right corner).

   The page displays the key ID and alias, along with the status and creation date of each CMK.

   ![Key Actions](image)

   - For **Region**, choose the appropriate AWS region. Do not use the region selector in the navigation bar (top right corner).
   - The page displays the key ID and alias, along with the status and creation date of each CMK.

3. To find the CMK ARN (key ARN), choose the alias name. This opens a page of details that includes the key ARN.

   ![Summary](image)

   - To find the CMK ARN (key ARN), choose the alias name. This opens a page of details that includes the key ARN.

   **To find the CMK ID and ARN (API)**
   - To find the CMK ID and ARN, use the **ListKeys** (p. 9) operation (see above).

**Editing Keys**

You can use the key detail page of the **Encryption keys** section of the AWS Management Console to edit some of the properties of the customer master keys (CMKs) that you manage. You can change the description, add and remove administrators and users, manage tags, and enable and disable key rotation.

You can also use the operations in the **AWS Key Management Service (AWS KMS) API** to edit the CMKs that you manage. You cannot changes the properties of AWS managed CMKs.

**Topics**

- Editing CMKs (console) (p. 12)
- Editing CMKs (API) (p. 15)
Editing CMKs (console)

To edit a customer-managed CMK, start at the key details page for the CMK.

To view the key details page for a CMK (console)

1. Sign in to the AWS Management Console and open the AWS Identity and Access Management (IAM) console at https://console.aws.amazon.com/iam/.
2. In the left navigation pane, choose Encryption keys.
3. For Region, choose the appropriate AWS Region. Do not use the region selector in the navigation bar (top right corner).
4. Choose the alias of the CMK whose details you want to see.

   Note
   You cannot edit AWS managed CMKs, which are denoted by the orange AWS icon.

On the key details page, you can view metadata about the CMK, and you can edit the CMK in the following ways:

Change the description

In the Summary section, type a brief description of the CMK in the Description box. When you are finished, choose Save Changes.

Add and remove key administrators, and allow or disallow key administrators to delete the CMK

Use the controls in the Key Administrators area in the Key Policy section of the page.
Add and remove key users, and allow and disallow external AWS accounts to use the CMK

Use the controls in the Key Users area in the Key Policy section of the page.
Add, edit, and remove tags

Use the controls in the Tags section of the page.

Enable or disable rotation

Use the controls in the Key Rotation section of the page to enable and disable automatic rotation (p. 64) of the cryptographic material in a CMK.
Editing CMKs (API)

You can use the AWS Key Management Service (AWS KMS) API to edit your customer-managed CMKs. These examples use the AWS Command Line Interface (AWS CLI), but you can use any supported programming language. This section demonstrates several operations that return details about existing CMKs.

You cannot edit the properties of AWS managed CMKs.

Topics

- UpdateKeyDescription: Change the Description of a CMK (p. 15)
- PutKeyPolicy: Change the Key Policy for a CMK (p. 16)
- Enable and Disable Key Rotation (p. 16)

Tip

For information about adding, deleting, and editing tags, see Tagging Keys (p. 16).

UpdateKeyDescription: Change the Description of a CMK

The UpdateKeyDescription operation adds or changes the description of a CMK. To see the description, use the DescribeKey operation.

For example, this call to the UpdateKeyDescription operation changes the description of the specified CMK.

```bash
$ aws kms update-key-description --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
   --description "Example key"
```

To get the description of a key, use the DescribeKey operation, as shown in the following example.

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

{
   "KeyMetadata": {
      "Origin": "AWS_KMS",
      "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
      "Description": "Example key",
      "KeyManager": "CUSTOMER",
      "Enabled": true,
      "KeyUsage": "ENCRYPT_DECRYPT",
      "KeyState": "Enabled",
      "CreationDate": 1499988169.234,
      "Arn": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
      "AWSAccountId": "111122223333"
   }
}
PutKeyPolicy: Change the Key Policy for a CMK

The PutKeyPolicy operation changes the key policy of the CMK to the policy that you specify. The policy includes permissions for administrators, users, and roles. For a detailed example, see PutKeyPolicy Examples.

Enable and Disable Key Rotation

The EnableKeyRotation operation enables automatic rotation of the cryptographic material in a CMK. The DisableKeyRotation operation disables it. The GetKeyRotationStatus operation returns a Boolean value that tells you whether automatic key rotation is enabled (true) or disabled (false).

For an example, see Rotating Customer Master Keys.

Tagging Keys

You can use the Encryption keys section of the AWS Management Console to add, change, and delete tags for customer master keys (CMKs) that you manage. You can also use the operations in the AWS Key Management Service (AWS KMS) API to manage CMK tags. You cannot tag AWS managed CMKs.

Each tag consists of a tag key and a tag value, both of which you define. For example, the tag key might be “Cost Center” and the tag value might be “87654.”

You might use a tag to categorize and track your AWS costs. You can apply tags that represent business categories (such as cost centers, application names, or owners) to organize your costs across multiple services. When you add tags to your AWS resources, AWS generates a cost allocation report with usage and costs aggregated by tags. You can use this report to view your AWS KMS costs in terms of projects or applications, instead of viewing all AWS KMS costs as a single line item.

For more information about using tags for cost allocation, see Using Cost Allocation Tags in the AWS Billing and Cost Management User Guide. For information about the rules that apply to tag keys and tag values, see User-Defined Tag Restrictions in the AWS Billing and Cost Management User Guide.

Topics

- Managing CMK Tags (Console) (p. 16)
- Managing CMK Tags (API) (p. 17)

Managing CMK Tags (Console)

You can manage tags for your CMKs from the IAM section of the AWS Management Console. You can add tags to a CMK when you create it (p. 5). You can also use the console’s key details page to manage, add, edit, and delete tags for a CMK. For more information, see Editing Keys (p. 11).

To manage tags for your CMKs (console)

1. Sign in to the AWS Management Console and open the AWS Identity and Access Management (IAM) console at https://console.aws.amazon.com/iam/.
2. In the left navigation pane, choose Encryption keys.
3. For Region, choose the appropriate AWS Region. Do not use the region selector in the navigation bar (top right corner).
4. Select the check box next to the alias of the CMKs whose tags you want to manage.
Note
You cannot tag AWS managed CMKs, which are denoted by the orange AWS icon.

5. Choose Key actions, Add or edit tags.
6. Use the controls in the Add or edit tags window. When you're finished, choose Save.

Managing CMK Tags (API)

You can use the AWS Key Management Service (AWS KMS) API to add, delete, and list tags for the CMKs that you manage. These examples use the AWS Command Line Interface (AWS CLI), but you can use any supported programming language.

You cannot tag AWS managed CMKs.

Topics
• TagResource: Add or Change Tags for a CMK (p. 17)
• ListResourceTags: Get the Tags for a CMK (p. 18)
• UntagResource: Delete Tags from a CMK (p. 18)

TagResource: Add or Change Tags for a CMK

The TagResource operation adds one or more tags to a CMK.

You can also use TagResource to change the values for an existing tag. To replace tag values, specify the same tag key with different values. To add values to a tag, specify the tag key with both new and existing values.

For example, this call to the TagResource operation adds Purpose and Department tags to the specified CMK. You can use any keys and values as CMK tags.

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

When this command is successful, it does not return any output. To view the tags on a CMK, use the ListResourceTags operation.
ListResourceTags: Get the Tags for a CMK

The ListResourceTags operation gets the tags for a CMK. The key-id parameter is required.

For example, the following command gets the tags for the specified CMK.

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

"Truncated": false,
"Tags": [
    {
      "TagKey": "Purpose",
      "TagValue": "Test"
    },
    {
      "TagKey": "Department",
      "TagValue": "Finance"
    }
]
```

UntagResource: Delete Tags from a CMK

The UntagResource operation deletes tags from a CMK. The key-id and tag-keys parameters are required.

For example, this command deletes the Purpose tag and all of its values from the specified CMK.

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

When this command is successful, it does not return any output.

Enabling and Disabling Keys

You can disable and reenable the AWS Key Management Service (AWS KMS) customer master keys (CMKs) that you manage. You cannot change the status of AWS managed CMKs.

When you create a CMK, it is enabled by default. If you disable a CMK, it cannot be used to encrypt or decrypt data until you re-enable it. AWS managed CMKs are permanently enabled for use by services that use AWS KMS (p. 96). You cannot disable them.

You can also delete CMKs. For more information, see Deleting Customer Master Keys (p. 81).

Note
AWS KMS does not rotate the backing keys of customer-managed CMKs while they are disabled. For more information, see How Automatic Key Rotation Works (p. 65).

Topics
- Enabling and Disabling CMKs (Console) (p. 18)
- Enabling and Disabling CMKs (API) (p. 19)

Enabling and Disabling CMKs (Console)

You can enable and disable customer managed CMKs from the IAM section of the AWS Management Console.
To enable a CMK (console)

1. Sign in to the AWS Management Console and open the AWS Identity and Access Management (IAM) console at https://console.aws.amazon.com/iam/.
2. In the left navigation pane, choose Encryption keys.
3. For Region, choose the appropriate AWS Region. Do not use the region selector in the navigation bar (top right corner).
4. Select the check box next to the alias of the CMKs that you want to enable or disable.
   
   **Note**
   
   You cannot disable AWS managed CMKs, which are denoted by the orange AWS icon.
5. To enable a CMK, choose Key actions, Enable. To disable a CMK, choose Key actions, Disable.

Enabling and Disabling CMKs (API)

The EnableKey operation enables a disabled AWS KMS customer master key (CMK). These examples use the AWS Command Line Interface (AWS CLI), but you can use any supported programming language. The key-id parameter is required.

This operation does not return any output. To see the key status, use the DescribeKey operation.

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

The DisableKey operation disables an enabled CMK. The key-id parameter is required.

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

This operation does not return any output. To see the key status, use the DescribeKey operation, and see the Enabled field.

```bash
$ 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": false,
    "KeyUsage": "ENCRYPT_DECRYPT",
    "KeyState": "Disabled",
    "CreationDate": 1502910355.475,
    "Arn": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "AWSAccountId": "111122223333"
  }
}
```
Authentication and Access Control for AWS KMS

Access to AWS KMS requires credentials that AWS can use to authenticate your requests. The credentials must have permissions to access AWS resources, such as AWS KMS customer master keys (CMKs). The following sections provide details about how you can use AWS Identity and Access Management (IAM) and AWS KMS to help secure your resources by controlling who can access them.

Topics
- Authentication (p. 20)
- Access Control (p. 21)

Authentication

You can access AWS as any of the following types of identities:

- **AWS account root user** – When you sign up for AWS, you provide an email address and password for your AWS account. These are your *root credentials* and they provide complete access to all of your AWS resources.

  **Important**
  For security reasons, we recommend that you use the root credentials only to create an *administrator user*, which is an *IAM user* with full permissions to your AWS account. Then, you can use this administrator user to create other IAM users and roles with limited permissions. For more information, see Create Individual IAM Users (IAM Best Practices) and Creating An Admin User and Group in the IAM User Guide.

- **IAM user** – An *IAM user* is an identity within your AWS account that has specific permissions (for example, to use a KMS CMK). You can use an IAM user name and password to sign in to secure AWS webpages like the AWS Management Console, AWS Discussion Forums, or the AWS Support Center.

  In addition to a user name and password, you can also create *access keys* for each user to enable the user to access AWS services programmatically, through one of the AWS SDKs or the command line tools. The SDKs and command line tools use the access keys to cryptographically sign API requests. If you don’t use the AWS tools, you must sign API requests yourself. AWS KMS supports Signature Version 4, an AWS protocol for authenticating API requests. For more information about authenticating API requests, see Signature Version 4 Signing Process in the AWS General Reference.

- **IAM role** – An *IAM role* is another IAM identity you can create in your account that has specific permissions. It is similar to an IAM user, but it is not associated with a specific person. An IAM role enables you to obtain temporary access keys to access AWS services and resources programmatically. IAM roles are useful in the following situations:

  - **Federated user access** – Instead of creating an IAM user, you can use preexisting user identities from AWS Directory Service, your enterprise user directory, or a web identity provider. These are known as *federated users*. Federated users use IAM roles through an identity provider. For more information about federated users, see Federated Users and Roles in the IAM User Guide.
• **Cross-account access** – You can use an IAM role in your AWS account to allow another AWS account permissions to access your account's resources. For an example, see Tutorial: Delegate Access Across AWS Accounts Using IAM Roles in the *IAM User Guide*.

• **AWS service access** – You can use an IAM role in your account to allow an AWS service permissions to access your account's resources. For example, you can create a role that allows Amazon Redshift to access an S3 bucket on your behalf and then load data stored in the S3 bucket into an Amazon Redshift cluster. For more information, see Creating a Role to Delegate Permissions to an AWS Service in the *IAM User Guide*.

• **Applications running on EC2 instances** – Instead of storing access keys on an EC2 instance for use by applications that run on the instance and make AWS API requests, you can use an IAM role to provide temporary access keys for these applications. To assign an IAM role to an EC2 instance, you create an *instance profile* and then attach it when you launch the instance. An instance profile contains the role and enables applications running on the EC2 instance to get temporary access keys. For more information, see Using Roles for Applications on Amazon EC2 in the *IAM User Guide*.

## Access Control

You can have valid credentials to authenticate your requests, but you also need permissions to make AWS KMS API requests to create, manage, or use AWS KMS resources. For example, you must have permissions to create a KMS CMK, to manage the CMK, to use the CMK for cryptographic operations (such as encryption and decryption), and so on.

The following pages describe how to manage permissions for AWS KMS. We recommend that you read the overview first.

- Overview of Managing Access (p. 21)
- Using Key Policies (p. 24)
- Using IAM Policies (p. 40)
- AWS KMS API Permissions Reference (p. 43)
- Using Policy Conditions (p. 47)
- Using Grants (p. 57)

### Overview of Managing Access to Your AWS KMS Resources

Every AWS resource belongs to an AWS account, and permissions to create or access the resources are defined in permissions policies in that account. An account administrator can attach permissions policies to IAM identities (that is, users, groups, and roles), and some services (including AWS KMS) also support attaching permissions policies to other kinds of resources.

**Note**

An *account administrator* (or administrator user) is a user with administrator permissions. For more information, see Creating an Admin User and Group in the *IAM User Guide*.

When managing permissions, you decide who gets the permissions, the resources they get permissions for, and the specific actions allowed.
AWS KMS Resources and Operations

To manage permissions, you should understand some basic information about resources and operations. In AWS KMS, the primary resource type is a customer master key (CMK). AWS KMS also supports another resource type you can use with CMKs: an alias. An alias is a friendly name that points to a CMK. Some AWS KMS operations allow you to specify a CMK by its alias.

These resource types have unique Amazon Resource Names (ARNs) associated with them, as shown in the following list.

- **Customer master key (CMK)**
  
  ARN format:
  
  arn:aws:kms:AWS region:AWS account ID:key/CMK key ID
  
  Example ARN:
  
  arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab

- **Alias**
  
  ARN format:
  
  arn:aws:kms:AWS region:AWS account ID:alias/alias name
  
  Example ARN:
  

AWS KMS provides a set of API operations to work with your AWS KMS resources. For a list of available operations and the resources affected by each operation, see AWS KMS API Permissions Reference (p. 43).

Managing Access to AWS KMS CMKs

The primary way to manage access to your AWS KMS CMKs is with policies. Policies are documents that describe who has access to what. Policies attached to an IAM identity are called identity-based policies (or IAM policies), and policies attached to other kinds of resources are called resource-based policies. In AWS KMS, you must attach resource-based policies to your customer master keys (CMKs). These are called key policies. All KMS CMKs have a key policy.

You can control access to your KMS CMKs in these ways:

- **Use the key policy** – You must use the key policy to control access to a CMK. You can use the key policy alone to control access, which means the full scope of access to the CMK is defined in a single document (the key policy).
• **Use IAM policies in combination with the key policy** – You can use IAM policies in combination with the key policy to control access to a CMK. Controlling access this way enables you to manage all of the permissions for your IAM identities in IAM.

• **Use grants in combination with the key policy** – You can use grants in combination with the key policy to allow access to a CMK. Controlling access this way enables you to allow access to the CMK in the key policy, and to allow users to delegate their access to others.

For most AWS services, IAM policies are the only way to control access to the service's resources. Some services offer resource-based policies or other access control mechanisms to complement IAM policies, but these are generally optional and you can control access to the resources in these services with only IAM policies. This is not the case for AWS KMS, however. To allow access to a KMS CMK, you must use the key policy, either alone or in combination with IAM policies or grants. IAM policies by themselves are not sufficient to allow access to a CMK, though you can use them in combination with a CMK's key policy.

For more information about using key policies, see Using Key Policies (p. 24).

For more information about using IAM policies, see Using IAM Policies (p. 40).

For more information about using grants, see Using Grants (p. 57).

**Specifying Permissions in a Policy**

AWS KMS provides a set of API operations. To control access to these API operations, AWS KMS provides a set of **actions** that you can specify in a policy. For more information, see AWS KMS API Permissions Reference (p. 43).

A policy is a document that describes a set of permissions. The following are the basic elements of a policy.

• **Resource** – In an IAM policy, you use an Amazon Resource Name (ARN) to specify the resource that the policy applies to. For more information, see AWS KMS Resources and Operations (p. 22). In a key policy, you use "*" for the resource, which effectively means “this CMK.” A key policy applies only to the CMK it is attached to.

• **Action** – You use actions to specify the API operations you want to allow or deny. For example, the `kms:Encrypt` action corresponds to the AWS KMS Encrypt API operation.

• **Effect** – You use the effect to specify whether to allow or deny the permissions. If you don't explicitly allow access to a resource, access is implicitly denied. You can also explicitly deny access to a resource, which you might do to make sure that a user cannot access it, even when a different policy allows access.

• **Principal** – In an IAM policy, you don't specify a principal. Instead, the identity (the IAM user, group, or role) that the policy is attached to is the implicit principal. In a key policy, you must specify the principal (the identity) that the permissions apply to. You can specify AWS accounts (root), IAM users, IAM roles, and some AWS services as principals in a key policy. IAM groups are not valid principals in a key policy.

For more information, see Using Key Policies (p. 24) and Using IAM Policies (p. 40).
Specifying Conditions in a Policy

You can use another policy element called the condition to specify the circumstances in which a policy takes effect. For example, you might want a policy statement to take effect only after a specific date. Or, you might want a policy statement to control access based on whether a specific value exists in the API request.

To specify conditions, you use predefined condition keys. Some condition keys apply generally to AWS, and some are specific to AWS KMS. For more information, see Using Policy Conditions (p. 47).

Using Key Policies in AWS KMS

Key policies are the primary way to control access to customer master keys (CMKs) in AWS KMS. They are not the only way to control access, but you cannot control access without them. For more information, see Managing Access to AWS KMS CMKs (p. 22).

Topics

- Overview of Key Policies (p. 24)
- Default Key Policy (p. 25)
- Example Key Policy (p. 31)

Overview of Key Policies

A key policy is a document that uses JSON (JavaScript Object Notation) to specify permissions. You can work with these JSON documents directly, or you can use the AWS Management Console to work with them using a graphical interface called the default view. For more information about the console's default view for key policies, see Default Key Policy (p. 25) and Modifying a Key Policy (p. 34).

Key policy documents share a common JSON syntax with other permissions policies in AWS, and have the following basic structure:

```json
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "statement identifier",
    "Effect": "effect",
    "Principal": "principal",
    "Action": "action",
    "Resource": "resource",
    "Condition": {
      "condition operator": {
        "condition context key": "context key value"
      }
    }
  }]
}
```

A key policy document must have a Version element. We recommend setting the version to 2012-10-17 (the latest version). In addition, a key policy document must have one or more statements, and each statement consists of up to six elements:

- **Sid** – (Optional) The Sid is a statement identifier, an arbitrary string you can use to identify the statement.
- **Effect** – (Required) The effect specifies whether to allow or deny the permissions in the policy statement. The Effect must be Allow or Deny. If you don't explicitly allow access to a CMK, access is implicitly denied. You can also explicitly deny access to a CMK. You might do this to make sure that a user cannot access it, even when a different policy allows access.
• **Principal** – (Required) The principal is the identity that the permissions in the policy statement apply to. You can specify AWS accounts (root), IAM users, IAM roles, and some AWS services as principals in a key policy. IAM groups are not valid principals.

• **Action** – (Required) Actions specify the API operations to allow or deny. For example, the `kms:Encrypt` action corresponds to the AWS KMS `Encrypt` API operation. You can list more than one action in a policy statement. For more information, see AWS KMS API Permissions Reference (p. 43).

• **Resource** – (Required) In a key policy, you use "*" for the resource, which means "this CMK." A key policy applies only to the CMK it is attached to.

• **Condition** – (Optional) Conditions specify requirements that must be met for a key policy to take effect. With conditions, AWS can evaluate the context of an API request to determine whether or not the policy statement applies. For more information, see Using Policy Conditions (p. 47).

For more information about AWS policy syntax, see AWS IAM Policy Reference in the IAM User Guide.

### Default Key Policy

**Default key policy when you create a CMK programmatically**

When you create a CMK programmatically—that is, with the AWS KMS API (including through the AWS SDKs and command line tools)—you have the option of providing the key policy for the new CMK. If you don't provide one, AWS KMS creates one for you. This default key policy has one policy statement that gives the AWS account (root user) that owns the CMK full access to the CMK and enables IAM policies in the account to allow access to the CMK. For more information about this policy statement, see Allows Access to the AWS Account and Enables IAM Policies (p. 25).

**Default key policy when you create a CMK with the AWS Management Console**

When you create a CMK with the AWS Management Console (p. 5), you can choose the IAM users, IAM roles, and AWS accounts that are given access to the CMK. The users, roles, and accounts that you choose are added to a default key policy that the console creates for you. With the console, you can use the default view to view or modify this key policy, or you can work with the key policy document directly. The default key policy created by the console allows the following permissions, each of which is explained in the corresponding section.

**Permissions**

- Allows Access to the AWS Account and Enables IAM Policies (p. 25)
- Allows Key Administrators to Administer the CMK (p. 26)
- Allows Key Users to Use the CMK (p. 28)

**Allows Access to the AWS Account and Enables IAM Policies**

The default key policy gives the AWS account (root user) that owns the CMK full access to the CMK, which accomplishes the following two things.

1. **Reduces the risk of the CMK becoming unmanageable.**
   
   You cannot delete your AWS account's root user, so allowing access to this user reduces the risk of the CMK becoming unmanageable. Consider this scenario:
   
   1. A CMK's key policy allows only one IAM user, Alice, to manage the CMK. This key policy does not allow access to the root user.
   2. Someone deletes IAM user Alice.
   
   In this scenario, the CMK is now unmanageable, and you must contact AWS Support to regain access to the CMK. The root user does not have access to the CMK, because the root user can access a CMK
only when the key policy explicitly allows it. This is different from most other resources in AWS, which implicitly allow access to the root user.

2. Enables IAM policies to allow access to the CMK.

IAM policies by themselves are not sufficient to allow access to a CMK. However, you can use them in combination with a CMK's key policy if the key policy enables it. Giving the AWS account full access to the CMK does this; it enables you to use IAM policies to give IAM users and roles in the account access to the CMK. It does not by itself give any IAM users or roles access to the CMK, but it enables you to use IAM policies to do so. For more information, see Managing Access to AWS KMS CMKs (p. 22).

The following example shows the policy statement that allows access to the AWS account and thereby enables IAM policies.

```
{"Sid": "Enable IAM User Permissions",
"Effect": "Allow",
"Principal": {"AWS": "arn:aws:iam::111122223333:root"},
"Action": "kms:*",
"Resource": "*"
}
```

Allows Key Administrators to Administer the CMK

The default key policy created by the console allows you to choose IAM users and roles in the account and make them key administrators. Key administrators have permissions to manage the CMK, but do not have permissions to use the CMK to encrypt and decrypt data.

**Warning**

Even though key administrators do not have permissions to use the CMK to encrypt and decrypt data, they do have permission to modify the key policy. This means they can give themselves these permissions.

You can add IAM users and roles to the list of key administrators when you create the CMK. You can also edit the list with the console's default view for key policies, as shown in the following image. The default view for key policies is available on the key details page for each CMK.
When you use the console's default view to modify the list of key administrators, the console modifies the Principal element in a particular statement in the key policy. This statement is called the key administrators statement. The following example shows the key administrators statement.

```json
{
    "Sid": "Allow access for Key Administrators",
    "Effect": "Allow",
    "Principal": {
        "AWS": [
            "arn:aws:iam::111122223333:user/KMSAdminUser",
            "arn:aws:iam::111122223333:role/KMSAdminRole"
        ]
    },
    "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": "*"
}
```

The key administrators statement allows the following permissions:
• **kms:Create*** – Allows key administrators to create aliases and grants (p. 57) for this CMK.
• **kms:Describe*** – Allows key administrators to retrieve information about this CMK including its identifiers, creation date, state, and more. This permission is necessary to view the key details page in the AWS Management Console.
• **kms:Enable*** – Allows key administrators to set this CMK’s state to enabled and to specify annual rotation of the CMK’s key material (p. 64).
• **kms:List*** – Allows key administrators to retrieve lists of the aliases, grants, key policies, and tags for this CMK. This permission is necessary to view the list of CMKs in the AWS Management Console.
• **kms:Put*** – Allows key administrators to modify the key policy for this CMK.
• **kms:Update*** – Allows key administrators to change the target of an alias to this CMK, and to modify this CMK’s description.
• **kms:Revoke*** – Allows key administrators to revoke the permissions for this CMK that are allowed by a grant (p. 57).
• **kms:Disable*** – Allows key administrators to set this CMK’s state to disabled and to disable annual rotation of this CMK’s key material (p. 64).
• **kms:Get*** – Allows key administrators to retrieve the key policy for this CMK and to determine whether this CMK’s key material is rotated annually. If this CMK’s origin is external, it also allows key administrators to download the public key and import token for this CMK. For more information about CMK origin, see Importing Key Material (p. 69).
• **kms:Delete*** – Allows key administrators to delete an alias that points to this CMK and, if this CMK’s origin is external, to delete the imported key material. For more information about imported key material, see Importing Key Material (p. 69). Note that this permission does not allow key administrators to delete the CMK (p. 81).
• **kms:ImportKeyMaterial** – Allows key administrators to import key material into the CMK.
  
  **Note**
  This permission is not shown in the preceding example policy statement. This permission is applicable only to CMKs whose origin is external. It is automatically included in the key administrators statement when you use the console to create a CMK with no key material (p. 71). For more information, see Importing Key Material (p. 69).
• **kms:TagResource** – Allows key administrators to add and update tags for this CMK.
• **kms:UntagResource** – Allows key administrators to remove tags from this CMK.
• **kms:ScheduleKeyDeletion** – Allows key administrators to delete this CMK (p. 81).
• **kms:CancelKeyDeletion** – Allows key administrators to cancel the pending deletion of this CMK.

The final two permissions in the preceding list, **kms:ScheduleKeyDeletion** and **kms:CancelKeyDeletion**, are included by default when you create a CMK (p. 5). However, you can optionally remove them from the key policy when you create a CMK by clearing the box for **Allow key administrators to delete this key**. In the same way, you can use the key details page to remove them from the default key policy for existing CMKs. For more information, see Editing Keys (p. 11).

Many of these permissions contain the wildcard character (**`). That means that if AWS KMS adds new API operations in the future, key administrators will automatically be allowed to perform all new API operations that begin with Create, Describe, Enable, List, Put, Update, Revoke, Disable, Get, or Delete.

**Note**
The key administrators statement described in the preceding section is in the latest version of the default key policy. For information about previous versions of the default key policy, see Keeping Key Policies Up to Date (p. 38).

**Allows Key Users to Use the CMK**

The default key policy created by the console allows you to choose IAM users and roles in the account, and external AWS accounts, and make them **key users**. Key users have permissions to use the CMK
directly for encryption and decryption. They also have permission to delegate a subset of their own permissions to some of the AWS services that are integrated with AWS KMS (p. 96). Key users can implicitly give these services permissions to use the CMK in specific and limited ways. This implicit delegation is done using grants (p. 57). For example, key users can do the following things:

- Use this CMK with Amazon Elastic Block Store (Amazon EBS) and Amazon Elastic Compute Cloud (Amazon EC2) to attach an encrypted EBS volume to an EC2 instance. The key user implicitly gives Amazon EC2 permission to use the CMK to attach the encrypted volume to the instance. For more information, see How Amazon Elastic Block Store (Amazon EBS) Uses AWS KMS (p. 103).

- Use this CMK with Amazon Redshift to launch an encrypted cluster. The key user implicitly gives Amazon Redshift permission to use the CMK to launch the encrypted cluster and create encrypted snapshots. For more information, see How Amazon Redshift Uses AWS KMS (p. 112).

- Use this CMK with other AWS services integrated with AWS KMS (p. 96), specifically the services that use grants, to create, manage, or use encrypted resources with those services.

The default key policy gives key users permissions to allow these integrated services to use the CMK, but users also need permission to use the integrated services. For details about giving users access to an AWS service that integrates with AWS KMS, consult the documentation for the integrated service.

The default key policy gives key users permissions to use a CMK with all of the integrated services that use grants, or none of them. You cannot use the default key policy to allow key users to use a CMK with some of the integrated services but not others. However, you can create a custom key policy to do this. For more information, see the kms:ViaService (p. 55) condition key.

You can add IAM users, IAM roles, and external AWS accounts to the list of key users when you create the CMK. You can also edit the list with the console’s default view for key policies, as shown in the following image. The default view for key policies is on the key details page.
When you use the console's default view to modify the list of key users, the console modifies the Principal element in two statements in the key policy. These statements are called the key users statements. The following examples show the key users statements.

```
{
    "Sid": "Allow use of the key",
    "Effect": "Allow",
    "Principal": {"AWS": [
        "arn:aws:iam::111122223333:user/KMSUser",
        "arn:aws:iam::111122223333:role/KMSRole",
        "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:user/KMSUser",
        "arn:aws:iam::111122223333:role/KMSRole",
        "arn:aws:iam::444455556666:root"
    ]},
    "Action": [
        "kms:List*",
        "kms:RecoverKey getKey*",
        "kms:Get*",
        "kms:Create*",
        "kms:Start*",
        "kms:Stop*",
        "kms:Tag*",
        "kms:Untag*",
        "kms:Cancel*",
        "kms:CreateGrant",
        "kms:ListGrants",
        "kms:DescribeGrants",
        "kms:TagResource",
        "kms:UntagResource"
    ],
    "Resource": "*"
}
```
Example Key Policy

The following example shows a complete key policy. This key policy combines the example policy statements from the preceding default key policy (p. 25) section into a single key policy that accomplishes the following:

- Allows the AWS account (root user) 111122223333 full access to the CMK, and thus enables IAM policies in the account to allow access to the CMK.
- Allows IAM user KMSAdminUser and IAM role KMSAdminRole to administer the CMK.
- Allows IAM user KMSUser, IAM role KMSRole, and AWS account 444455556666 to use the CMK.

```json
{
    "Version": "2012-10-17",
    "Id": "key-consolepolicy-2",
    "Statement": [
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal": "aws:arn:iam::111122223333:root",
            "Action": "kms:*",
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```
Example Key Policy

```
"Resource": "*
",
{
"Sid": "Allow access for Key Administrators",
"Effect": "Allow",
"Principal": {"AWS": [
  "arn:aws:iam::111122223333:user/KMSAdminUser",
  "arn:aws:iam::111122223333:role/KMSAdminRole"
]},
"Action": [
  "kms:Create\*",
  "kms:Describe\*",
  "kms:Enable\*",
  "kms:List\*",
  "kms:Put\*",
  "kms:Update\*",
  "kms:Revoke\*",
  "kms:Disable\*",
  "kms:Get\*",
  "kms:Delete\*",
  "kms:TagResource",
  "kms:UntagResource",
  "kms:ScheduleKeyDeletion",
  "kms:CancelKeyDeletion"
],
"Resource": "*
",
{
"Sid": "Allow use of the key",
"Effect": "Allow",
"Principal": {"AWS": [
  "arn:aws:iam::111122223333:user/KMSUser",
  "arn:aws:iam::111122223333:role/KMSRole",
  "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:user/KMSUser",
  "arn:aws:iam::111122223333:role/KMSRole",
  "arn:aws:iam::444455556666:root"
]},
"Action": [
  "kms:CreateGrant",
  "kms:ListGrants",
  "kms:RevokeGrant"
],
"Resource": "*
",
"Condition": {"Bool": {"kms:GrantIsForAWSResource": "true"}}
}
]
```
### Key Policy

**Key Administrators**

The following IAM users and roles can administer this key through the KMS API. You may need to add additional permissions for the users or roles to administer this key from this console. [Learn more.](#)

<table>
<thead>
<tr>
<th>Name</th>
<th>Path</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>KMSAdminUser</td>
<td>/</td>
<td>User</td>
</tr>
<tr>
<td>KMSAdminRole</td>
<td>/</td>
<td>Role</td>
</tr>
</tbody>
</table>

**Key Deletion**

- [x] Allow key administrators to delete this key

[Save Changes](#)

### Key Users

**This Account**

The following IAM users and roles can use this key to encrypt and decrypt data from within applications and when using AWS services integrated with KMS. [Learn more.](#)

<table>
<thead>
<tr>
<th>Name</th>
<th>Path</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>KMSUser</td>
<td>/</td>
<td>User</td>
</tr>
<tr>
<td>KMSRole</td>
<td>/</td>
<td>Role</td>
</tr>
</tbody>
</table>

### External Accounts

The following external accounts can use this key to encrypt and decrypt data. Administrators of the accounts shown below are responsible for managing the permissions that allow their IAM users and roles to use this key.

- `arn:aws:iam::444455556666:root`

[Add](#) [Remove](#)

[Save Changes](#)
Modifying a Key Policy

To change the permissions for a customer master key (CMK) in AWS KMS you modify the CMK’s key policy (p. 24). You can add or remove IAM users, IAM roles, and AWS accounts (root users) in the key policy, and change the actions that are allowed or denied for those principals. For more information about the ways to specify principals and permissions in a key policy, see Using Key Policies (p. 24).

You cannot add IAM groups to a key policy, though you can add multiple IAM users. For more information, see Allowing Multiple IAM Users to Access a CMK (p. 36).

When you add external AWS accounts to a key policy, you must also use IAM policies in the external accounts to give permissions to IAM users, groups, or roles in those accounts. For more information, see Allowing External AWS Accounts to Access a CMK (p. 37).

Topics
- How to Modify a Key Policy (p. 34)
- Allowing Multiple IAM Users to Access a CMK (p. 36)
- Allowing External AWS Accounts to Access a CMK (p. 37)

How to Modify a Key Policy

You can modify a key policy in three different ways, each of which is explained in the following sections.

Ways to modify a key policy
- Using the AWS Management Console's Default View (p. 34)
- Using the AWS Management Console's Policy View (p. 35)
- Using the AWS KMS API (p. 36)

Using the AWS Management Console's Default View

You can use the console to modify a key policy with a graphical interface called the default view.

Note
If the following steps don't match what you see in the console, it means that this key policy was not created by the console, or the key policy has been modified in a way that the console's default view does not support. In that case, follow the steps at Using the AWS Management Console's Policy View (p. 35) or Using the AWS KMS API (p. 36).

To modify a key policy (console default view)
1. Sign in to the AWS Management Console and open the AWS Identity and Access Management (IAM) console at https://console.aws.amazon.com/iam/.
2. In the left navigation pane, choose Encryption keys.
3. For Region, choose the appropriate AWS Region. Do not use the region selector in the navigation bar (top right corner).
4. Choose the alias of the CMK whose key policy you want to modify.
5. Decide what to modify.
   - To add or remove key administrators (p. 26), and to allow or disallow key administrators to delete the CMK (p. 81), use the controls in the Key Administrators area in the Key Policy section of the page.
To add or remove key users (p. 28), and to allow or disallow external AWS accounts to use the CMK, use the controls in the Key Users area in the Key Policy section of the page.

Using the AWS Management Console's Policy View

You can use the console to modify a key policy document with the console's policy view.

To modify a key policy document (console policy view)

1. Sign in to the AWS Management Console and open the AWS Identity and Access Management (IAM) console at https://console.aws.amazon.com/iam/.
2. In the left navigation pane, choose Encryption keys.
3. For Region, choose the appropriate AWS Region. Do not use the region selector in the navigation bar (top right corner).
4. Choose the alias of the CMK whose key policy document you want to edit.

5. On the Key Policy line, choose Switch to policy view.

6. Edit the key policy document, and then choose Save Changes.

Using the AWS KMS API

You can use the AWS KMS API to modify a key policy document. The following steps use the AWS KMS HTTP API. You can perform the same operations with the AWS SDKs or AWS command line tools, which is often easier than using the HTTP API. For the operations and syntax to use for other SDKs and tools, consult the reference documentation for that particular SDK or tool. For sample code that uses the AWS SDK for Java, see Working with Key Policies (p. 167).

To modify a key policy document (API)

1. Use GetKeyPolicy to retrieve the existing key policy document, and then save the key policy document to a file.
2. Open the key policy document in your preferred text editor, edit the key policy document, and then save the file.
3. Use PutKeyPolicy to apply the updated key policy document to the CMK.

Allowing Multiple IAM Users to Access a CMK

IAM groups are not valid principals in a key policy. To allow multiple IAM users to access a CMK, do one of the following:

- Add each IAM user to the key policy. This approach requires that you update the key policy each time the list of authorized users changes.
- Ensure that the key policy includes the statement that enables IAM policies to allow access to the CMK (p. 25). Then create an IAM policy that allows access to the CMK, and then attach that policy to an IAM group that contains the authorized IAM users. Using this approach, you don't need to modify any policies when the list of authorized users changes. Instead, you only need to add or remove those users from the appropriate IAM group.

For more information about how AWS KMS key policies and IAM policies work together, see Understanding Policy Evaluation (p. 58).
Allowing External AWS Accounts to Access a CMK

You can allow IAM users or roles in one AWS account to access a CMK in another account. For example, suppose that users or roles in account 111122223333 need to use a CMK in account 444455556666. To allow this, you must do two things:

1. Modify the key policy for the CMK in account 444455556666.
2. Add an IAM policy (or modify an existing one) for the users or roles in account 111122223333.

Neither step by itself is sufficient to give access to a CMK across accounts—you must do both.

Modifying the CMK's Key Policy to Allow External Accounts

To allow IAM users or roles in one AWS account to use a CMK in a different account, you first add the external account (root user) to the CMK's key policy. Note that you don't add the individual IAM users or roles to the key policy, only the external account that owns them.

Decide what permissions you want to give to the external account:

- To add the external account to a key policy as a key user, you can use the AWS Management Console's default view for the key policy. For more information, see Using the AWS Management Console's Default View (p. 34).

You can also modify the key policy document directly using the console's policy view or the AWS KMS API, as described in Using the AWS Management Console's Policy View (p. 35) and Using the AWS KMS API (p. 36).

- To add the external account to a key policy as a key administrator or give custom permissions, you must modify the key policy document directly using the console's policy view or the AWS KMS API. For more information, see Using the AWS Management Console's Policy View (p. 35) or Using the AWS KMS API (p. 36).

For an example of JSON syntax that adds an external account to the Principal element of a key policy document, see the policy statement in the default console key policy (p. 28) that allows key users to use the CMK.

Adding or modifying an IAM Policy to Allow Access to a CMK in Another AWS Account

After you add the external account to the CMK's key policy, you then add an IAM policy (or modify an existing one) to the users or roles in the external account. In this scenario, users or roles in account 111122223333 need to use a CMK that is in account 444455556666. To allow this, you create an IAM policy in account 111122223333 that allows access to the CMK in account 444455556666, and then attach the policy to the users or roles in account 111122223333. The following example shows a policy that allows access to a CMK in account 444455556666.

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowUseOfCMKInAccount444455556666",
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*"
            ]
        }
    ]
}
```
This policy allows users and roles in account 111122223333 to use the CMK in account 444455556666 directly for encryption and decryption, and to delegate a subset of their own permissions to some of the AWS services that are integrated with AWS KMS (p. 96), specifically the services that use grants. Note the following details about this policy:

- The policy allows the use of a specific CMK in account 444455556666, identified by the CMK's Amazon Resource Name (ARN) (p. 22) in the Resource element of the policy statements. When you give access to CMKs with an IAM policy, always list the specific CMK ARNs in the policy's Resource element. Otherwise, you might inadvertently give access to more CMKs than you intend.
- IAM policies do not contain the Principal element, which differs from KMS key policies. In IAM policies, the principal is implied by the identity to which the policy is attached.
- The policy gives key users permissions to allow integrated services to use the CMK, but these users also need permission to use the integrated services themselves. For details about giving users access to an AWS service that integrates with AWS KMS, consult the documentation for the integrated service. Also, note that for users or roles in account 111122223333, the CMK in account 444455556666 will not appear in the AWS Management Console to select when creating encrypted resources, even when the users or roles have a policy like this attached. The console does not show CMKs in other accounts.

For more information about working with IAM policies, see Using IAM Policies (p. 40).

Keeping Key Policies Up to Date

When you use the AWS Management Console to create a customer master key (CMK) (p. 5), you can choose the IAM users, IAM roles, and AWS accounts that you want to have access to the CMK. These users, roles, and accounts are added to a default key policy (p. 25) that controls access to the CMK. Occasionally, the default key policy for new CMKs is updated. Typically, these updates correspond to new AWS KMS features.

When you create a new CMK, the latest version of the default key policy is added to the CMK. However, existing CMKs continue to use their existing key policy—that is, new versions of the default key policy are not automatically applied to existing CMKs. Instead, the console alerts you that a newer version is available and prompts you to upgrade it.

Note

The console alerts you only when you are using the default key policy that was applied when you created the CMK. If you manually modified the key policy document using the console's policy view or the PutKeyPolicy API operation, the console does not alert you when new permissions are available.
For information about the permissions that are added to a key policy when you upgrade it, see Changes to the Default Key Policy (p. 39). Upgrading to the latest version of the key policy should not cause problems because it only adds permissions; it doesn't remove any. We recommend keeping your key policies up to date unless you have a specific reason not to.

To determine if a newer version of the default key policy is available

1. Sign in to the AWS Management Console and open the AWS Identity and Access Management (IAM) console at https://console.aws.amazon.com/iam/.
2. In the left navigation pane, choose Encryption keys.
3. For Region, choose the appropriate AWS Region. Do not use the region selector in the navigation bar (top right corner).
4. Choose the alias of the CMK whose key policy you want to see. When a newer version of the default key policy is available, the console displays the following alert.

   A newer version of the default key policy is available. Preview and upgrade to the new key policy.

To upgrade to the latest version of the default key policy

1. When you see the preceding alert, choose Preview and upgrade to the new key policy.
2. Review the key policy document for the latest version of the default key policy. For more information about the difference between the latest version and previous versions, see Changes to the Default Key Policy (p. 39). After reviewing the key policy, choose Upgrade key policy.

Changes to the Default Key Policy

In the current version of the default key policy (p. 25), the key administrators statement contains more permissions than those in previous versions. These additional permissions correspond to new AWS KMS features.

CMKs that are using an older version of the default key policy might be missing the following permissions. When you upgrade to the latest version of the default key policy, they're added to the key administrators statement.

kms:TagResource and kms:UntagResource

These permissions allow key administrators to add, update, and remove tags from the CMK. They were added to the default key policy when AWS KMS released the tagging feature (p. 16).

kms:ScheduleKeyDeletion and kms:CancelKeyDeletion

These permissions allow key administrators to schedule and cancel deletion for the CMK. They were added to the default key policy when AWS KMS released the CMK deletion feature (p. 81).

Note

The kms:ScheduleKeyDeletion and kms:CancelKeyDeletion permissions are included by default when you create a CMK (p. 5) and when you upgrade to the latest version of the default key policy. However, you can optionally remove them from the default key policy when you create a CMK by clearing the box for Allow key administrators to delete this key. In the same way, you can use the key details page to remove them from the default key policy for existing CMKs. That includes CMKs whose key policy you upgraded to the latest version.
Using IAM Policies with AWS KMS

You can use IAM policies in combination with key policies (p. 24) to control access to your customer master keys (CMKs) in AWS KMS.

**Note**

This section discusses using IAM in the context of AWS KMS. It doesn't provide detailed information about the IAM service. For complete IAM documentation, see the IAM User Guide.

Policies attached to IAM identities (that is, users, groups, and roles) are called identity-based policies (or IAM policies), and policies attached to resources outside of IAM are called resource-based policies. In AWS KMS, you must attach resource-based policies to your CMKs. These are called key policies. All KMS CMKs have a key policy, and you must use it to control access to a CMK. IAM policies by themselves are not sufficient to allow access to a CMK, though you can use them in combination with a CMK’s key policy. To do so, ensure that CMK’s key policy includes the policy statement that enables IAM policies (p. 25).

**Topics**

- Overview of IAM Policies (p. 40)
- Permissions Required to Use the AWS KMS Console (p. 41)
- AWS Managed (Predefined) Policies for AWS KMS (p. 41)
- Customer Managed Policy Examples (p. 41)

**Overview of IAM Policies**

You can use IAM policies in the following ways:

- **Attach a permissions policy to a user or a group** – You can attach a policy that allows an IAM user or group of users to, for example, create new CMKs.

- **Attach a permissions policy to a role for federation or cross-account permissions** – You can attach an IAM policy to an IAM role to enable identity federation, allow cross-account permissions, or give permissions to applications running on EC2 instances. For more information about the various use cases for IAM roles, see IAM Roles in the IAM User Guide.

The following example shows an IAM policy with AWS KMS permissions. This policy allows the IAM identities to which it is attached to retrieve a list of all CMKs and aliases.

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

This policy doesn't specify the Principal element because in IAM policies you don’t specify the principal who gets the permissions. When you attach this policy to an IAM user, that user is the implicit principal. When you attach this policy to an IAM role, the assumed role user gets the permissions.

For a table showing all of the AWS KMS API actions and the resources that they apply to, see the AWS KMS API Permissions Reference (p. 43).
Permissions Required to Use the AWS KMS Console

To work with the AWS KMS console, users must have a minimum set of permissions that allow them to work with the AWS KMS resources in their AWS account. In addition to these AWS KMS permissions, users must also have permissions to list IAM users and roles. If you create an IAM policy that is more restrictive than the minimum required permissions, the AWS KMS console won’t function as intended for users with that IAM policy.

For the minimum permissions required to allow a user read-only access to the AWS KMS console, see Allow a User Read-Only Access to All CMKs through the AWS KMS Console (p. 42).

To allow users to work with the AWS KMS console to create and manage CMKs, attach the AWSKeyManagementServicePowerUser managed policy to the user, as described in the following section.

You don't need to allow minimum console permissions for users that are working with the AWS KMS API through the AWS SDKs or command line tools, though you do need to grant these users permission to use the API. For more information, see AWS KMS API Permissions Reference (p. 43).

AWS Managed (Predefined) Policies for AWS KMS

AWS addresses many common use cases by providing standalone IAM policies that are created and managed by AWS. These are called AWS managed policies. AWS managed policies provide the necessary permissions for common use cases so you don't have to investigate which permissions are needed. For more information, see AWS Managed Policies in the IAM User Guide.

AWS provides one AWS managed policy for AWS KMS called AWSKeyManagementServicePowerUser. This policy allows the following permissions:

- Allows users to list all CMKs and aliases.
- Allows users to retrieve information about each CMK, including its identifiers, creation date, rotation status, key policy, and more.
- Allows users to create CMKs that they can administer or use. When users create a CMK, they can set permissions in the CMK’s key policy (p. 24). This means users can create CMKs with any permissions they want, including allowing themselves to administer or use the CMK. The AWSKeyManagementServicePowerUser policy does not allow users to administer or use any other CMKs, only the ones they create.

Customer Managed Policy Examples

In this section, you can find example IAM policies that allow permissions for various AWS KMS actions.

Important
Some of the permissions in the following policies are allowed only when the CMK's key policy also allows them. For more information, see AWS KMS API Permissions Reference (p. 43).

Examples
- Allow a User Read-Only Access to All CMKs through the AWS KMS Console (p. 42)
- Allow a User to Encrypt and Decrypt with Any CMK in a Specific AWS Account (p. 42)
- Allow a User to Encrypt and Decrypt with Any CMK in a Specific AWS Account and Region (p. 42)
- Allow a User to Encrypt and Decrypt with Specific CMKs (p. 43)
- Prevent a User from Disabling or Deleting Any CMKs (p. 43)
Allow a User Read-Only Access to All CMKs through the AWS KMS Console

The following policy allows users read-only access to the AWS KMS console. That is, users can use the console to view all CMKs, but they cannot make changes to any CMKs or create new ones.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "kms:ListKeys",
      "kms:ListAliases",
      "kms:DescribeKey",
      "kms:ListKeyPolicies",
      "kms:GetKeyPolicy",
      "kms:GetKeyRotationStatus",
      "iam:ListUsers",
      "iam:ListRoles"
    ],
    "Resource": "*"
  }
}
```

Allow a User to Encrypt and Decrypt with Any CMK in a Specific AWS Account

The following policy allows a user to successfully request that AWS KMS encrypt and decrypt data with any CMK in AWS account 111122223333.

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

Allow a User to Encrypt and Decrypt with Any CMK in a Specific AWS Account and Region

The following policy allows a user to successfully request that AWS KMS encrypt and decrypt data with any CMK in AWS account 111122223333 in the US West (Oregon) region.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "kms:Encrypt",
      "kms:Decrypt"
    ]
  }
}
```
Allow a User to Encrypt and Decrypt with Specific CMKs

The following policy allows a user to successfully request that AWS KMS encrypt and decrypt data with the two CMKs specified in the policy's `Resource` element.

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

Prevent a User from Disabling or Deleting Any CMKs

The following policy prevents a user from disabling or deleting any CMKs, even when another IAM policy or a key policy allows these permissions. A policy that explicitly denies permissions overrides all other policies, even those that explicitly allow the same permissions. For more information, see Determining Whether a Request is Allowed or Denied in the IAM User Guide.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Deny",
        "Action": [
            "kms:DisableKey",
            "kms:ScheduleKeyDeletion"
        ],
        "Resource": "*"
    }
}
```

AWS KMS API Permissions: Actions and Resources Reference

When you are setting up access control (p. 21) with key policies (p. 24) and IAM policies (p. 40), you can use the following table as a reference. The first column in the table lists each AWS KMS API operation and the corresponding action (permission) that allows the operation. You specify actions in a policy's `Action` element. The remaining columns provide the following additional information:

- The type of policy you must use to allow permissions to perform the operation. When the key policy is required, you can allow the permissions directly in the key policy, or you can ensure the key policy...
contains the policy statement that enables IAM policies (p. 25) and then allow the permissions in an IAM policy.

- The resource or resources for which you can allow the operation. You specify resources in a policy's Resource element. For key policies, you always specify "*" for the resource, which effectively means "this CMK." A key policy applies only to the CMK it is attached to. For IAM policies, you can specify the Amazon Resource Name (ARN) for a specific resource or set of resources.
- The AWS KMS condition keys you can use to control access to the operation. You specify conditions in a policy's Condition element. For more information, see AWS KMS Condition Keys (p. 49).

### AWS KMS API Operations and Permissions

<table>
<thead>
<tr>
<th>API Operations and Actions (Permissions)</th>
<th>Policy Type</th>
<th>Resources and ARNs (for IAM Policies)</th>
<th>AWS KMS Condition Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>CancelKeyDeletion</td>
<td>Key policy</td>
<td>CMK  &lt;br&gt; arn:aws:kms:AWS_region:AWS_account_ID:role/CMK_key_ID</td>
<td>kms:CallerAccount</td>
</tr>
<tr>
<td>CreateAlias</td>
<td>IAM policy (for the alias)</td>
<td>Alias  &lt;br&gt; arn:aws:kms:AWS_region:AWS_account_ID:alias/alias_name</td>
<td>None (when controlling access to the alias)</td>
</tr>
<tr>
<td>CreateGrant</td>
<td>Key policy</td>
<td>CMK  &lt;br&gt; arn:aws:kms:AWS_region:AWS_account_ID:role/CMK_key_ID</td>
<td>kms:CallerAccount</td>
</tr>
<tr>
<td>CreateKey</td>
<td>IAM policy</td>
<td>*  &lt;br&gt; &lt;br&gt; arn:aws:kms:AWS_region:AWS_account_ID:role/CMK_key_ID</td>
<td>kms:BypassPolicyLockoutSafety</td>
</tr>
<tr>
<td>Decrypt</td>
<td>Key policy</td>
<td>CMK  &lt;br&gt; arn:aws:kms:AWS_region:AWS_account_ID:role/CMK_key_ID</td>
<td>kms:EncryptionContext:</td>
</tr>
<tr>
<td>DeleteAlias</td>
<td>IAM policy (for the alias)</td>
<td>Alias  &lt;br&gt; arn:aws:kms:AWS_region:AWS_account_ID:alias/alias_name</td>
<td>None (when controlling access to the alias)</td>
</tr>
<tr>
<td>key:DeleteAlias</td>
<td>Key policy</td>
<td>CMK  &lt;br&gt; arn:aws:kms:AWS_region:AWS_account_ID:role/CMK_key_ID</td>
<td>kms:CallerAccount</td>
</tr>
<tr>
<td>API Operations and Actions (Permissions)</td>
<td>Policy Type</td>
<td>Resources and ARNs (for IAM Policies)</td>
<td>AWS KMS Condition Keys</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-------------</td>
<td>--------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>requires permissions for both.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DescribeKey</td>
<td>Key policy</td>
<td>CMK</td>
<td>kms:CallerAccount</td>
</tr>
<tr>
<td>kms:DescribeKey</td>
<td></td>
<td>arn:aws:kms:AWS_region:AWS_account_ID:CMK_key_ID</td>
<td></td>
</tr>
<tr>
<td>DisableKey</td>
<td>Key policy</td>
<td>CMK</td>
<td>kms:CallerAccount</td>
</tr>
<tr>
<td>kms:DisableKey</td>
<td></td>
<td>arn:aws:kms:AWS_region:AWS_account_ID:CMK_key_ID</td>
<td></td>
</tr>
<tr>
<td>DisableKeyRotation</td>
<td>Key policy</td>
<td>CMK</td>
<td>kms:CallerAccount</td>
</tr>
<tr>
<td>kms:DisableKeyRotation</td>
<td></td>
<td>arn:aws:kms:AWS_region:AWS_account_ID:CMK_key_ID</td>
<td></td>
</tr>
<tr>
<td>EnableKey</td>
<td>Key policy</td>
<td>CMK</td>
<td>kms:CallerAccount</td>
</tr>
<tr>
<td>kms:EnableKey</td>
<td></td>
<td>arn:aws:kms:AWS_region:AWS_account_ID:CMK_key_ID</td>
<td></td>
</tr>
<tr>
<td>EnableKeyRotation</td>
<td>Key policy</td>
<td>CMK</td>
<td>kms:CallerAccount</td>
</tr>
<tr>
<td>kms:EnableKeyRotation</td>
<td></td>
<td>arn:aws:kms:AWS_region:AWS_account_ID:CMK_key_ID</td>
<td></td>
</tr>
<tr>
<td>Encrypt</td>
<td>Key policy</td>
<td>CMK</td>
<td>kms:EncryptionContext:CMK_key_ID</td>
</tr>
<tr>
<td>GenerateDataKey</td>
<td>Key policy</td>
<td>CMK</td>
<td>kms:EncryptionContext:CMK_key_ID</td>
</tr>
<tr>
<td>kms:GenerateDataKey</td>
<td></td>
<td>arn:aws:kms:AWS_region:AWS_account_ID:CMK_key_ID</td>
<td></td>
</tr>
<tr>
<td>GenerateDataKeyWithoutPlaintext</td>
<td>Key policy</td>
<td>CMK</td>
<td>kms:EncryptionContext:CMK_key_ID</td>
</tr>
<tr>
<td>kms:GenerateDataKeyWithoutPlaintext</td>
<td></td>
<td>arn:aws:kms:AWS_region:AWS_account_ID:CMK_key_ID</td>
<td></td>
</tr>
<tr>
<td>GenerateRandom</td>
<td>IAM policy</td>
<td>*</td>
<td>None</td>
</tr>
<tr>
<td>kms:GenerateRandom</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>API Operations and Actions (Permissions)</td>
<td>Policy Type</td>
<td>Resources and ARNs (for IAM Policies)</td>
<td>AWS KMS Condition Keys</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>-------------</td>
<td>--------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>GetKeyPolicy</td>
<td>Key policy</td>
<td>CMK</td>
<td>kms:CallerAccount</td>
</tr>
<tr>
<td>kms:GetKeyPolicy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>arn:aws:kms:AWS_region:AWS_account_ID:key/CMK_key_ID</td>
<td></td>
</tr>
<tr>
<td>GetKeyRotationStatus</td>
<td>Key policy</td>
<td>CMK</td>
<td>kms:CallerAccount</td>
</tr>
<tr>
<td>kms:GetKeyRotationStatus</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>arn:aws:kms:AWS_region:AWS_account_ID:key/CMK_key_ID</td>
<td></td>
</tr>
<tr>
<td>ListAliases</td>
<td>IAM policy</td>
<td>*</td>
<td>None</td>
</tr>
<tr>
<td>kms:ListAliases</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ListGrants</td>
<td>Key policy</td>
<td>CMK</td>
<td>kms:CallerAccount</td>
</tr>
<tr>
<td>kms:ListGrants</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>arn:aws:kms:AWS_region:AWS_account_ID:key/CMK_key_ID</td>
<td></td>
</tr>
<tr>
<td>ListKeyPolicies</td>
<td>Key policy</td>
<td>CMK</td>
<td>kms:CallerAccount</td>
</tr>
<tr>
<td>kms:ListKeyPolicies</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>arn:aws:kms:AWS_region:AWS_account_ID:key/CMK_key_ID</td>
<td></td>
</tr>
<tr>
<td>ListKeys</td>
<td>IAM policy</td>
<td>*</td>
<td>None</td>
</tr>
<tr>
<td>kms:ListKeys</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ListRetirableGrants</td>
<td>IAM policy</td>
<td>*</td>
<td>None</td>
</tr>
<tr>
<td>kms:ListRetirableGrants</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PutKeyPolicy</td>
<td>Key policy</td>
<td>CMK</td>
<td>kms:CallerAccount</td>
</tr>
<tr>
<td>kms:PutKeyPolicy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>arn:aws:kms:AWS_region:AWS_account_ID:key/CMK_key_ID</td>
<td></td>
</tr>
<tr>
<td>ReEncrypt</td>
<td>Key policy</td>
<td>CMK</td>
<td>kms:CallerAccount</td>
</tr>
<tr>
<td>kms:ReEncryptFrom</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kms:ReEncryptTo</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>This operation requires access to two CMKs, one for the decryption (kms:ReEncryptFrom) and one for the subsequent encryption (kms:ReEncryptTo). Users need permissions for both.</td>
<td></td>
<td>arn:aws:kms:AWS_region:AWS_account_ID:key/CMK_key_ID</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

46
Using Policy Conditions with AWS KMS

You can specify conditions in the key policies (p. 24) and IAM policies (p. 40) that control access to AWS KMS resources. The policy statement is effective only when the conditions are true. For example, you might want a policy statement to take effect only after a specific date. Or, you might want a policy statement to control access only when a specific value appears in an API request.

To specify conditions, you use predefined condition keys in the Condition element of a policy statement. Some condition keys apply generally to AWS; others are specific to AWS KMS.

Topics
AWS Condition Keys

AWS provides AWS global condition keys, a set of predefined condition keys for all AWS services that use IAM for access control. For example, you can use the aws:MultiFactorAuthPresent condition key to require multi-factor authentication (MFA). For more information and a list of the global condition keys, see Available Global Condition Keys in the IAM User Guide.

Topics

- Using the IP Address Condition in Policies with AWS KMS Permissions (p. 48)
- Using VPC Endpoint Conditions in Policies with AWS KMS Permissions (p. 48)

Using the IP Address Condition in Policies with AWS KMS Permissions

You can use AWS KMS to protect your data in an integrated AWS service (p. 96). But use caution when specifying the IP address condition operators or the aws:SourceIp condition key in the same policy statement that allows or denies access to AWS KMS. For example, the policy in AWS: Denies Access to AWS Based on the Source IP restricts AWS actions to requests from the specified IP range.

Consider this scenario:

1. You attach a policy like the one shown at AWS: Denies Access to AWS Based on the Source IP to an IAM user. You set the value of the aws:SourceIp condition key to the range of IP addresses for the user's company. This IAM user has other policies attached that allow it to use Amazon EBS, Amazon EC2, and AWS KMS.

2. The user attempts to attach an encrypted EBS volume to an EC2 instance. This action fails with an authorization error even though the user has permission to use all the relevant services.

Step 2 fails because the request to AWS KMS to decrypt the volume's encrypted data key comes from an IP address that is associated with the Amazon EC2 infrastructure. To succeed, the request must come from the IP address of the originating user. Because the policy in step 1 explicitly denies all requests from IP addresses other than those specified, Amazon EC2 is denied permission to decrypt the EBS volume's encrypted data key.

Also, the aws:sourceIp condition key is not effective when the request comes from an Amazon VPC endpoint. To restrict requests to a VPC endpoint, including an AWS KMS VPC endpoint (p. 156), use the aws:sourceVpce or aws:sourceVpc condition keys. For more information, see VPC Endpoints - Controlling the Use of Endpoints in the Amazon VPC User Guide.

Using VPC Endpoint Conditions in Policies with AWS KMS Permissions

AWS KMS supports Amazon Virtual Private Cloud (Amazon VPC) endpoints (p. 156) that are powered by AWS PrivateLink. You can use the following global condition keys in IAM policies to grant or deny access to a particular VPC or VPC endpoint.

You can also use these condition keys in AWS KMS key policies (p. 160) to restrict access to AWS KMS CMKs to requests from the VPC or VPC endpoint.
• `aws:SourceVpc` limits access to requests from the specified VPC.
• `aws:SourceVpce` limits access to requests from the specified VPC endpoint.

You can also use these condition keys in AWS KMS key policies to restrict access to AWS KMS CMKs to requests from the VPC or VPC endpoint.

If you use these condition keys in a key policy statement that allows or denies access to AWS KMS CMKs, you might inadvertently deny access to services that use AWS KMS on your behalf.

Take care to avoid a situation like the IP address condition keys (p. 48) example. If you restrict requests for a CMK to a VPC or VPC endpoint, calls to AWS KMS from an integrated service, such as Amazon S3 or Amazon EBS, might fail. This can happen even if the source request ultimately originates in the VPC or from the VPC endpoint.

**AWS KMS Condition Keys**

AWS KMS provides an additional set of predefined condition keys that you can use in key policies and IAM policies. These condition keys are specific to AWS KMS. For example, you can use the `kms:EncryptionContext` condition key to require a particular encryption context (p. 175) when controlling access to a KMS customer master key (CMK).

The following topics describe each AWS KMS condition key and include example policy statements that demonstrate policy syntax.

**Topics**

- `kms:BypassPolicyLockoutSafetyCheck` (p. 49)
- `kms:CallerAccount` (p. 50)
- `kms:EncryptionContext:` (p. 51)
- `kms:EncryptionContextKeys` (p. 52)
- `kms:GrantConstraintType` (p. 52)
- `kms:GrantIsForAWSResource` (p. 53)
- `kms:GrantOperations` (p. 54)
- `kms:ReEncryptOnSameKey` (p. 54)
- `kms:ViaService` (p. 55)

**kms:BypassPolicyLockoutSafetyCheck**

<table>
<thead>
<tr>
<th>AWS KMS Condition Keys</th>
<th>Condition Type</th>
<th>API Operations</th>
<th>Policy Type</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>kms:BypassPolicyLockoutSafetyCheck</code> (p. 49)</td>
<td>Boolean</td>
<td>CreateKey</td>
<td>IAM policies only</td>
</tr>
</tbody>
</table>

You can use this condition key to control access to the `CreateKey` operation based on the `BypassPolicyLockoutSafetyCheck` parameter in the request. For example, you can prevent users from bypassing the policy lockout safety check by denying them permission to create CMKS when the request's `BypassPolicyLockoutSafetyCheck` parameter is true. This is shown in the following example policy statement from an IAM policy.

{ }
"Version": "2012-10-17",
"Statement": {
  "Effect": "Deny",
  "Action": ["kms:CreateKey"],
  "Resource": ["*"],
  "Condition": {
    "Bool": {
      "kms:BypassPolicyLockoutSafetyCheck": true
    }
  }
},

**kms:CallerAccount**

<table>
<thead>
<tr>
<th>AWS KMS Condition Keys</th>
<th>Condition Type</th>
<th>API Operations</th>
<th>Policy Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>kms:CallerAccount (p. 50)</td>
<td>String</td>
<td>The kms:CallerAccount condition key exists for all AWS KMS operations except for these: CreateKey, GenerateRandom, ListAliases, ListKeys, ListRetirableGrants, RetireGrant.</td>
<td>Key policies only</td>
</tr>
</tbody>
</table>

You can use this condition key to allow or deny access to all identities (IAM users and roles) in an AWS account. In key policies, you use the `Principal` element to specify the identities to which the policy statement applies. The syntax for the `Principal` element does not provide a way to specify all identities in an AWS account. But you can achieve this effect by combining this condition key with a `Principal` element that specifies all AWS identities.

For example, the following policy statement demonstrates how to use the `kms:CallerAccount` condition key. This policy statement is in the key policy for the AWS-managed CMK for Amazon EBS. It combines a `Principal` element that specifies all AWS identities with the `kms:CallerAccount` condition key to effectively allow access to all identities in AWS account 111122223333. It contains an additional AWS KMS condition key (`kms:ViaService`) to further limit the permissions by only allowing requests that come through Amazon EBS. For more information, see `kms:ViaService` (p. 55).

```json
{
  "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:PutKeyPolicy",
    "kms:GetKeyPolicy",
    "kms:DescribeKey",
    "kms:EnableKeyRotation",..."```
You can use this condition key prefix to control access based on the encryption context (p. 175) in the AWS KMS API request. Encryption context is a set of key–value pairs that you can include with AWS KMS API operations that perform encryption and decryption (Encrypt, Decrypt, GenerateDataKey, GenerateDataKeyWithoutPlaintext, and ReEncrypt). Use this condition key prefix to check both sides of the encryption context; that is, both the key and the value. To use this condition key prefix, pair it with the encryption context key to form a custom condition key, like this:

**kms:EncryptionContext:**

<table>
<thead>
<tr>
<th>AWS KMS Condition Keys</th>
<th>Condition Type</th>
<th>API Operations</th>
<th>Policy Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>kms:EncryptionContext:</td>
<td>String</td>
<td>Encrypt, Decrypt, GenerateDataKey, GenerateDataKeyWithoutPlaintext, ReEncrypt</td>
<td>IAM and key policies</td>
</tr>
</tbody>
</table>

The following example policy statement uses the **kms:EncryptionContext:** condition key prefix to allow access to use a CMK only when the encryption context contains the following key–value pairs:

- AppName = ExampleApp
- FilePath = /var/opt/secrets/

To do this, the **kms:EncryptionContext:** condition key prefix is paired with each encryption context key to form custom condition keys (**kms:EncryptionContext:AppName** and **kms:EncryptionContext:FilePath**).

The following example shows a policy statement in a key policy:

```json
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:AppName": "ExampleApp",
      "kms:EncryptionContext:FilePath": "/var/opt/secrets/
    }
  }
}
```
**kms:EncryptionContextKeys**

<table>
<thead>
<tr>
<th>AWS KMS Condition Keys</th>
<th>Condition Type</th>
<th>API Operations</th>
<th>Policy Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>kms:EncryptionContextKeys</td>
<td>String</td>
<td>Encrypt, Decrypt, GenerateDataKey,</td>
<td>IAM and key policies</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GenerateDataKeyWithoutPlaintext, ReEncrypt</td>
<td></td>
</tr>
</tbody>
</table>

You can use this condition key to control access based on the encryption context (p. 175) in the AWS KMS API request. Encryption context is a set of key–value pairs that you can include with AWS KMS API operations that perform encryption and decryption (Encrypt, Decrypt, GenerateDataKey, GenerateDataKeyWithoutPlaintext, and ReEncrypt). Use this condition key to check only the encryption context keys, not the values.

The following example policy statement uses the kms:EncryptionContextKeys condition key with the Null condition operator to allow access to use a CMK only when the request contains encryption context. It does this by allowing access only when the kms:EncryptionContextKeys condition key exists (is not null) in the API request. It does not check the keys or values of the encryption context, only that the encryption context exists. The example shows a policy statement in a key policy.

```json
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": [
    "kms:Encrypt",
    "kms:GenerateDataKey*"
  ],
  "Resource": "+",
  "Condition": {
    "Null": {
      "kms:EncryptionContextKeys": false
    }
  }
}
```

**kms:GrantConstraintType**

<table>
<thead>
<tr>
<th>AWS KMS Condition Keys</th>
<th>Condition Type</th>
<th>API Operations</th>
<th>Policy Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>kms:GrantConstraintType</td>
<td>String</td>
<td>CreateGrant</td>
<td>IAM and key policies</td>
</tr>
</tbody>
</table>

You can use this condition key to control access to the CreateGrant operation based on the type of grant constraint in the request. When you create a grant, you can optionally specify a grant constraint to allow
the operations permitted by the grant only when a particular encryption context is present. The grant constraint can be one of two types: EncryptionContextEquals or EncryptionContextSubset. You can use this condition key to check that the request contains one type or the other. For more information about grant constraints, see GrantConstraints in the AWS Key Management Service API Reference.

The following example policy statement uses the kms:GrantConstraintType condition key to allow a user to create grants only when the request includes an EncryptionContextEquals grant constraint. The example shows a policy statement in a key policy.

```
{
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:user/ExampleUser"
    },
    "Action": "kms:CreateGrant",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:GrantConstraintType": "EncryptionContextEquals"
        }
    }
}
```

**kms:GrantIsForAWSResource**

<table>
<thead>
<tr>
<th>AWS KMS Condition Keys</th>
<th>Condition Type</th>
<th>API Operations</th>
<th>Policy Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>kms:GrantIsForAWSResource</td>
<td>Boolean</td>
<td>CreateGrant</td>
<td>IAM and key policies</td>
</tr>
</tbody>
</table>

You can use this condition key to control access to the CreateGrant operation based on whether the grant is created in the context of an AWS service integrated with AWS KMS (p. 96). This condition key is set to true when one of the following integrated services is used to create the grant:

- Amazon Elastic Block Store (Amazon EBS) – For more information, see How Amazon Elastic Block Store (Amazon EBS) Uses AWS KMS (p. 103).
- Amazon Relational Database Service (Amazon RDS) – For more information, see How Amazon Relational Database Service (Amazon RDS) Uses AWS KMS (p. 113).
- Amazon Redshift – For more information, see How Amazon Redshift Uses AWS KMS (p. 112).
- AWS Certificate Manager (ACM) – For more information, see ACM Private Key Security in the AWS Certificate Manager User Guide.

For example, the following policy statement uses the kms:GrantIsForAWSResource condition key to allow a user to create grants only through one of the integrated services in the preceding list. It does not allow the user to create grants directly. The example shows a policy statement in a key policy.

```
{
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:user/ExampleUser"
    },
    "Action": "kms:CreateGrant",
    "Resource": "*",
    "Condition": {
        "Bool": {
            "kms:GrantIsForAWSResource": true
        }
    }
}
```
You can use this condition key to control access to the `CreateGrant` operation based on the grant operations in the request. For example, you can allow a user to create grants that delegate permission to encrypt but not decrypt.

The following example policy statement uses the `kms:GrantOperations` condition key to allow a user to create grants that delegate permission to encrypt and to reencrypt when this CMK is the destination CMK. The example shows a policy statement in a key policy.

```json
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:user/ExampleUser"
  },
  "Action": "kms:CreateGrant",
  "Resource": "*",
  "Condition": {
    "ForAllValues:StringEquals": {
      "kms:GrantOperations": [
        "Encrypt",
        "ReEncryptTo"
      ]
    }
  }
}
```

You can use this condition key to control access to the `ReEncrypt` operation based on whether the request specifies a destination CMK that is the same one used for the original encryption. For example, the following policy statement uses the `kms:ReEncryptOnSameKey` condition key to allow a user to reencrypt only when the destination CMK is the same one used for the original encryption. The example shows a policy statement in a key policy.

```json
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:user/ExampleUser"
  },
  "Action": "kms:ReEncrypt",
  "Resource": "*",
  "Condition": {
    "Equal": {
      "kms:ReEncryptOnSameKey": true
    }
  }
}
```
"AWS": "arn:aws:iam::111122223333:user/ExampleUser",

"Action": "ReEncrypt*",
"Resource": "*",
"Condition": {
  "Bool": {
    "kms:ReEncryptOnSameKey": true
  }
}

### kms:ViaService

<table>
<thead>
<tr>
<th>AWS KMS Condition Keys</th>
<th>Condition Type</th>
<th>API Operations</th>
<th>Policy Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>kms:ViaService (p. 55)</td>
<td>String</td>
<td>The kms:ViaService condition key exists for all AWS KMS operations except for these: CreateKey, GenerateRandom, ListAliases, ListKeys, ListRetirableGrants, RetireGrant.</td>
<td>IAM and key policies</td>
</tr>
</tbody>
</table>

You can use a kms:ViaService condition key to control access to a CMK when the CMK is used in the context of an **AWS service that is integrated with AWS KMS** (p. 96). For example, you can allow a user to use a CMK only through one particular integrated service. To do this, use the kms:ViaService condition key with the KMS ViaService name for the service. You can specify one or more services in each kms:ViaService condition key.

**Important**
When you use the kms:ViaService condition key, verify that the principals have the following permissions:

- Permission to use the CMK. The principal needs to grant these permissions to the integrated service so it can use the CMK on its behalf. For more information, see How AWS Services use AWS KMS (p. 96).
- Permission to use the integrated service. For details about giving users access to an AWS service that integrates with AWS KMS, consult the documentation for the integrated service.

The following table shows the KMS ViaService name for each service that supports the kms:ViaService condition key. The services in this table might not be available in all regions.

#### Services that support the kms:ViaService condition key

<table>
<thead>
<tr>
<th>Service Name</th>
<th>KMS ViaService Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS Certificate Manager (ACM)</td>
<td>acm.AWS_region.amazonaws.com</td>
</tr>
<tr>
<td>AWS CodeCommit</td>
<td>codecommit.AWS_region.amazonaws.com</td>
</tr>
<tr>
<td>Amazon Connect</td>
<td>connect.AWS_region.amazonaws.com</td>
</tr>
</tbody>
</table>
## AWS Key Management Service Developer Guide

### AWS KMS Condition Keys

<table>
<thead>
<tr>
<th>Service Name</th>
<th>KMS ViaService Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS Database Migration Service (AWS DMS)</td>
<td>dms.AWS_region.amazonaws.com</td>
</tr>
<tr>
<td>Amazon EC2 Systems Manager</td>
<td>ssm.AWS_region.amazonaws.com</td>
</tr>
<tr>
<td>Amazon Elastic Block Store (Amazon EBS)</td>
<td>ec2.AWS_region.amazonaws.com (EBS only)</td>
</tr>
<tr>
<td>Amazon Elastic File System</td>
<td>elasticfilesystem.AWS_region.amazonaws.com</td>
</tr>
<tr>
<td>Amazon Kinesis</td>
<td>kinesis.AWS_region.amazonaws.com</td>
</tr>
<tr>
<td>AWS Lambda</td>
<td>lambda.AWS_region.amazonaws.com</td>
</tr>
<tr>
<td>Amazon Lex</td>
<td>lex.AWS_region.amazonaws.com</td>
</tr>
<tr>
<td>Amazon Lightsail</td>
<td>lightsail.AWS_region.amazonaws.com</td>
</tr>
<tr>
<td>Amazon Redshift</td>
<td>redshift.AWS_region.amazonaws.com</td>
</tr>
<tr>
<td>Amazon Relational Database Service (Amazon RDS)</td>
<td>rds.AWS_region.amazonaws.com</td>
</tr>
<tr>
<td>Amazon Simple Email Service (Amazon SES)</td>
<td>ses.AWS_region.amazonaws.com</td>
</tr>
<tr>
<td>Amazon Simple Storage Service (Amazon S3)</td>
<td>s3.AWS_region.amazonaws.com</td>
</tr>
<tr>
<td>AWS Snowball</td>
<td>importexport.AWS_region.amazonaws.com</td>
</tr>
<tr>
<td>Amazon SQS</td>
<td>sqs.AWS_region.amazonaws.com</td>
</tr>
<tr>
<td>Amazon WorkMail</td>
<td>workmail.AWS_region.amazonaws.com</td>
</tr>
<tr>
<td>Amazon WorkSpaces</td>
<td>workspaces.AWS_region.amazonaws.com</td>
</tr>
</tbody>
</table>

The following example shows a policy statement from a key policy. The policy statement uses the `kms:ViaService` condition key to control access to a set of AWS KMS actions. It allows access only when the CMK is used through Amazon EBS or Amazon RDS in the US West (Oregon) region.

```json
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:user/ExampleUser"
  },
  "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"
      ]
    }
  }
}
```
Using Grants

AWS KMS supports two resource-based access control mechanisms: key policies and grants. Grants enable you to programatically delegate the use of KMS customer master keys (CMKs) to other AWS principals. You can also use key policies to allow other principals to access a CMK, but key policies work best for relatively static assignments of permissions.

Key policy changes follow the same permissions model used for policy editing elsewhere in AWS. That is, users either have permission to change the key policy or they do not. Users with the kms:PutKeyPolicy permission for a CMK can completely replace the key policy for a CMK with a different key policy of their choice. To enable more granular permissions management, use grants.

You call the CreateGrant API operation to create a grant. You pass the identifier of the CMK for which the grant is to be created, the grantee principal being given permission to use the CMK, and a list of operations to be allowed. The CreateGrant operation returns a grant ID that you can use to identify the grant in subsequent operations. To further customize the grant permissions, you can also pass optional parameters that define grant constraints. After the grant has been created, the principal identified in the grant can execute the permitted operations, subject to the defined constraints, for as long as the grant is active. Grants can be explicitly revoked by a user who has the kms:RevokeGrant permission on the CMK, or they can be retired by the principal designated as the retiring principal for the grant.

There are two supported grant constraints: EncryptionContextEquals and EncryptionContextSubset. EncryptionContextEquals specifies that the grant applies only when the exact specified encryption context is present in the request. EncryptionContextSubset specifies that the grant applies as long as all the entries in the EncryptionContextSubset constraint are matched by the request. In this case, the request can contain additional encryption context entries. For example, a grant that allows the encrypt and decrypt operations with an EncryptionContextSubset constraint of \{"Department":"Finance","Classification":"Public"\} allows encryption and decryption when the request contains an encryption context of either \{"Department":"Finance","Classification":"Public"\} or \{"Department":"Finance","Classification":"Public","Customer":"12345"\}, but not when the request contains an encryption context of \{"Department":"Finance"\}.

When the grant includes CreateGrant as an allowed operation, the grant only allows creation of equally or more restrictive grants. That is, the grant operations passed with a subsequent CreateGrant API request can include any subset of the currently-allowed grant operations, and the grant constraints can be the same or more restrictive (fields can be added to an EncryptionContextSubset constraint, or an EncryptionContextSubset constraint can be turned into an EncryptionContextEquals constraint).

For Java code samples that demonstrate how to work with grants, see Working with Grants (p. 168).

Determining Access to an AWS KMS Customer Master Key

To determine the full extent of who or what currently has access to a customer master key (CMK) in AWS KMS, you must examine the CMK's key policy, all grants (p. 57) that apply to the CMK, and potentially all AWS Identity and Access Management (IAM) policies. You might do this to determine the scope of potential usage of a CMK, or to help you meet compliance or auditing requirements. The following topics
can help you generate a complete list of the AWS principals (identities) that currently have access to a CMK.

Topics
- Understanding Policy Evaluation (p. 58)
- Examining the Key Policy (p. 58)
- Examining IAM Policies (p. 61)
- Examining Grants (p. 62)

Understanding Policy Evaluation

When authorizing access to a CMK, AWS KMS evaluates the key policy attached to the CMK, all grants that apply to the CMK, and all IAM policies attached to the IAM user or role making the request. In many cases, AWS KMS must evaluate the CMK's key policy and IAM policies together to determine whether access to the CMK is allowed or denied. To do this, AWS KMS uses a process similar to the one described at Determining Whether a Request is Allowed or Denied in the IAM User Guide. Remember, though, that IAM policies by themselves are not sufficient to allow access to a KMS CMK. The CMK's key policy must also allow access.

For example, assume that you have two CMKs and three users, all in the same AWS account. The CMKs and users have the following policies:

- CMK1's key policy allows access to the AWS account (root user) and thereby enables IAM policies to allow access to CMK1 (p. 25).
- CMK2's key policy allows access to Alice and Charlie.
- Alice has no IAM policy.
- Bob's IAM policy allows all AWS KMS actions for all CMKs.
- Charlie's IAM policy denies all AWS KMS actions for all CMKs.

Alice cannot access CMK1 because CMK1's key policy does not explicitly allow her access, and she has no IAM policy that allows access. Alice can access CMK2 because the CMK’s key policy explicitly allows her access.

Bob can access CMK1 because CMK1’s key policy enables IAM policies to allow access, and Bob has an IAM policy that allows access. Bob cannot access CMK2 because the key policy for CMK2 does not allow access to the account, so Bob’s IAM policy does not by itself allow access to CMK2.

Charlie cannot access CMK1 or CMK2 because all AWS KMS actions are denied in his IAM policy. The explicit deny in Charlie’s IAM policy overrides the explicit allow in CMK2’s key policy.

Examining the Key Policy

You can examine the key policy in two ways:

- If the CMK was created in the AWS Management Console, you can use the console’s default view on the key details page to view the principals listed in the key policy. If you can view the key policy in this way, it means the key policy allows access with IAM policies (p. 25). Be sure to examine IAM policies (p. 61) to determine the complete list of principals that can access the CMK.
- You can use the GetKeyPolicy operation in the AWS KMS API to retrieve a copy of the key policy document, and then examine the document. You can also view the policy document in the AWS Management Console.

Ways to examine the key policy
Examining the Key Policy in the AWS Management Console

To view a customer master key (CMK)'s permissions on the key details page (console)

1. Sign in to the AWS Management Console and open the AWS Identity and Access Management (IAM) console at https://console.aws.amazon.com/iam/.
2. In the left navigation pane, choose Encryption keys.
3. For Region, choose the appropriate AWS Region. Do not use the region selector in the navigation bar (top right corner).
4. In the list of keys, choose the alias of the key that you want to examine.
5. In the Key Policy section of the key details page, find the list of IAM users and roles in the Key Administrators section, and another list in the Key Users section. The listed users, roles, and AWS accounts all have access to manage or use this CMK.

   Important
   The IAM users, roles, and AWS accounts listed here are the ones that have been explicitly granted access in the key policy. If you use IAM policies to allow access to CMKs, other IAM users and roles might have access to this CMK, even if they are not listed here. Take care to examine all IAM policies (p. 61) in this account to determine if they allow access to this CMK.
6. (Optional) To view the key policy document, choose Switch to policy view.

Examining the Key Policy Document

You can view the key policy document in a couple of ways:

- Use the key details page of the AWS Management Console (see the preceding section for instructions).
- Use the GetKeyPolicy operation in the AWS KMS API to retrieve a copy of the key policy document.

Examine the key policy document and take note of all principals specified in each policy statement's Principal element. The IAM users, IAM roles, and AWS accounts in the Principal elements are those that have access to this CMK.

The following examples use the policy statements found in the default key policy (p. 25) to demonstrate how to do this.

Example Policy Statement 1

```json
{"Sid": "Enable IAM User Permissions",
"Effect": "Allow",
"Principal": {"AWS": "arn:aws:iam::111122223333:root"},
"Action": "kms:*",
"Resource": "*"}
```

In the preceding policy statement, arn:aws:iam::111122223333:root refers to the AWS account 111122223333. By default, a policy statement like this one is present in the key policy document when you create a new CMK with the console, and when you create a new CMK programmatically but do not provide a key policy.
A key policy document with a statement that allows access to the AWS account (root user) enables IAM policies in the account to allow access to the CMK (p. 25). This means that IAM users and roles in the account might have access to the CMK even if they are not explicitly listed as principals in the key policy document. Take care to examine all IAM policies (p. 61) in all AWS accounts listed as principals to determine whether they allow access to this CMK.

**Example Policy Statement 2**

```json
{
    "Sid": "Allow access for Key Administrators",
    "Effect": "Allow",
    "Principal": {"AWS": "arn:aws:iam::111122223333:user/KMSKeyAdmin"},
    "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": "*"
}
```

In the preceding policy statement, `arn:aws:iam::111122223333:user/KMSKeyAdmin` refers to the IAM user named KMSKeyAdmin in AWS account 111122223333. This user is allowed to perform the actions listed in the policy statement, which are the administrative actions for managing a CMK.

**Example Policy Statement 3**

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

In the preceding policy statement, `arn:aws:iam::111122223333:role/EncryptionApp` refers to the IAM role named EncryptionApp in AWS account 111122223333. Principals that can assume this role are allowed to perform the actions listed in the policy statement, which are the cryptographic actions for encrypting and decrypting data with a CMK.

**Example Policy Statement 4**

```json
{
    "Sid": "Allow attachment of persistent resources",
    "Effect": "Allow",
    "Principal": {"AWS": "arn:aws:iam::111122223333:role/EncryptionApp"},
    "Action": [
       "kms:PutKeyPolicy",
       "kms:DescribeKey",
       "kms:ListKeyVersions",
       "kms:ListTemplates",
       "kms:ListKeyIds",
       "kms:GetPublicKey",
       "kms:CreateGrant",
       "kms:DeleteKeyPolicy",
       "kms:CreateGrant",
       "kms:ListGrants",
       "kms:GetKeyPolicy",
       "kms:ReEncrypt*",
       "kms:EnableKey",
       "kms:GetKeyPolicy",
       "kms:PutGrant",
       "kms:ReEncrypt*",
       "kms:GenerateDataKey"  
    ],
    "Resource": "*"
}
```

In the preceding policy statement, `arn:aws:iam::111122223333:role/EncryptionApp` refers to the IAM role named EncryptionApp in AWS account 111122223333. Principals that can assume this role are allowed to perform the actions listed in the policy statement, which are the additional actions for managing persistent resources with a CMK.
In the preceding policy statement, `arn:aws:iam::111122223333:role/EncryptionApp` refers to the IAM role named EncryptionApp in AWS account 111122223333. Principals that can assume this role are allowed to perform the actions listed in the policy statement. These actions, when combined with the actions allowed in Example policy statement 3, are those necessary to delegate use of the CMK to most AWS services that integrate with AWS KMS (p. 96), specifically the services that use grants (p. 57). The Condition element ensures that the delegation is allowed only when the delegate is an AWS service that integrates with AWS KMS and uses grants for authorization.

To learn all the different ways you can specify a principal in a key policy document, see Specifying a Principal in the IAM User Guide.

To learn more about AWS KMS key policies, see Using Key Policies in AWS KMS (p. 24).

Examining IAM Policies

In addition to the key policy and grants, you can also use IAM policies in combination with a CMK's key policy to allow access to a CMK. For more information about how IAM policies and key policies work together, see Understanding Policy Evaluation (p. 58).

To determine which principals currently have access to a CMK through IAM policies, you can use the browser-based IAM Policy Simulator tool, or you can make requests to the IAM API.

Ways to examine IAM policies

- Examining IAM Policies with the IAM Policy Simulator (p. 61)
- Examining IAM Policies with the IAM API (p. 62)

Examining IAM Policies with the IAM Policy Simulator

The IAM Policy Simulator can help you learn which principals have access to a KMS CMK through an IAM policy.

To use the IAM Policy Simulator to determine access to a KMS CMK

1. Sign in to the AWS Management Console and then open the IAM Policy Simulator at https://policysim.aws.amazon.com/.
2. In the Users, Groups, and Roles pane, choose the user, group, or role whose policies you want to simulate.
3. (Optional) Clear the check box next to any policies that you want to omit from the simulation. To simulate all policies, leave all policies selected.
4. In the Policy Simulator pane, do the following:
   a. For Select service, choose Key Management Service.
   b. To simulate specific AWS KMS actions, for Select actions, choose the actions to simulate. To simulate all AWS KMS actions, choose Select All.
5. (Optional) The Policy Simulator simulates access to all KMS CMKs by default. To simulate access to a specific KMS CMK, select Simulation Settings and then type the Amazon Resource Name (ARN) of the KMS CMK to simulate.
6. Select **Run Simulation**.

You can view the results of the simulation in the **Results** section. Repeat steps 2 through 6 for every IAM user, group, and role in the AWS account.

### Examining IAM Policies with the IAM API

You can use the IAM API to examine IAM policies programmatically. The following steps provide a general overview of how to do this:

1. For each AWS account listed as a principal in the CMK’s key policy (that is, each *root account* listed in this format: **"Principal": {"AWS": "arn:aws:iam::111122223333:root"}**), use the **ListUsers** and **ListRoles** operations in the IAM API to retrieve a list of every IAM user and role in the account.

2. For each IAM user and role in the list, use the **SimulatePrincipalPolicy** operation in the IAM API, passing in the following parameters:
   - For **PolicySourceArn**, specify the Amazon Resource Name (ARN) of a user or role from your list. You can specify only one **PolicySourceArn** for each **SimulatePrincipalPolicy** API request, so you must call this API multiple times, once for each IAM user and role in your list.
   - For the **ActionNames** list, specify every AWS KMS API action to simulate. To simulate all AWS KMS API actions, use **kms:***. To test individual AWS KMS API actions, precede each API action with "**kms:**", for example "**kms:**ListKeys". For a complete list of all AWS KMS API actions, see **Actions** in the **AWS Key Management Service API Reference**.
   - (Optional) To determine whether the IAM users or roles have access to specific KMS CMKs, use the **ResourceArns** parameter to specify a list of the Amazon Resource Names (ARNs) of the CMKs. To determine whether the IAM users or roles have access to any CMK, do not use the **ResourceArns** parameter.

IAM responds to each **SimulatePrincipalPolicy** API request with an evaluation decision: **allowed**, **explicitDeny**, or **implicitDeny**. For each response that contains an evaluation decision of **allowed**, the response will also contain the name of the specific AWS KMS API action that is allowed and, if applicable, the ARN of the CMK that was used in the evaluation.

### Examining Grants

Grants are advanced mechanisms for specifying permissions that you or an AWS service integrated with AWS KMS can use to specify how and when a CMK can be used. Grants are attached to a CMK, and each grant contains the principal who receives permission to use the CMK and a list of operations that are allowed. Grants are an alternative to the key policy, and are useful for specific use cases. For more information, see Using Grants (p. 57).

To retrieve a list of grants attached to a CMK, use the AWS KMS **ListGrants** API (or **list-grants** AWS CLI command). You can examine the grants for a CMK to determine who or what currently has access to use the CMK via those grants. For example, the following is a JSON representation of a grant that was obtained from the **list-grants** command in the AWS CLI.

```json
{"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": "dc716f5c39acacaf291b1540de3e5a232b76256c83b2ecb22cd6fa26576a2d3e",
  "IssuingAccount": "arn:aws:iam::111122223333:root",
  "CreationDate": 1.444151834E9,
}]
```
"Constraints": {"EncryptionContextSubset": {"aws:ebs:id": "vol-5cccfb4e"}}
}}

To find out who or what has access to use the CMK, look for the "GranteePrincipal" element. In the preceding example, the grantee principal is an assumed role user associated with the EC2 instance i-5d476fab, which the EC2 infrastructure uses to attach the encrypted EBS volume vol-5cccfb4e to the instance. In this case, the EC2 infrastructure role has permission to use the CMK because you previously created an encrypted EBS volume protected by this CMK, and then attached the volume to an EC2 instance.

The following is another example of a JSON representation of a grant that was obtained from the list-grants command in the AWS CLI. In the following example, the grantee principal is another AWS account.

{"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": "f271e8328717f8be5d03f4981f06a6b3fc18bca5a2da12a38bd9186e7925d11",
  "IssuingAccount": "arn:aws:iam::111122223333:root",
  "CreationDate": 1.444151269E9
}]}
Rotating Customer Master Keys

Cryptographic best practices discourage extensive reuse of encryption keys. To create new cryptographic material for your AWS Key Management Service (AWS KMS) customer master keys (CMKs), you can create new CMKs, and then change your applications or aliases to use the new CMKs. Or, you can enable automatic key rotation for an existing CMK.

When you enable automatic key rotation for a customer managed CMK, AWS KMS generates new cryptographic material for the CMK every year. AWS KMS also saves the CMK's older cryptographic material so it can be used to decrypt data that it encrypted.

Key rotation changes only the CMK's backing key, which is the cryptographic material that is used in encryption operations. The properties of the CMK do not change, as shown in the following image. The CMK is the same logical resource, regardless of whether or how many times its backing key changes.

Automatic key rotation has the following benefits:

- The properties of the CMK, including its key ID, key ARN, region, policies, and permissions, do not change when the key is rotated.
- You do not need to change applications or aliases that refer to the CMK ID or ARN.
- After you enable key rotation, AWS KMS rotates the CMK automatically every year. You don't need to remember or schedule the update.

However, you might decide to create a new CMK and use it in place of the original CMK. This has the same effect as rotating the key material in an existing CMK, so it's often thought of as manually rotating the key (p. 67). Manual rotation is a good choice when you want to control the key rotation schedule. It also provides a way to rotate CMKs with imported key material.

More Information About Key Rotation

Rotating customer managed CMKs might result in extra monthly charges. For details, see AWS Key Management Service Pricing. For more detailed information about backing keys and rotation, see the KMS Cryptographic Details whitepaper.

Topics

- How Automatic Key Rotation Works (p. 65)
- How to Enable and Disable Automatic Key Rotation (p. 65)
How Automatic Key Rotation Works

Key rotation in AWS KMS is a cryptographic best practice that is designed to be transparent and easy to use.

- **Backing key management.** AWS KMS retains all backing keys for a CMK, even if key rotation is disabled. The backing keys are deleted only when the CMK is deleted. When you use a CMK to encrypt, AWS KMS uses the current backing key. When you use the CMK to decrypt, AWS KMS uses the backing key that was used to encrypt.

- **Enable and disable key rotation.** Automatic key rotation is disabled by default on customer managed CMKs. When you enable (or re-enable) key rotation, AWS KMS automatically rotates the CMK 365 days after the enable date and every 365 days thereafter.

- **Disabled CMKs.** While a CMK is disabled, AWS KMS does not rotate it. However, the underlying key rotation status does not change, and you cannot change it while the CMK is disabled. When the CMK is re-enabled, if the backing key is more than 365 days old, AWS KMS rotates it immediately and every 365 days thereafter. If the backing key is less than 365 days old, AWS KMS resumes the original key rotation schedule.

- **CMKs pending deletion.** While a CMK is pending deletion, AWS KMS does not rotate it. The key rotation status is set to `false` and you cannot change it while deletion is pending. If deletion is canceled, the previous key rotation status is restored. If the backing key is more than 365 days old, AWS KMS rotates it immediately and every 365 days thereafter. If the backing key is less than 365 days old, AWS KMS resumes the original key rotation schedule.

- **Customer managed CMKs.** Automatic key rotation is available for all customer managed CMKs with KMS-generated key material. It is not available for CMKs that have imported key material (p. 69) (the value of the Origin field is External), but you can rotate these CMKs manually (p. 67).

- **AWS managed CMKs.** You cannot manage key rotation for AWS managed CMKs. AWS KMS automatically rotates AWS managed keys every three years (1095 days).

- **Logging key rotation.** When AWS KMS rotates a CMK, it writes the KMS CMK Rotation event to Amazon CloudWatch Events. You can use this event to verify that the CMK was rotated.

How to Enable and Disable Automatic Key Rotation

You can use the AWS KMS console or the AWS KMS API to enable and disable automatic key rotation, and view the rotation status of any customer managed CMK.

When you enable automatic key rotation, AWS KMS rotates the CMK 365 days after the enable date and every 365 days thereafter.
Enabling and Disabling Key Rotation in the Console

To enable or disable automatic key rotation, start at the key details page for the CMK.

1. Sign in to the AWS Management Console and open the AWS Identity and Access Management (IAM) console at https://console.aws.amazon.com/iam/.
2. In the left navigation pane, choose Encryption keys.
3. For Region, choose the appropriate AWS Region. Do not use the region selector in the navigation bar (top right corner).
4. Choose the alias of the CMK whose details you want to see.

   **Note**
   You cannot edit AWS managed CMKs, which are identified by the orange AWS icon.

5. Use the controls in the Key Rotation section of the page.

   **Note**
   If a CMK is disabled or pending deletion, the Key Rotation check box is cleared, and you cannot change it. This reminds you that AWS KMS does not rotate CMKs while they are disabled or pending deletion. The key rotation status is restored when you re-enable the CMK or cancel deletion. For details, see How Automatic Key Rotation Works (p. 65).

**Enabling and Disabling Key Rotation with the API**

You can use the AWS Key Management Service (AWS KMS) API to enable and disable automatic key rotation, and view the current rotation status of any customer managed CMK. These examples use the AWS Command Line Interface (AWS CLI), but you can use any supported programming language.

The EnableKeyRotation operation enables automatic key rotation for the specified CMK. The DisableKeyRotation operation disables it. To identify the CMK, use its key ID, key ARN, alias name, or alias ARN. By default, key rotation is disabled for customer managed CMKs.

The following example enables key rotation on the specified CMK and uses the GetKeyRotationStatus operation to see the result. Then, it disables key rotation and, again, uses GetKeyRotationStatus to see the change.

```bash
$ aws kms enable-key-rotation --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
$ aws kms get-key-rotation-status --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
{   "KeyRotationEnabled": true
}
$ aws kms disable-key-rotation --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
$ aws kms get-key-rotation-status --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
{   "KeyRotationEnabled": false
}
```
Rotating Keys Manually

You might want to create a new CMK and use it in place of a current CMK instead of enabling automatic key rotation. When the new CMK has different cryptographic material than the current CMK, using the new CMK has the same effect as changing the backing key in an existing CMK. The process of replacing one CMK with another is known as manual key rotation.

You might prefer to rotate keys manually so you can control the rotation frequency. It’s also a good solution for CMKs that are not eligible for automatic key rotation, such as CMKs with imported key material (p. 69).

**Note**

When you begin using the new CMK, be sure to keep the original CMK enabled so that AWS KMS can decrypt data that the original CMK encrypted. When decrypting data, KMS identifies the CMK that was used to encrypt the data, and it uses the same CMK to decrypt the data. As long as you keep both the original and new CMKs enabled, AWS KMS can decrypt any data that was encrypted by either CMK.

Because the new CMK is a different resource from the current CMK, it has a different key ID and ARN. When you change CMKs, you need to update references to the CMK ID or ARN in your applications. Aliases, which associate a friendly name with a CMK, make this process easier. Use an alias to refer to a CMK in your applications. Then, when you want to change the CMK that the application uses, change the target CMK of the alias.

To update the target CMK of an alias, use UpdateAlias operation in the AWS KMS API. For example, this command updates the TestCMK alias to point to a new CMK. Because the operation does not return any output, the example uses the ListAliases operation to show that the alias is now associated with a different CMK.

```bash
$ aws kms list-aliases
```
```json
{
   "Aliases": [
      {
         "AliasName": "alias/TestCMK",
         "TargetKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
      }
   ]
}

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

$ aws kms list-aliases
{
   "Aliases": [
      {
         "AliasName": "alias/TestCMK",
         "TargetKeyId": "0987dcba-09fe-87dc-65ba-ab0987654321"
      }
   ]
}
```
Importing Key Material in AWS Key Management Service (AWS KMS)

A customer master key (CMK) is a logical representation of a master key in AWS KMS. In addition to the master key's identifiers and other metadata including its creation date, description, and key state (p. 93), a CMK contains the key material used to encrypt and decrypt data. When you create a CMK (p. 5), by default AWS KMS generates the key material for that CMK. But you can choose to create a CMK without key material and then import your own key material into that CMK.

When you use imported key material, you remain responsible for the key material while allowing AWS KMS to use a copy of it. You might choose to do this for one or more of the following reasons:

- To prove that you generated the key material using a source of randomness that meets your requirements.

- To use key material from your own infrastructure with AWS services, and to use AWS KMS to manage the lifecycle of that key material within AWS.

- To gain the ability to set an expiration time for the key material in AWS and to manually delete it (p. 78), but to also make it available again in the future. In contrast, scheduling key deletion (p. 81) requires a waiting period of 7 to 30 days, after which you cannot recover the deleted CMK.

- To own the original copy of the key material, and to keep it outside of AWS for additional durability and disaster recovery during the complete lifecycle of the key material.

For information about important differences between CMKs with imported key material and those with key material generated by AWS KMS, see Considerations for Imported Key Material (p. 70).

The key material you import must be a 256-bit symmetric encryption key.

Topics

- How To Import Key Material (p. 69)
- Considerations for Imported Key Material (p. 70)

How To Import Key Material

The following overview describes the process to import your key material into AWS KMS. For more details about each step in the process, see the corresponding topic.

1. Create a CMK with no key material (p. 71) – To get started with importing key material, first create a CMK whose origin is EXTERNAL. This indicates that the key material was generated outside of AWS.
KMS and prevents AWS KMS from generating key material for the CMK. In a later step you will import your own key material into this CMK.

2. **Download the public key and import token (p. 73)** – After completing step 1, download a public key and an import token. These items protect the import of your key material to AWS KMS.

3. **Encrypt the key material (p. 76)** – Use the public key that you downloaded in step 2 to encrypt the key material that you created on your own system.

4. **Import the key material (p. 77)** – Upload the encrypted key material that you created in step 3 and the import token that you downloaded in step 2.

## Considerations for Imported Key Material

Before you decide to import key material into AWS KMS, you should understand the following characteristics of imported key material.

**Availability and durability**

You remain responsible for the key material's overall availability and durability. AWS KMS is designed to keep imported key material highly available, but the service does not maintain the durability of imported key material at the same level as key material generated on your behalf. This difference is meaningful in the following cases:

- When you set an expiration time for your imported key material, AWS KMS deletes the key material after it expires. AWS KMS does not delete the CMK or its metadata. You cannot set an expiration time for key material generated by AWS KMS.
- When you manually delete imported key material (p. 78), AWS KMS deletes the key material but does not delete the CMK or its metadata. In contrast, **scheduling key deletion** (p. 81) requires a waiting period of 7 to 30 days, after which AWS KMS deletes the key material and all of the CMK's metadata.
- In the unlikely event of certain regionwide failures that affect the service (such as a total loss of power), AWS KMS cannot automatically restore your imported key material. However, AWS KMS can restore the CMK and its metadata.

To make your key material available again after any of these events, you must retain a copy of the key material in a system that you control so that you can reimport it into the original CMK.

**Secure key generation**

You are responsible for generating the key material using a source of randomness that meets your security requirements.

**One key per CMK**

When you import key material into a CMK, the CMK is permanently associated with that key material. You cannot import different key material into that CMK, and you cannot **enable automatic key rotation** (p. 64) for a CMK with imported key material. However, you can manually rotate a CMK with imported key material. To do so, **create a new CMK** (p. 71) and then import the new key material into that CMK. Then change the CMK identifier in your applications or AWS service configurations to the key ID for the new CMK. Also, if you have a KMS alias that points to the old CMK, you can update it to point to the new one to complete the rotation process.
Ciphertexts are not portable between CMKs

When you encrypt data under a KMS CMK, the ciphertext cannot be decrypted with any other CMK. This applies to all KMS CMKs, and remains true even when you import the same key material into a different CMK.

Importing Key Material Step 1: Create an AWS KMS Customer Master Key (CMK) With No Key Material

By default, AWS KMS creates key material for you when you create a customer master key (CMK). To instead import your own key material, start by creating a CMK with no key material. You distinguish between these two types of CMKs by the CMK’s origin. When AWS KMS creates the key material for you, the CMK’s origin is AWS_KMS. When you create a CMK with no key material, the CMK’s origin is EXTERNAL, which indicates that the key material was generated outside of AWS KMS.

A CMK with no key material is in the pending import state and is not available for use. To use it, you must import key material as explained later. When you import key material, the CMK’s key state changes to enabled. For more information about key state, see How Key State Affects Use of a Customer Master Key (p. 93).

To create a CMK with no key material, you can use the AWS Management Console or the AWS KMS API. You can use the API directly by making HTTP requests, or through one of the AWS SDKs or command line tools.

Topics
- Create a CMK with No Key Material (AWS Management Console) (p. 71)
- Create a CMK with No Key Material (AWS KMS API) (p. 72)

Create a CMK with No Key Material (AWS Management Console)

You can use the AWS Management Console to create a CMK with no key material. Before you do this, you can configure the console to show additional columns in the list of KMS CMKs to more easily distinguish your CMKs with imported key material.

To show additional columns in the list of KMS CMKs
1. Sign in to the AWS Management Console and open the AWS Identity and Access Management (IAM) console at https://console.aws.amazon.com/iam/.
2. In the left navigation pane, choose Encryption keys.
3. For Region, choose the appropriate AWS Region. Do not use the region selector in the navigation bar (top right corner).
4. Choose the settings button in the upper-right corner of the page.
5. Select the check boxes for Expiration Date and Origin, and then choose Close.

To create a CMK with no key material (console)

You need to create a CMK for the imported key material only once. To reimport the same key material into an existing CMK, see Step 2: Download the Public Key and Import Token (p. 73).
1. Sign in to the AWS Management Console and open the AWS Identity and Access Management (IAM) console at https://console.aws.amazon.com/iam/.
2. In the left navigation pane, choose Encryption keys.
3. For Region, choose the appropriate AWS Region. Do not use the region selector in the navigation bar (top right corner).
4. Choose Create key.
5. Type an alias and (optionally) a description for the CMK.
6. Choose Advanced Options.
7. For Key Material Origin, choose External. Then select the check box next to I understand the security, availability, and durability implications of using an imported key to indicate that you understand the implications of using imported key material. To read about these implications, choose the security, availability, and durability implications link.
8. Select which IAM users and roles can administer the CMK. For more information, see Allows Key Administrators to Administer the CMK (p. 26).
   Note
   All IAM users and roles with IAM policies that specify the appropriate permissions can also administer the CMK.
9. Select which IAM users and roles can use the CMK to encrypt and decrypt data. For more information, see Allows Key Users to Use the CMK (p. 28).
   Note
   All IAM users and roles with IAM policies that specify the appropriate permissions can also use the CMK.
10. (Optional) At the bottom of the page, you can give permissions to other AWS accounts to use the CMK to encrypt and decrypt data. Choose Add an External Account and then type the AWS account ID of the account to give permissions to. Repeat as necessary to add more than one external account.
   Note
   Administrators of the external accounts must also allow access to the CMK by creating IAM policies for their users. For more information, see Allowing External AWS Accounts to Access a CMK (p. 37).
11. Choose Finish to create the CMK.
   After you complete this step, the console displays the Import key material wizard. To continue the process now, see Download the Public Key and Import Token (AWS Management Console) (p. 74).

     Otherwise, choose Skip and do this later. To find your CMK in the list, you can show additional columns as described previously, or you can look in the Status column for Pending Import. Your new CMK remains in the Pending Import state until you import key material as described in the following steps.

Proceed to Step 2: Download the Public Key and Import Token (p. 73).

Create a CMK with No Key Material (AWS KMS API)

To use the AWS KMS API to create a CMK with no key material, send a CreateKey request with the Origin parameter set to EXTERNAL. The following example shows how to do this with the AWS Command Line Interface (AWS CLI).
When the command is successful, you see output similar to the following. The CMK's Origin is EXTERNAL and its KeyState is PendingImport.

```
{
    "KeyMetadata": {
        "Origin": "EXTERNAL",
        "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "Description": "",
        "Enabled": false,
        "KeyUsage": "ENCRYPT_DECRYPT",
        "KeyState": "PendingImport",
        "CreationDate": 1470811233.761,
        "Arn": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "AWSAccountId": "111122223333"
    }
}
```

Copy the CMK's key ID from your command output to use in later steps, and then proceed to Step 2: Download the Public Key and Import Token (p. 73).

Importing Key Material Step 2: Download the Public Key and Import Token

After you create a customer master key (CMK) with no key material (p. 71), you download a public key and import token for that CMK. You need these items to import your key material, and you can download both items in one step using the AWS Management Console or the AWS KMS API.

You also download these items when you want to reimport key material into a CMK. You might do this to change the expiration time for the key material, or to restore a CMK after the key material has expired or been deleted.

Use of the public key

When you import key material, you don't upload the raw key material to AWS KMS. You must first encrypt the key material with the public key that you download in this step, and then upload the encrypted key material to AWS KMS. When AWS KMS receives your encrypted key material, it uses the corresponding private key to decrypt it. The public key you receive from AWS KMS is a 2048-bit RSA public key and is always unique to your AWS account.

Use of the import token

The import token contains metadata to ensure that your key material is imported correctly. When you upload your encrypted key material to AWS KMS, you must upload the same import token that you download in this step.

Plan ahead

Before you download a public key and import token, you must determine how you will encrypt your key material. Typically, you choose an option based on the capabilities of the hardware security module (HSM) or key management system that protects your key material. You must use the RSA PKCS #1 encryption scheme with one of three padding options, represented by the following choices. These choices are listed in order of AWS preference. The technical details of the schemes represented by these choices are explained in section 7 of the PKCS #1 Version 2.1 standard.
• **RSAES_OAEP_SHA_256** – The RSA encryption algorithm with Optimal Asymmetric Encryption Padding (OAEP) with the SHA-256 hash function.

• **RSAES_OAEP_SHA_1** – The RSA encryption algorithm with Optimal Asymmetric Encryption Padding (OAEP) with the SHA-1 hash function.

• **RSAES_PKCS1_V1_5** – The RSA encryption algorithm with the padding format defined in PKCS #1 Version 1.5.

**Note**
If you plan to try the Encrypt Key Material with OpenSSL (p. 76) proof-of-concept example in Step 3 (p. 76), use RSAES_OAEP_SHA_1.

If your HSM or key management system supports it, we recommending using RSAES_OAEP_SHA_256 to encrypt your key material. If that option is not available, you should use RSAES_OAEP_SHA_1. If neither of the OAEP options are available, you must use RSAES_PKCS1_V1_5. For information about how to encrypt your key material, see the documentation for the hardware security module or key management system that protects your key material.

The public key and import token are valid for 24 hours. If you don't use them to import key material within 24 hours of downloading them, you must download new ones.

To download the public key and import token, you can use the AWS Management Console or the AWS KMS API. You can use the API directly by making HTTP requests, or through one of the AWS SDKs or command line tools.

**Topics**
- Download the Public Key and Import Token (AWS Management Console) (p. 74)
- Download the Public Key and Import Token (AWS KMS API) (p. 75)

**Download the Public Key and Import Token (AWS Management Console)**

You can use the AWS Management Console to download the public key and import token. If you just completed the steps to create a CMK with no key material (p. 71), skip to Step 6.

**To download the public key and import token (console)**

1. Sign in to the AWS Management Console and open the AWS Identity and Access Management (IAM) console at https://console.aws.amazon.com/iam/.
2. In the left navigation pane, choose **Encryption keys**.
3. For **Region**, choose the appropriate AWS Region. Do not use the region selector in the navigation bar (top right corner).
4. Choose the alias of the CMK for which you are downloading the public key and import token.
   
   **Tip**
   The CMK’s **Origin** must be **External**. If you don't see the **Origin** column, choose the settings button (⚙️) in the upper-right corner of the page. Select the check box next to **Origin**, and then choose **Close**.
5. In the **Key Material** section of the page, choose **Download wrapping key and import token**.
6. For **Select wrapping algorithm**, choose the option that you will use to encrypt your key material. For more information about the options, see the preceding section.

   If you plan to try the Encrypt Key Material with OpenSSL (p. 76) proof-of-concept example in Step 3 (p. 76), choose RSAES_OAEP_SHA_1.
7. Choose **Download wrapping key and import token**, and then save the file.
8. Decompress the .zip file that you saved in the previous step (ImportParameters.zip).

   The folder contains the following files:

   - The wrapping key (public key), in a file named wrappingKey_CMK_key_ID_timestamp (for example, wrappingKey_f44c4e20-f83c-48f4-adc6-1ae6f38829760_0809092909). This is a 2048-bit RSA public key.
   - The import token, in a file named importToken_CMK_key_ID_timestamp (for example, importToken_f44c4e20-f83c-48f4-adc6-1ae6f38829760_0809092909).
   - A text file named README_CMK_key_ID_timestamp.txt (for example, README_f44c4e20-f83c-48f4-adc6-1ae6f38829760_0809092909.txt). This file contains information about the wrapping key (public key), the wrapping algorithm to use to encrypt your key material, and the date and time when the wrapping key (public key) and import token expire.

   To continue the process now, proceed to the next step. Otherwise, choose **Skip and do this later** and then proceed to **Step 3: Encrypt the Key Material** (p. 76).

9. (Optional) To continue the process now, **encrypt your key material** (p. 76). Then do one of the following:

   - If you are in the Import key material wizard, select the check box for **I am ready to upload my exported key material** and choose **Next**.
   - If you are in the key details page, choose **Upload key material**.

After you complete this step, proceed to **Step 3: Encrypt the Key Material** (p. 76).

### Download the Public Key and Import Token (AWS KMS API)

To use the **AWS KMS API** to download the public key and import token, send a `GetParametersForImport` request that specifies the CMK for which you are downloading these items. The following example shows how to do this with the **AWS CLI**.

This example specifies RSAES_OAEP_SHA_1 as the encryption option. To specify a different option, replace `RSAES_OAEP_SHA_1` with `RSAES_OAEP_SHA_256` or `RSAES_PKCS1_V1_5`. Replace `1234abcd-12ab-34cd-56ef-1234567890ab` with the key ID of the CMK for which to download the public key and import token. You can use the CMK's key ID or Amazon Resource Name (ARN), but you cannot use an alias for this operation.

**Note**

If you plan to try the **Encrypt Key Material with OpenSSL** (p. 76) proof-of-concept example in **Step 3** (p. 76), specify `RSAES_OAEP_SHA_1`.

```bash
$ aws kms get-parameters-for-import --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
   --wrapping-algorithm RSAES_OAEP_SHA_1
   --wrapping-key-spec RSA_2048
```

When the command is successful, you see output similar to the following:

```json
{
   "ParametersValidTo": 1470933314.949,
   "PublicKey": "public key base64 encoded data",
   "KeyId": "arn:aws:kms:us-west-2:1111222333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
   "ImportToken": "import token base64 encoded data"
}
```
When you receive this output, save the base64 encoded public key and import token in separate files. Then base64 decode each file into binary data and save the binary data in new files. Doing so prepares these items for later steps. See the following example.

**To prepare the public key and import token for later steps**

1. Copy the public key's base64 encoded data (represented by *public key base64 encoded data* in the example output), paste it into a new file, and then save the file. Give the file a descriptive name, for example *PublicKey.b64*.
2. Use OpenSSL to base64 decode the file's contents and save the decoded data to a new file. The following example decodes the data in the file that you saved in the previous step (*PublicKey.b64*) and saves the output to a new file named *PublicKey.bin*.

```bash
$ openssl enc -d -base64 -A -in PublicKey.b64 -out PublicKey.bin
```

Repeat these two steps for the import token, and then proceed to **Step 3: Encrypt the Key Material**.

---

**Importing Key Material Step 3: Encrypt the Key Material**

After you download the public key and import token (p. 73), you use the public key to encrypt your key material. The key material must be in binary format.

Typically, you encrypt your key material when you export it from your hardware security module (HSM) or key management system. For information about how to export key material in binary format, see the documentation for your HSM or key management system. You can also refer to the following section that provides a proof of concept demonstration using OpenSSL.

When you encrypt your key material, use the encryption scheme with the padding option that you specified when you downloaded the public key and token (p. 73) (RSAES_OAEP_SHA_256, RSAES_OAEP_SHA_1, or RSAES_PKCS1_V1_5).

**Example: Encrypt Key Material with OpenSSL**

The following example demonstrates how to use OpenSSL to generate a 256-bit symmetric key and then encrypt this key material for import into AWS KMS customer master key (CMK).

**Important**

This example is a proof of concept demonstration only. For production systems, use a more secure method (such as a commercial HSM or key management system) to generate and store your key material.

The *RSAES_OAEP_SHA_1* encryption algorithm works best with this example. Before running the example, make sure that you used *RSAES_OAEP_SHA_1* for the wrapping algorithm in **Step 2** (p. 73). If necessary, repeat the step to download and import the public key and token.

**To use OpenSSL to generate binary key material and encrypt it for import into AWS KMS**

1. Use the following command to generate a 256-bit symmetric key and save it in a file named *PlaintextKeyMaterial.bin*. 

---

76
# openssl rand -out PlaintextKeyMaterial.bin 32

2. Use the following command to encrypt the key material with the public key that you downloaded previously (see Download the Public Key and Import Token (AWS KMS API) (p. 75)) and save it in a file named EncryptedKeyMaterial.bin. Replace PublicKey.bin> with the name of the file that contains the public key. If you downloaded the public key from the console, this file is named wrappingKey_CMK_key_ID_timestamp (for example, wrappingKey_f44c4e20-f83c-48f4-adc6-alef38829760_0809092909).

```bash
# openssl rsautl -encrypt \
  -in PlaintextKeyMaterial.bin \ 
  -oaep \ 
  -inkey PublicKey.bin \ 
  -keyform DER \ 
  -pubin \ 
  -out EncryptedKeyMaterial.bin
```

Proceed to Step 4: Import the Key Material (p. 77).

### Importing Key Material Step 4: Import the Key Material

After you encrypt your key material (p. 76), you can import the key material to use with an AWS KMS customer master key (CMK). To import key material, you upload the encrypted key material from Step 3: Encrypt the Key Material (p. 76) and the import token that you downloaded at Step 2: Download the Public Key and Import Token (p. 73). You must import key material into the same CMK that you specified when you downloaded the public key and import token.

When you import key material, you can optionally specify a time at which the key material expires. When the key material expires, AWS KMS deletes the key material and the CMK becomes unusable. To use the CMK again, you must reimport key material.

After you successfully import key material, the CMK's key state changes to enabled, and you can use the CMK.

To import key material, you can use the AWS Management Console or the AWS KMS API. You can use the API directly by making HTTP requests, or through one of the AWS SDKs or command line tools.

**Topics**
- Import Key Material (AWS Management Console) (p. 77)
- Import Key Material (AWS KMS API) (p. 78)

### Import Key Material (AWS Management Console)

You can use the AWS Management Console to import key material. If you just completed the optional final step of downloading the public key and import token with the console (p. 74), skip to Step 6.

**To import key material (console)**

1. Sign in to the AWS Management Console and open the AWS Identity and Access Management (IAM) console at [https://console.aws.amazon.com/iam/](https://console.aws.amazon.com/iam/).
2. In the left navigation pane, choose **Encryption keys**.
3. For **Region**, choose the appropriate AWS Region. Do not use the region selector in the navigation bar (top right corner).
4. Choose the alias of the CMK for which you downloaded the public key and import token.
5. In the **Key Material** section of the page, choose **Upload key material**.
6. In the **Specify key material details** section, for **Encrypted key material**, choose the file that contains your encrypted key material. For **Import token**, choose the file that contains the import token that you downloaded previously (p. 74).
7. In the **Choose an expiration option** section, choose whether the key material expires. If you choose expiration, type a date and a time in the corresponding boxes.
8. Choose **Finish** or **Upload key material**.

### Import Key Material (AWS KMS API)

To use the AWS KMS API to import key material, send an `ImportKeyMaterial` request. The following example shows how to do this with the AWS CLI.

This example specifies an expiration time for the key material. To import key material with no expiration, replace `KEY_MATERIAL_EXPIRES` with `KEY_MATERIAL_DOES_NOT_EXPIRE` and omit the `--valid-to` parameter.

To use this example:

1. Replace `1234abcd-12ab-34cd-56ef-1234567890ab` with the key ID of the CMK that you used when you downloaded the public key and import token. To identify the CMK, use its key ID or ARN. You cannot use an alias for this operation.
2. Replace `EncryptedKeyMaterial.bin` with the name of the file that contains the encrypted key material.
3. Replace `ImportToken.bin` with the name of the file that contains the import token.

```
$ 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 2016-11-08T12:00:00-08:00
```

### Deleting Imported Key Material

When you import key material, you have the option of specifying a time at which the key material expires. When the key material expires, AWS KMS deletes the key material and the customer master key (CMK) becomes unusable. You can also delete key material on demand. Whether you wait for the key material to expire or you delete it manually, the effect is the same. AWS KMS deletes the key material, the CMK's **key state** (p. 93) changes to **pending import**, and the CMK is unusable. To use the CMK again, you must reimport the same key material.

Deleting key material affects the CMK right away, but you can reverse the deletion of key material by reimporting the same key material into the CMK. In contrast, **scheduling key deletion** (p. 81) for a CMK is irreversible. It deletes the key material and all metadata associated with the CMK, and requires a waiting period of between 7 and 30 days.

To delete key material, you can use the AWS Management Console or the AWS KMS API. You can use the API directly by making HTTP requests, or through one of the AWS SDKs or **command line tools**.
How Deleting Key Material Affects AWS Services Integrated With AWS KMS

When you delete key material, the CMK becomes unusable right away. However, *data encryption keys* that are actively in use by AWS services are not immediately affected. This means that deleting key material might not immediately affect all of the data and AWS resources protected under the CMK, though they are affected eventually.

Several [AWS services integrate with AWS KMS](https://aws.amazon.com/kms/enable/) to protect your data, such as Amazon Elastic Block Store (Amazon EBS), Amazon Relational Database Service (Amazon RDS), Amazon Simple Storage Service (Amazon S3), and others. Most of these services use *envelope encryption* to protect your data. Envelope encryption means that the CMK protects a data encryption key (or *data key*), and the data key protects your data. These data keys persist in memory on the AWS service host while the data they are protecting are actively in use. For more information about how envelope encryption works, see [How Envelope Encryption Works with Supported AWS Services](https://docs.aws.amazon.com/kms/latest/developerguide/how-envelopes-work.html).

For example, consider this scenario:

1. You create an encrypted EBS volume, protected under a CMK with imported key material. This action creates a corresponding request to AWS KMS to generate a unique data key for that volume.

2. AWS KMS generates a new data key, encrypts it with the specified CMK, and then sends the encrypted data key to Amazon EBS to store with the volume until you attach the volume to an Amazon Elastic Compute Cloud (Amazon EC2) instance.

3. You attach the EBS volume to an EC2 instance. This action creates a corresponding request to AWS KMS to decrypt the EBS volume's encrypted data key.

4. AWS KMS decrypts the encrypted data key and sends the decrypted (plaintext) data key to Amazon EC2.

5. Amazon EC2 uses the plaintext data key in hypervisor memory to encrypt disk I/O to the EBS volume while the volume is attached to the EC2 instance.

6. You delete the CMK's imported key material. This has no immediate effect on the EC2 instance or the EBS volume, because Amazon EC2 is using the plaintext data key—not the CMK—to encrypt all disk I/O while the volume is attached to the instance.

7. When the EBS volume is detached (due to your explicit request or an event that affects the EBS volume or the EC2 instance), the plaintext data key is deleted from memory. The next attempt to attach the encrypted EBS volume to an EC2 instance fails. It fails because the CMK needed to decrypt the EBS volume's encrypted data key (step 3 in this scenario) is unusable (it has no key material). To use the EBS volume again, you must reimport the same key material into the CMK.
Delete Key Material (AWS Management Console)

You can use the AWS Management Console to delete key material.

To delete key material (console)

1. Sign in to the AWS Management Console and open the AWS Identity and Access Management (IAM) console at https://console.aws.amazon.com/iam/.
2. In the left navigation pane, choose Encryption keys.
3. For Region, choose the appropriate AWS Region. Do not use the region selector in the navigation bar (top right corner).
4. Choose one of the following:
   - Select the check box for the CMK whose key material you want to delete. Choose Key actions, Delete key material.
   - Choose the alias of the CMK whose key material you want to delete. In the Key Material section of the page, choose Delete key material.
5. Confirm that you want to delete the key material and then choose Delete key material. The CMK's key state changes to Pending Import.

Delete Key Material (AWS KMS API)

To use the AWS KMS API to delete key material, send a DeleteImportedKeyMaterial request. The following example shows how to do this with the AWS CLI.

Replace `1234abcd-12ab-34cd-56ef-1234567890ab` with the key ID of the CMK whose key material you want to delete. You can use the CMK's key ID or ARN but you cannot use an alias for this operation.

```
$ aws kms delete-imported-key-material --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```
Deleting Customer Master Keys

Deleting a customer master key (CMK) in AWS Key Management Service (AWS KMS) is destructive and potentially dangerous. It deletes the key material and all metadata associated with the CMK, and is irreversible. After a CMK is deleted you can no longer decrypt the data that was encrypted under that CMK, which means that data becomes unrecoverable. You should delete a CMK only when you are sure that you don't need to use it anymore. If you are not sure, consider disabling the CMK (p. 18) instead of deleting it. You can re-enable a disabled CMK if you need to use it again later, but you cannot recover a deleted CMK.

Before deleting a CMK, you might want to know how many ciphertexts were encrypted under that CMK. AWS KMS does not store this information, and does not store any of the ciphertexts. To get this information, you must determine on your own the past usage of a CMK. For some guidance that might help you do this, go to Determining Past Usage of a Customer Master Key (p. 89).

You might choose to delete a CMK for one or more of the following reasons:

- To complete the key lifecycle for CMKs that you no longer need
- To avoid the management overhead and costs associated with maintaining unused CMKs
- To reduce the number of CMKs that count against your limit (p. 181)

**Note**
If you close or delete your AWS account, your CMKs become inaccessible and you are no longer billed for them. You do not need to schedule deletion of your CMKs separate from closing the account.

**Topics**
- How Deleting Customer Master Keys Works (p. 81)
- Scheduling and Canceling Key Deletion (p. 82)
- Adding Permission to Schedule and Cancel Key Deletion (p. 84)
- Creating an Amazon CloudWatch Alarm to Detect Usage of a Customer Master Key that is Pending Deletion (p. 87)
- Determining Past Usage of a Customer Master Key (p. 89)

How Deleting Customer Master Keys Works

Because it is destructive and potentially dangerous to delete a customer master key (CMK), AWS KMS enforces a waiting period. To delete a CMK in AWS KMS you schedule key deletion. You can set the waiting period from a minimum of 7 days up to a maximum of 30 days. The default waiting period is 30 days.

During the waiting period, the CMK state is pending deletion.

- A CMK that is pending deletion cannot be used in any cryptographic operations.
- AWS KMS does not rotate the backing keys (p. 65) of CMKs that are pending deletion.

After the waiting period ends, AWS KMS deletes the CMK and all AWS KMS data associated with it, including all aliases that point to it.

When you schedule key deletion, AWS KMS reports the date and time when the waiting period ends. This date and time is at least the specified number of days from when you scheduled key deletion, but it can be up to 24 hours longer. For example, when you schedule key deletion and specify a waiting period of
7 days, the end of the waiting period occurs no earlier than 7 days and no more than 8 days from the
time of your request. You can confirm the exact date and time when the waiting period ends in the AWS
Management Console, AWS CLI, or AWS KMS API.

Use the waiting period to ensure that you don't need the CMK now or in the future. You can configure
an Amazon CloudWatch alarm (p. 87) to warn you if a person or application attempts to use the CMK
during the waiting period. To recover the CMK, you can cancel key deletion before the waiting period
ends. After the waiting period ends you cannot cancel key deletion, and AWS KMS deletes the CMK.

How Deleting Customer Master Keys Affects AWS Services Integrated With AWS KMS

Several AWS services integrate with AWS KMS to protect your data. Some of these services, such as
Amazon EBS and Amazon Redshift, continually modify data in your AWS account while they are in use.
These services protect your data using envelope encryption, which means the customer master key (CMK)
in AWS KMS encrypts a data key, and the data key encrypts your data. These data keys persist in memory
as long as the data they are protecting is actively in use. For more information about how envelope
encryption works, go to How Envelope Encryption Works with Supported AWS Services (p. 96).

When you schedule a CMK for deletion it becomes unusable. However, data keys that are actively in use
are unaffected. This means that scheduling a CMK for deletion does not immediately affect resources
and data that are actively in use.

For example, consider this scenario:

1. You create an encrypted EBS volume, at which time Amazon EBS requests a unique data key
   encrypted with the CMK that you specified when creating the volume.
2. AWS KMS creates a new data key, encrypts it with the specified CMK, and then sends the encrypted
data key to Amazon EBS to store with the volume.
3. You attach the EBS volume to an EC2 instance, at which time Amazon EC2 calls the AWS KMS
   Decrypt API to decrypt the EBS volume's encrypted data key. AWS KMS sends the decrypted
   (plaintext) data key to Amazon EC2.
4. Amazon EC2 uses the plaintext data key in hypervisor memory to encrypt disk I/O to the EBS volume.
The data key persists in memory as long as the EBS volume is attached to the EC2 instance.
5. You schedule the CMK for deletion. This has no immediate effect on the EC2 instance or the EBS
   volume, because Amazon EC2 is using the plaintext data key—not the CMK—to encrypt the EBS
   volume.
6. The key deletion waiting period ends, and AWS KMS deletes the CMK. This has no immediate effect
   on the EC2 instance or the EBS volume, because Amazon EC2 is using the plaintext data key—not the
   CMK—to encrypt the EBS volume.

However, the next time the encrypted EBS volume is attached to an EC2 instance, the attachment fails
because at that time Amazon EC2 calls the AWS KMS Decrypt API (step 3 in the preceding scenario) but
the CMK needed for decryption is unusable (it is pending deletion or deleted).

Scheduling and Canceling Key Deletion

The following procedures describe how to schedule key deletion and cancel key deletion in AWS Key
Management Service (AWS KMS) using the AWS Management Console, the AWS CLI, and the AWS SDK
for Java.

Warning
Deleting a customer master key (CMK) in AWS KMS is destructive and potentially dangerous. You
should proceed only when you are sure that you don't need to use the CMK anymore and won't
need to use it in the future. If you are not sure, you should disable the CMK (p. 18) instead of deleting it.

Before you can delete a CMK, you must have permission to do so. If you rely on the key policy alone to specify AWS KMS permissions, you might need to add additional permissions before you can delete the CMK. For information about adding these permissions, go to Adding Permission to Schedule and Cancel Key Deletion (p. 84).

Ways to schedule and cancel key deletion
- Scheduling and Canceling Key Deletion (AWS Management Console) (p. 83)
- Scheduling and Canceling Key Deletion (AWS CLI) (p. 83)
- Scheduling and Canceling Key Deletion (AWS SDK for Java) (p. 84)

Scheduling and Canceling Key Deletion (AWS Management Console)

You can schedule and cancel key deletion in the AWS Management Console.

To schedule key deletion
1. Sign in to the AWS Management Console and open the AWS Identity and Access Management (IAM) console at https://console.aws.amazon.com/iam/.
2. In the left navigation pane, choose Encryption keys.
3. For Region, choose the appropriate AWS Region. Do not use the region selector in the navigation bar (top right corner).
4. Select the check box next to the CMK that you want to delete.
5. Choose Key Actions, Schedule key deletion.
6. For Waiting period (in days), type a number of days between 7 and 30. Choose Schedule deletion.

The CMK status changes to Pending Deletion.

To cancel key deletion
1. Open the IAM console at https://console.aws.amazon.com/iam/.
2. In the left navigation pane, choose Encryption keys.
3. For Region, choose the appropriate AWS Region. Do not use the region selector in the navigation bar (top right corner).
4. Select the check box next to the CMK that you want to recover.
5. Choose Key Actions, Cancel key deletion.

The CMK status changes from Pending Deletion to Disabled. To use the CMK, you must enable it (p. 18).

Scheduling and Canceling Key Deletion (AWS CLI)

Use the `aws kms schedule-key-deletion` command to schedule key deletion from the AWS CLI as shown in the following example.

```bash
# aws kms schedule-key-deletion --key-id 1234abcd-12ab-34cd-56ef-1234567890ab --pending-window-in-days 10
```

When used successfully, the AWS CLI returns output like the output shown in the following example:
Use the `aws kms cancel-key-deletion` command to cancel key deletion from the AWS CLI as shown in the following example.

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

When used successfully, the AWS CLI returns output like the output shown in the following example:

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

The status of the CMK changes from **Pending Deletion** to **Disabled**. To use the CMK, you must enable it (p. 18).

### Scheduling and Canceling Key Deletion (AWS SDK for Java)

The following example demonstrates how to schedule a CMK for deletion with the AWS SDK for Java. This example requires that you previously instantiated an `AWSKMSClient` as `kms`.

```java
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);
```

The following example demonstrates how to cancel key deletion with the AWS SDK for Java. This example requires that you previously instantiated an `AWSKMSClient` as `kms`.

```java
String KeyId = "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
CancelKeyDeletionRequest cancelKeyDeletionRequest = new CancelKeyDeletionRequest().withKeyId(KeyId);
kms.cancelKeyDeletion(cancelKeyDeletionRequest);
```

The status of the CMK changes from **Pending Deletion** to **Disabled**. To use the CMK, you must enable it (p. 18).

### Adding Permission to Schedule and Cancel Key Deletion

If you use IAM policies to allow AWS KMS permissions, all IAM users and roles that have AWS administrator access ("Action": "*") or AWS KMS full access ("Action": "kms:*") are already...
allowed to schedule and cancel key deletion for AWS KMS CMKs. If you rely on the key policy alone to allow AWS KMS permissions, you might need to add additional permissions to allow your IAM users and roles to delete CMKs. To add those permissions, see the following steps.

The following procedures describe how to add permissions to a key policy using the AWS Management Console or the AWS CLI.

**Ways to add permission to schedule and cancel key deletion**
- Adding Permission to Schedule and Cancel Key Deletion (AWS Management Console) (p. 85)
- Adding Permission to Schedule and Cancel Key Deletion (AWS CLI) (p. 86)

**Adding Permission to Schedule and Cancel Key Deletion (AWS Management Console)**

You can use the AWS Management Console to add permissions for scheduling and canceling key deletion.

**To add permission to schedule and cancel key deletion**

1. Sign in to the AWS Management Console and open the AWS Identity and Access Management (IAM) console at https://console.aws.amazon.com/iam/.
2. In the left navigation pane, choose Encryption keys.
3. For Region, choose the appropriate AWS Region. Do not use the region selector in the navigation bar (top right corner).
4. Choose the alias of the CMK whose permissions you want to change.
5. In the Key Policy section, under Key Deletion, select Allow key administrators to delete this key and then choose Save Changes.

**Note**
If you do not see the Allow key administrators to delete this key option, this likely means that you have previously modified this key policy using the AWS KMS API. In this case you must update the key policy document manually. Add the kms:ScheduleKeyDeletion and kms:CancelKeyDeletion permissions to the key administrators statement ("Sid": "Allow access for Key Administrators") in the key policy, and then choose Save Changes.
Adding Permission to Schedule and Cancel Key Deletion (AWS CLI)

You can use the AWS Command Line Interface to add permissions for scheduling and canceling key deletion.

To add permission to schedule and cancel key deletion

1. Use the `aws kms get-key-policy` command to retrieve the existing key policy, and then save the policy document to a file.
2. Open the policy document in your preferred text editor, add the `kms:ScheduleKeyDeletion` and `kms:CancelKeyDeletion` permissions to the policy statement that gives permissions to the key administrators (for example, the policy statement with "Sid": "Allow access for Key Administrators"), and save the file. The following example shows a policy statement with these two permissions:

```json
{
  "Sid": "Allow access for Key Administrators",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:user/KMSKeyAdmin"
  },
  "Action": [
    "kms:ScheduleKeyDeletion",
    "kms:CancelKeyDeletion"
  ],
  "Resource": "*"
}
```
Creating a CloudTrail Trail

Before you begin these procedures, you must have already turned on CloudTrail in the AWS account and region where you intend to monitor AWS KMS API requests. For instructions, go to Creating a Trail for the First Time in the AWS CloudTrail User Guide.

Steps
- Part 1: Configure CloudTrail Log File Delivery to CloudWatch Logs (p. 87)
- Part 2: Create the CloudWatch Alarm (p. 88)

Part 1: Configure CloudTrail Log File Delivery to CloudWatch Logs

You must configure delivery of your CloudTrail log files to CloudWatch Logs so that CloudWatch Logs can monitor them for AWS KMS API requests that attempt to use a customer master key (CMK) that is pending deletion.

Creating an Amazon CloudWatch Alarm to Detect Usage of a Customer Master Key that is Pending Deletion

You can use a combination of AWS CloudTrail, Amazon CloudWatch Logs, and Amazon Simple Notification Service (Amazon SNS) to create an alarm that notifies you of AWS KMS API requests that attempt to use a customer master key (CMK) that is pending deletion. If you receive a notification from such an alarm, you might want to cancel deletion of the CMK to give yourself more time to determine whether you want to delete it.

The following procedures explain how to receive a notification whenever an AWS KMS API request that results in the **Key ARN is pending deletion** error message is written to your CloudTrail log files. Note that not all AWS KMS API requests that use a CMK that is pending deletion result in this error message. For example, you can successfully use the ListKeys, CancelKeyDeletion, and PutKeyPolicy APIs (and others) with CMK that are pending deletion. The intent of this CloudWatch alarm is to detect usage that might indicate that a person or application still expects to use the CMK for cryptographic operations (Encrypt, Decrypt, GenerateDataKey, and others). To see a list of which AWS KMS APIs do and don't result in this error message, go to How Key State Affects Use of a Customer Master Key (p. 93).

Before you begin these procedures, you must have already turned on CloudTrail in the AWS account and region where you intend to monitor AWS KMS API requests. For instructions, go to Creating a Trail for the First Time in the AWS CloudTrail User Guide.

Steps
- Part 1: Configure CloudTrail Log File Delivery to CloudWatch Logs (p. 87)
- Part 2: Create the CloudWatch Alarm (p. 88)

Part 1: Configure CloudTrail Log File Delivery to CloudWatch Logs

You must configure delivery of your CloudTrail log files to CloudWatch Logs so that CloudWatch Logs can monitor them for AWS KMS API requests that attempt to use a customer master key (CMK) that is pending deletion.

3. Use the `aws kms put-key-policy` command to apply the key policy to the CMK.
To configure CloudTrail log file delivery to CloudWatch Logs

1. Sign in to the AWS Management Console and open the CloudTrail console at https://console.aws.amazon.com/cloudtrail/.
2. On the top navigation bar, choose the AWS region in which you intend to monitor activity.
3. If necessary, in the left navigation pane, choose Configuration.
4. In the content pane, in the CloudWatch Logs (Optional) section, choose Configure.
5. If necessary, for New or existing log group, type a name for the log group, such as CloudTrail/DefaultLogGroup, and then choose Continue.
6. On the AWS CloudTrail will deliver CloudTrail events associated with API activity in your account to your CloudWatch Logs log group page, choose Allow.

Part 2: Create the CloudWatch Alarm

To receive a notification when AWS KMS API requests attempt to use a customer master key (CMK) that is pending deletion, you must create a CloudWatch alarm and configure notification.

To create a CloudWatch alarm that monitors attempted usage of a KMS CMK that is pending deletion

1. Sign in to the AWS Management Console and open the CloudWatch console at https://console.aws.amazon.com/cloudwatch/.
2. On the top navigation bar, choose the AWS region in which you intend to monitor activity.
3. In the left navigation pane, choose Logs.
4. In the list of Log Groups, select the check box next to the log group that you created previously, such as CloudTrail/DefaultLogGroup. Then choose Create Metric Filter.
5. For Filter Pattern, type or paste the following:

   `{ $.eventSource = kms* && $.errorMessage = "* is pending deletion." }`

   Choose Assign Metric.
6. On the Create Metric Filter and Assign a Metric page, do the following:

   a. For Metric Namespace, type CloudTrailLogMetrics.
   b. For Metric Name, type KMSKeyPendingDeletionErrorCount.
   c. Choose Show advanced metric settings, and then if necessary for Metric Value, type 1.
   d. Choose Create Filter.
7. In the filter box, choose Create Alarm.
8. In the Create Alarm window, do the following:

   a. For Name, type KMSKeyPendingDeletionErrorAlarm.
   b. Following Whenever, for is:, choose >= and then type 1.
   c. For for consecutive period(s), if necessary, type 1.
   d. Next to Send notification to, do one of the following:
      - To use a new Amazon SNS topic, choose New list, and then type a new topic name. For Email list, type at least one email address. You can type more than one email address by separating them with commas.
      - To use an existing Amazon SNS topic, choose the name of the topic to use.
   e. Choose Create Alarm.
If you chose to send notifications to an email address, open the email message you receive from no-reply@sns.amazonaws.com with a subject “AWS Notification - Subscription Confirmation.” Confirm your email address by choosing the Confirm subscription link in the email message.

Note
You will not receive email notifications until after you have confirmed your email address.

After you complete this procedure, you will receive a notification each time this CloudWatch alarm enters the ALARM state. If you receive a notification for this alarm, it might mean that someone or something still needs to use this CMK. In that case, you should cancel deletion of the CMK (p. 82) to give yourself more time to determine whether you really want to delete it.

Determining Past Usage of a Customer Master Key

Before deleting a customer master key (CMK), you might want to know how many ciphertexts were encrypted under that key. AWS KMS does not store this information, and does not store any of the ciphertexts. To obtain this information, you must determine on your own the past usage of a CMK. Knowing how a CMK was used in the past might help you decide whether or not you will need it in the future. The following guidance can help you determine the past usage of a CMK.

Topics
- Examining CMK Permissions to Determine the Scope of Potential Usage (p. 90)
- Examining AWS CloudTrail Logs to Determine Actual Usage (p. 90)
Examining CMK Permissions to Determine the Scope of Potential Usage

Determining who or what currently has access to a customer master key (CMK) might help you determine how widely the CMK was used and whether it is still needed. To learn how to determine who or what currently has access to a CMK, go to Determining Access to an AWS KMS Customer Master Key (p. 57).

Examining AWS CloudTrail Logs to Determine Actual Usage

AWS KMS is integrated with AWS CloudTrail, so all AWS KMS API activity is recorded in CloudTrail log files. If you have CloudTrail turned on in the region where your customer master key (CMK) is located, you can examine your CloudTrail log files to view a history of all AWS KMS API activity for a particular CMK, and thus its usage history. You might be able to use a CMK's usage history to help you determine whether or not you still need it.

The following examples show CloudTrail log entries that are generated when a KMS CMK is used to protect an object stored in Amazon Simple Storage Service (Amazon S3). In this example, the object is uploaded to Amazon S3 using server-side encryption with AWS KMS-managed keys (SSE-KMS) (p. 117). When you upload an object to Amazon S3 with SSE-KMS, you specify the KMS CMK to use for protecting the object. Amazon S3 uses the AWS KMS GenerateDataKey API to request a unique data key for the object, and this API event is logged in CloudTrail with an entry similar to the following:

```
{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROACKCEVSQ6C2EXAMPLE:example-user",
    "arn": "arn:aws:sts::111122223333:assumed-role/Admns/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/Admns",
        "accountId": "111122223333",
        "userName": "Admns"
      }
    },
    "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,
}  
```
When you later download this object from Amazon S3, Amazon S3 sends a Decrypt API request to AWS KMS to decrypt the object’s data key using the specified CMK. When you do this, your CloudTrail log files include an entry similar to the following:

```
{
  "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-a249-205dda330e3",
  "readOnly": true,
  "resources": [{
    "ARN": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "accountId": "111122223333"
  }],
  "eventType": "AwsApiCall",
  "recipientAccountId": "111122223333"
}
```

All AWS KMS API activity is logged by CloudTrail. By evaluating these log entries, you might be able to determine the past usage of a particular CMK, and this might help you determine whether or not you want to delete it.
To see more examples of how AWS KMS API activity appears in your CloudTrail log files, go to Logging AWS KMS API Calls Using AWS CloudTrail (p. 136). For more information about CloudTrail go to the AWS CloudTrail User Guide.
# How Key State Affects Use of a Customer Master Key

Each customer master key (CMK) in AWS KMS exists in one of three states: enabled, disabled, or pending deletion. Enabled CMKs are available for use. CMKs in the disabled or pending deletion state are available for some APIs, but are unavailable for others. CMKs in the disabled or pending deletion state cannot be used for cryptographic operations.

Consult the following table to learn the result of each AWS KMS API on existing CMKs in each state. The CreateKey and GenerateRandom APIs do not affect existing CMKs, so they are not applicable. The results in this table assume that the API caller is authorized to use the CMK.

**Legend**

- ✔ – Succeeds.
- ❌ – Results in DisabledException with the message "Key ARN is disabled."
- ❌ – Results in DisabledException with the message "Key ARN is pending deletion."
- ❌ – Results in KMSInvalidStateException with the message "Key ARN is pending deletion."
- ❌ – Results in KMSInvalidStateException with the message "Key ARN is not pending deletion."
- 🔄 – Applies only to the UpdateAlias API request. When a CMK that is pending deletion is the "source" key, the request succeeds. When a CMK that is pending deletion is the target key, the request results in KMSInvalidStateException with the message "Key ARN is pending deletion."

N/A – Not applicable

<table>
<thead>
<tr>
<th>API</th>
<th>Enabled</th>
<th>Disabled</th>
<th>Pending Deletion</th>
</tr>
</thead>
<tbody>
<tr>
<td>CancelKeyDeletion</td>
<td>❌</td>
<td>❌</td>
<td>✔</td>
</tr>
<tr>
<td>CreateAlias</td>
<td>✔</td>
<td>✔</td>
<td>🔄</td>
</tr>
<tr>
<td>CreateGrant</td>
<td>✔</td>
<td>❌</td>
<td>❌</td>
</tr>
<tr>
<td>CreateKey</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>API</td>
<td>Enabled</td>
<td>Disabled</td>
<td>Pending Deletion</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------</td>
<td>----------</td>
<td>------------------</td>
</tr>
<tr>
<td>Decrypt</td>
<td>✔️</td>
<td>✖️</td>
<td>✖️</td>
</tr>
<tr>
<td>DeleteAlias</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>DescribeKey</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>DisableKey</td>
<td>✔️</td>
<td>✔️</td>
<td>✖️</td>
</tr>
<tr>
<td>DisableKeyRotation</td>
<td>✔️</td>
<td>✖️</td>
<td>✖️</td>
</tr>
<tr>
<td>EnableKey</td>
<td>✔️</td>
<td>✔️</td>
<td>✖️</td>
</tr>
<tr>
<td>EnableKeyRotation</td>
<td>✔️</td>
<td>✖️</td>
<td>✖️</td>
</tr>
<tr>
<td>Encrypt</td>
<td>✔️</td>
<td>✖️</td>
<td>✖️</td>
</tr>
<tr>
<td>GenerateDataKey</td>
<td>✔️</td>
<td>✖️</td>
<td>✖️</td>
</tr>
<tr>
<td>GenerateDataKeyWithoutPlaintext</td>
<td>✔️</td>
<td>✖️</td>
<td>✖️</td>
</tr>
<tr>
<td>GenerateRandom</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>GetKeyPolicy</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>GetKeyRotationStatus</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>ListAliases</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>ListGrants</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>ListKeyPolicies</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>ListKeys</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>ListRetireableGrants</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>API</td>
<td>Enabled</td>
<td>Disabled</td>
<td>Pending Deletion</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------</td>
<td>----------</td>
<td>-----------------</td>
</tr>
<tr>
<td>PutKeyPolicy</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>ReEncrypt</td>
<td>✔️</td>
<td>☠️</td>
<td>☠️</td>
</tr>
<tr>
<td>RetireGrant</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>RevokeGrant</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>ScheduleKeyDeletion</td>
<td>✔️</td>
<td>✔️</td>
<td>☢️</td>
</tr>
<tr>
<td>UpdateAlias</td>
<td>✔️</td>
<td>✔️</td>
<td>☝️</td>
</tr>
<tr>
<td>UpdateKeyDescription</td>
<td>✔️</td>
<td>✔️</td>
<td>☢️</td>
</tr>
</tbody>
</table>
How AWS Services use AWS KMS

Several AWS services use AWS KMS to provide encryption of customer data. The following topics discuss the details of how each service uses AWS KMS. The first topic in the list describes in general terms how envelope encryption works in the context of the supported services.

Topics
- How Envelope Encryption Works with Supported AWS Services (p. 96)
- How AWS CloudTrail Uses AWS KMS (p. 98)
- How Amazon Elastic Block Store (Amazon EBS) Uses AWS KMS (p. 103)
- How Amazon Elastic Transcoder Uses AWS KMS (p. 105)
- How Amazon EMR Uses AWS KMS (p. 109)
- How Amazon Redshift Uses AWS KMS (p. 112)
- How Amazon Relational Database Service (Amazon RDS) Uses AWS KMS (p. 113)
- How Amazon Simple Email Service (Amazon SES) Uses AWS KMS (p. 114)
- How Amazon Simple Storage Service (Amazon S3) Uses AWS KMS (p. 117)
- How AWS Systems Manager Parameter Store Uses AWS KMS (p. 118)
- How Amazon WorkMail Uses AWS KMS (p. 123)
- How Amazon WorkSpaces Uses AWS KMS (p. 125)

How Envelope Encryption Works with Supported AWS Services

This topic describes how and when AWS KMS generates, encrypts, and decrypts keys that can be used to encrypt your data in a supported AWS service.

Envelope Encryption

AWS KMS supports two kinds of keys—master keys and data keys. Master keys can be used to directly encrypt and decrypt up to 4 kilobytes (4096 bytes) of data and can also be used to protect data keys. The data keys are then used to encrypt and decrypt customer data.

Customer master keys are stored securely in AWS KMS. They can never be exported from AWS KMS. Data keys created inside of AWS KMS can be exported and are protected for export by being encrypted under a master key. The data key encryption process is illustrated by the following diagram:
Encrypting User Data

When an AWS application or service requests a data key, AWS KMS returns both the encrypted and plaintext key. The service uses the plaintext data key to encrypt the user's data in memory. The plaintext key should never be written to disk and should be deleted from memory as soon as practical. The encrypted copy of the data key should be written to disk alongside of the encrypted data. This is an acceptable security practice that simplifies management of the encrypted data key.

Decrypting User Data

Decryption reverses the encryption process. When a service or application decrypts data, it sends AWS KMS the encrypted data key. AWS KMS automatically uses the correct customer master key to decrypt the data key. Then, it sends the plaintext key back to the service or application that requested it. The application or service uses the plaintext key to decrypt the data. The plaintext key should never be written to disk and should be deleted as soon as practical. The following illustration shows the customer master key used with a symmetric decryption algorithm to decrypt the data key.
The next illustration shows the plaintext data key and symmetric algorithm used together to decrypt the user's encrypted data. The plaintext data key should be removed from memory as soon as is practical.

Managed Keys in AWS Services and in Custom Applications

You can choose to encrypt data in one of the services integrated with AWS KMS by using the AWS-managed key for that service under your account. In this case, all users who have access to that service can use the key. For more granular control, you can choose to create a customer-managed key and set policies that define who can use the key and what actions the users can perform.

How AWS CloudTrail Uses AWS KMS

You can use AWS CloudTrail to record AWS API calls and other activity for your AWS account and to save the recorded information to log files in an Amazon Simple Storage Service (Amazon S3) bucket that you choose. By default, the log files delivered by CloudTrail to your S3 bucket are encrypted using server-side encryption with Amazon S3–managed encryption keys (SSE-S3). But you can choose instead to use server-side encryption with AWS KMS–managed keys (SSE-KMS). To learn how to encrypt your CloudTrail log files with AWS KMS, see Encrypting CloudTrail Log Files with AWS KMS–Managed Keys (SSE-KMS) in the AWS CloudTrail User Guide.

Topics
- Understanding When Your CMK is Used (p. 99)
- Understanding How Often Your CMK is Used (p. 102)
Understanding When Your CMK is Used

Encrypting CloudTrail log files with AWS KMS builds on the Amazon S3 feature called server-side encryption with AWS KMS–managed keys (SSE-KMS). To learn more about SSE-KMS, see How Amazon Simple Storage Service (Amazon S3) Uses AWS KMS (p. 117) in this guide or Protecting Data Using Server-Side Encryption with AWS KMS–Managed Keys (SSE-KMS) in the Amazon Simple Storage Service Developer Guide.

When you configure AWS CloudTrail to use SSE-KMS to encrypt your log files, CloudTrail and Amazon S3 use your KMS customer master key (CMK) when you perform certain actions with those services. The following sections explain when and how those services can use your CMK, and provide additional information that you can use to validate this explanation.

Actions that cause CloudTrail and Amazon S3 to use your CMK

- You Configure CloudTrail to Encrypt Log Files with Your Customer Master Key (CMK) (p. 99)
- CloudTrail Puts a Log File into Your S3 Bucket (p. 100)
- You Get an Encrypted Log File from Your S3 Bucket (p. 101)

You Configure CloudTrail to Encrypt Log Files with Your Customer Master Key (CMK)

When you update your CloudTrail configuration to use your CMK, CloudTrail sends a `GenerateDataKey` request to AWS KMS to verify that the CMK exists and that CloudTrail has permission to use it for encryption. CloudTrail does not use the resulting data key.

The `GenerateDataKey` request includes the following information for the encryption context (p. 175):

- The Amazon Resource Name (ARN) of the CloudTrail trail
- The ARN of the S3 bucket and path where the CloudTrail log files are delivered

The `GenerateDataKey` request results in an entry in your CloudTrail logs similar to the following example. When you see a log entry like this one, you can determine that CloudTrail (1) called the AWS KMS (2) `GenerateDataKey` API (3) for a specific trail (4). AWS KMS created the data key under a specific CMK (5).

**Note**

You might need to scroll to the right to see some of the callouts in the following example log entry.

```json
{
"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"
}
```
CloudTrail Puts a Log File into Your S3 Bucket

Each time CloudTrail puts a log file into your S3 bucket, Amazon S3 sends a `GenerateDataKey` request to AWS KMS on behalf of CloudTrail. In response to this request, AWS KMS generates a unique data key and then sends Amazon S3 two copies of the data key, one in plaintext and one that is encrypted with the specified CMK. Amazon S3 uses the plaintext data key to encrypt the CloudTrail log file and then removes the plaintext data key from memory as soon as possible after use. Amazon S3 stores the encrypted data key as metadata with the encrypted CloudTrail log file.

The `GenerateDataKey` request includes the following information for the encryption context (p. 175):

- The Amazon Resource Name (ARN) of the CloudTrail trail
- The ARN of the S3 object (the CloudTrail log file)

Each `GenerateDataKey` request results in an entry in your CloudTrail logs similar to the following example. When you see a log entry like this one, you can determine that CloudTrail called the AWS KMS `GenerateDataKey` API for a specific trail to protect a specific log file. AWS KMS created the data key under the specified CMK, shown twice in the same log entry.

**Note**
You might need to scroll to the right to see some of the callouts in the following example log entry.
You Get an Encrypted Log File from Your S3 Bucket

Each time you get an encrypted CloudTrail log file from your S3 bucket, Amazon S3 sends a Decrypt request to AWS KMS on your behalf to decrypt the log file's encrypted data key. In response to this request, AWS KMS uses your CMK to decrypt the data key and then sends the plaintext data key to Amazon S3. Amazon S3 uses the plaintext data key to decrypt the CloudTrail log file and then removes the plaintext data key from memory as soon as possible after use.

The Decrypt request includes the following information for the encryption context (p. 175):

- The Amazon Resource Name (ARN) of the CloudTrail trail
- The ARN of the S3 object (the CloudTrail log file)
Each Decrypt request results in an entry in your CloudTrail logs similar to the following example. When you see a log entry like this one, you can determine that an IAM user in your AWS account (1) called the AWS KMS (2) Decrypt API (3) for a specific trail (4) and a specific log file (5). AWS KMS decrypted the data key under a specific CMK (6).

**Note**
You might need to scroll to the right to see some of the callouts in the following example log entry.

```
{
    "eventVersion": "1.02",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/cloudtrail-admin",
        "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",
        "eventName": "Decrypt",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "internal.amazonaws.com",
        "userAgent": "internal.amazonaws.com",
        "requestParameters": {
            "encryptionContext": {
            }
        },
        "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",
            "accountId": "111122223333"
        }],
        "eventType": "AwsApiCall",
        "recipientAccountId": "111122223333"
    }
}
```

### Understanding How Often Your CMK is Used

To predict costs and better understand your AWS bill, you might want to know how often CloudTrail uses your CMK. AWS KMS charges for all API requests to the service that exceed the free tier. For the exact charges, see [AWS Key Management Service Pricing](https://aws.amazon.com/keymanagement/pricing/).
When you encrypt CloudTrail log files with AWS KMS–Managed Keys (SSE-KMS), each time CloudTrail puts a log file into your S3 bucket (p. 100) it results in an AWS KMS API request. Typically, CloudTrail puts a log file into your S3 bucket once every five minutes, which results in approximately 288 AWS KMS API requests per day, per region, and per AWS account. For example:

- If you enable this feature in two regions in a single AWS account, you can expect approximately 576 AWS KMS API requests per day (2 x 288).
- If you enable this feature in two regions in each of three AWS accounts, you can expect approximately 1,728 AWS KMS API requests per day (6 x 288).

These numbers represent only the AWS KMS API requests that occur when CloudTrail puts a log file into your S3 bucket. Each time you get an encrypted log file from your S3 bucket (p. 101) it results in an additional AWS KMS API request.

How Amazon Elastic Block Store (Amazon EBS) Uses AWS KMS

This topic discusses in detail how Amazon Elastic Block Store (Amazon EBS) uses AWS KMS to encrypt volumes and snapshots. For basic instructions about encrypting Amazon EBS volumes, see Amazon EBS Encryption.

Topics

- Amazon EBS Encryption (p. 103)
- Amazon EBS Encryption Context (p. 104)
- Detecting Amazon EBS Failures (p. 104)
- Using AWS CloudFormation to Create Encrypted Amazon EBS Volumes (p. 105)

Amazon EBS Encryption

When you attach an encrypted Amazon EBS volume to a supported Amazon Elastic Compute Cloud (Amazon EC2) instance type, data stored at rest on the volume, disk I/O, and snapshots created from the volume are all encrypted. The encryption occurs on the servers that host Amazon EC2 instances.

This feature is supported on all Amazon EBS volume types. You access encrypted volumes the same way you access other volumes; encryption and decryption are handled transparently and they require no additional action from you, your EC2 instance, or your application. Snapshots of encrypted volumes are automatically encrypted, and volumes that are created from encrypted snapshots are also automatically encrypted.

The encryption status of an EBS volume is determined when you create the volume. You cannot change the encryption status of an existing volume. However, you can migrate data between encrypted and unencrypted volumes and apply a new encryption status while copying a snapshot.

To create an encrypted Amazon EBS volume, select the appropriate box in the Amazon EBS section of the Amazon EC2 console. You can use a custom customer master key (CMK) (p. 2) by choosing one from the list that appears below the encryption box. If you do not specify a custom CMK, Amazon EBS uses the AWS-managed CMK for Amazon EBS in your account. If there is no AWS-managed CMK for Amazon EBS in your account, Amazon EBS creates one.

The following explains how Amazon EBS uses your CMK:
1. When you create an encrypted EBS volume, Amazon EBS sends a `GenerateDataKeyWithoutPlaintext` request to AWS KMS, specifying the CMK that you chose for EBS volume encryption.

2. AWS KMS generates a new data key, encrypts it under the specified CMK, and then sends the encrypted data key to Amazon EBS to store with the volume metadata.

3. When you attach the encrypted volume to an EC2 instance, Amazon EC2 sends the encrypted data key to AWS KMS with a `Decrypt` request.

4. AWS KMS decrypts the encrypted data key and then sends the decrypted (plaintext) data key to Amazon EC2.

5. Amazon EC2 uses the plaintext data key in hypervisor memory to encrypt disk I/O to the EBS volume. The data key persists in memory as long as the EBS volume is attached to the EC2 instance.

### Amazon EBS Encryption Context

Amazon EBS sends encryption context (p. 175) when making AWS KMS API requests to generate data keys and decrypt. Amazon EBS uses the volume ID as encryption context for all volumes and for encrypted snapshots created with the `CreateSnapshot` operation in the Amazon EC2 API. In the `requestParameters` field of a CloudTrail log entry, the encryption context looks similar to the following:

```json
"encryptionContext": {
    "aws:ebs:id": "vol-0cfb133e847d28be9"
}
```

Amazon EBS uses the snapshot ID as encryption context for encrypted snapshots created with the `CopySnapshot` operation in the Amazon EC2 API. In the `requestParameters` field of a CloudTrail log entry, the encryption context looks similar to the following:

```json
"encryptionContext": {
    "aws:ebs:id": "snap-069a655b568de654f"
}
```

### Detecting Amazon EBS Failures

To create an encrypted EBS volume or attach the volume to an EC2 instance, Amazon EBS and the Amazon EC2 infrastructure must be able to use the CMK that you specified for EBS volume encryption. When the CMK is not usable—for example, when it is not in the enabled key state (p. 93)—the volume creation or volume attachment fails. In this case, Amazon EBS sends an event to Amazon CloudWatch Events to notify you about the failure. With CloudWatch Events, you can establish rules that trigger automatic actions in response to these events. For more information, see Amazon CloudWatch Events for Amazon EBS in the Amazon EC2 User Guide for Linux Instances, especially the following sections:

- Invalid Encryption Key on Volume Attach or Reattach
- Invalid Encryption Key on Create Volume

To fix these failures, ensure that the CMK that you specified for EBS volume encryption is enabled. To do this, first view the CMK (p. 7) to determine its current key state (the `Status` column in the AWS Management Console). Then, see the information at one of the following links:

- If the CMK's key state is disabled, enable it (p. 18).
- If the CMK's key state is pending import, import key material (p. 69).
- If the CMK's key state is pending deletion, cancel key deletion (p. 82).
Using AWS CloudFormation to Create Encrypted Amazon EBS Volumes

You can use AWS CloudFormation to create encrypted Amazon EBS volumes. For more information, see AWS::EC2::Volume in the AWS CloudFormation User Guide.

How Amazon Elastic Transcoder Uses AWS KMS

You can use Amazon Elastic Transcoder to convert media files stored in an Amazon S3 bucket into formats required by consumer playback devices. Both input and output files can be encrypted and decrypted. The following sections discuss how AWS KMS is used for both processes.

Topics
- Encrypting the input file (p. 105)
- Decrypting the input file (p. 106)
- Encrypting the output file (p. 106)
- HLS Content Protection (p. 108)
- Elastic Transcoder Encryption Context (p. 108)

Encrypting the input file

Before you can use Elastic Transcoder, you must create an Amazon S3 bucket and upload your media file into it. You can encrypt the file before uploading by using AES client-side encryption or after uploading by using Amazon S3 server-side encryption.

If you choose client-side encryption using AES, you are responsible for encrypting the file before uploading it to Amazon S3, and you must provide Elastic Transcoder access to the encryption key. You do this by using an AWS KMS customer master key (CMK) to protect the AES encryption key you used to encrypt the media file.

If you choose server-side encryption, you are allowing Amazon S3 to perform all encryption and decryption of files on your behalf. You can configure Amazon S3 to use one of three different master keys to protect the unique data key used to encrypt your file:

- The Amazon S3 master key, a key that is owned and managed by AWS
- The AWS-managed CMK for Amazon S3, a master key that is owned by your account but managed by AWS
- Any customer-managed CMK that you create by using AWS KMS

You can request encryption and the master key you want by using the Amazon S3 console or the appropriate Amazon S3 APIs. For more information about how Amazon S3 performs encryption, see Protecting Data Using Encryption in the Amazon Simple Storage Service Developer Guide.

When you use an AWS KMS CMK as the master key (the AWS-managed CMK for Amazon S3 in your account or a customer-managed CMK) to protect the input file, Amazon S3 and AWS KMS interact in the following manner:

1. Amazon S3 requests a plaintext data key and a copy of the data key encrypted under the specified CMK.
2. AWS KMS creates a data key, encrypts it with the specified CMK, and then sends both the plaintext data key and the encrypted data key to Amazon S3.
3. Amazon S3 uses the plaintext data key to encrypt the media file and then stores the file in the specified Amazon S3 bucket.
4. Amazon S3 stores the encrypted data key alongside of the encrypted media file.

## Decrypting the input file

If you choose Amazon S3 server-side encryption to encrypt the input file, Elastic Transcoder does not decrypt the file. Instead, Elastic Transcoder relies on Amazon S3 to perform decryption depending on the settings you specify when you create a job and a pipeline.

The following combination of settings are available.

<table>
<thead>
<tr>
<th>Encryption mode</th>
<th>AWS KMS key</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>S3</td>
<td>Default</td>
<td>Amazon S3 creates and manages the keys used to encrypt and decrypt the media file. The process is opaque to the user.</td>
</tr>
<tr>
<td>S3-AWS-KMS</td>
<td>Default</td>
<td>Amazon S3 uses a data key encrypted by the default AWS-managed CMK for Amazon S3 in your account to encrypt the media file.</td>
</tr>
<tr>
<td>S3-AWS-KMS</td>
<td>Custom (with ARN)</td>
<td>Amazon S3 uses a data key encrypted by the specified customer-managed CMK to encrypt the media file.</td>
</tr>
</tbody>
</table>

When **S3-AWS-KMS** is specified, Amazon S3 and AWS KMS work together in the following manner to perform the decryption.

1. Amazon S3 sends the encrypted data key to AWS KMS.
2. AWS KMS decrypts the data key by using the appropriate CMK, and then sends the plaintext data key back to Amazon S3.
3. Amazon S3 uses the plaintext data key to decrypt the ciphertext.

If you choose client-side encryption using an AES key, Elastic Transcoder retrieves the encrypted file from the Amazon S3 bucket and decrypts it. Elastic Transcoder uses the CMK you specified when you created the pipeline to decrypt the AES key and then uses the AES key to decrypt the media file.

## Encrypting the output file

Elastic Transcoder encrypts the output file depending on how you specify the encryption settings when you create a job and a pipeline. The following options are available.

<table>
<thead>
<tr>
<th>Encryption mode</th>
<th>AWS KMS key</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>S3</td>
<td>Default</td>
<td>Amazon S3 creates and manages the keys used to encrypt the output file.</td>
</tr>
</tbody>
</table>
### Encrypting the output file

<table>
<thead>
<tr>
<th>Encryption mode</th>
<th>AWS KMS key</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>S3-AWS-KMS</td>
<td>Default</td>
<td>Amazon S3 uses a data key created by AWS KMS and encrypted by the AWS-managed CMK for Amazon S3 in your account.</td>
</tr>
<tr>
<td>S3-AWS-KMS</td>
<td>Custom (with ARN)</td>
<td>Amazon S3 uses a data key encrypted by using the customer-managed CMK specified by the ARN to encrypt the media file.</td>
</tr>
<tr>
<td>AES-</td>
<td>Default</td>
<td>Elastic Transcoder uses the AWS-managed CMK for Amazon S3 in your account to decrypt the specified AES key you provide and uses that key to encrypt the output file.</td>
</tr>
<tr>
<td>AES-</td>
<td>Custom (with ARN)</td>
<td>Elastic Transcoder uses the customer-managed CMK specified by the ARN to decrypt the specified AES key you provide and uses that key to encrypt the output file.</td>
</tr>
</tbody>
</table>

When you specify that an AWS KMS CMK (the AWS-managed CMK for Amazon S3 in your account or a customer-managed CMK) be used to encrypt the output file, Amazon S3 and AWS KMS interact in the following manner:

1. Amazon S3 requests a plaintext data key and a copy of the data key encrypted by using the specified CMK.
2. AWS KMS creates a data key, encrypts it under the CMK, and sends both the plaintext data key and the encrypted data key to Amazon S3.
3. Amazon S3 encrypts the media using the data key and stores it in the specified Amazon S3 bucket.
4. Amazon S3 stores the encrypted data key alongside the encrypted media file.

When you specify that your provided AES key be used to encrypt the output file, the AES key must be encrypted using a CMK in AWS KMS. Elastic Transcoder, AWS KMS, and you interact in the following manner:

1. You encrypt your AES key by calling the `Encrypt` operation in the AWS KMS API. AWS KMS encrypts the key by using the specified CMK. You specify which CMK to use when you are creating the pipeline.
2. You specify the file containing the encrypted AES key when you create the Elastic Transcoder job.
3. Elastic Transcoder decrypts the key by calling the `Decrypt` operation in the AWS KMS API, passing the encrypted key as ciphertext.
4. Elastic Transcoder uses the decrypted AES key to encrypt the output media file and then deletes the decrypted AES key from memory. Only the encrypted copy you originally defined in the job is saved to disk.
5. You can download the encrypted output file and decrypt it locally by using the original AES key that you defined.
**Important**

Your private encryption keys are never stored by AWS. Therefore, it is important that you safely and securely manage your keys. If you lose them, you won't be able to decrypt your data.

## HLS Content Protection

HTTP Live Streaming (HLS) is an adaptive streaming protocol. Elastic Transcoder supports HLS by breaking your input file into smaller individual files called media segments. A set of corresponding individual media segments contain the same material encoded at different bit rates, thereby enabling the player to select the stream that best fits the available bandwidth. Elastic Transcoder also creates playlists that contain metadata for the various segments that are available to be streamed.

You can use AES-128 encryption to protect the transcoded media segments. When you enable HLS content protection, each media segment is encrypted using an AES-128 encryption key. When the content is viewed, the player downloads the key and decrypts the media segments during the playback process.

Two types of keys are used: an AWS KMS CMK and a data key. You must create a CMK to use to encrypt and decrypt the data key. Elastic Transcoder uses the data key to encrypt and decrypt media segments. The data key must be AES-128. All variations and segments of the same content are encrypted using the same data key. You can provide a data key or have Elastic Transcoder create it for you.

The CMK can be used to encrypt the data key at the following points:

- If you provide your own data key, you must encrypt it before passing it to Elastic Transcoder.
- If you request that Elastic Transcoder generate the data key, then Elastic Transcoder encrypts the data key for you.

The CMK can be used to decrypt the data key at the following points:

- Elastic Transcoder decrypts your provided data key when it needs to use the data key to encrypt the output file or decrypt the input file.
- You decrypt a data key generated by Elastic Transcoder and use it to decrypt output files.

For more information, see [HLS Content Protection](#) in the *Amazon Elastic Transcoder Developer Guide*.

## Elastic Transcoder Encryption Context

Elastic Transcoder sends encryption context (p. 175) when making AWS KMS API requests to generate data keys, encrypt, and decrypt. The encryption context is written to CloudTrail logs to help you understand why a given AWS KMS CMK was used. Elastic Transcoder uses the service name as encryption context. In the `requestParameters` field of a CloudTrail log file, the encryption context looks similar to the following:

```
"encryptionContext": { 
  "service": "elastictranscoder.amazonaws.com"
}
```

For more information about how to configure Elastic Transcoder jobs to use one of the supported encryption options, see [Data Encryption Options](#) in the *Amazon Elastic Transcoder Developer Guide*. 
How Amazon EMR Uses AWS KMS

When you use an Amazon EMR cluster, you can configure the cluster to encrypt data at rest, which means the cluster encrypts data before saving it to a persistent storage location. You can encrypt data at rest on the EMR File System (EMRFS), on the storage volumes of cluster nodes, or both. To encrypt data at rest, you can use a customer master key (CMK) in AWS KMS. The following topics explain how an Amazon EMR cluster uses a CMK to encrypt data at rest.

Amazon EMR clusters also encrypt data in transit, which means the cluster encrypts data before sending it through the network. You cannot use a CMK to encrypt data in transit. For more information, see In-Transit Data Encryption in the Amazon EMR Release Guide.

For more information about all the encryption options available in Amazon EMR, see Understanding Encryption Options with Amazon EMR in the Amazon EMR Release Guide.

Topics
- Encrypting Data on the EMR File System (EMRFS) (p. 109)
- Encrypting Data on the Storage Volumes of Cluster Nodes (p. 111)
- Encryption Context (p. 111)

Encrypting Data on the EMR File System (EMRFS)

Amazon EMR clusters use two distributed file systems:

- The Hadoop Distributed File System (HDFS). HDFS encryption does not use a CMK in AWS KMS.

- The EMR File System (EMRFS). EMRFS is an implementation of HDFS that allows Amazon EMR clusters to store data in Amazon Simple Storage Service (Amazon S3). EMRFS supports four encryption options, two of which use a CMK in AWS KMS. For more information about all four of the EMRFS encryption options, see At-Rest Encryption for Amazon S3 with EMRFS in the Amazon EMR Release Guide.

The two EMRFS encryption options that use a CMK use the following encryption features offered by Amazon S3:

- **Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS).** With SSE-KMS, the Amazon EMR cluster sends data to Amazon S3, and then Amazon S3 uses a CMK to encrypt the data before saving it to an S3 bucket. For more information about how this works, see Process for Encrypting Data on EMRFS with SSE-KMS (p. 110).

- **Client-Side Encryption with AWS KMS-Managed Keys (CSE-KMS).** With CSE-KMS, the Amazon EMR cluster uses a CMK to encrypt data before sending it to Amazon S3 for storage. For more information about how this works, see Process for Encrypting Data on EMRFS with CSE-KMS (p. 110).

When you configure an Amazon EMR cluster to encrypt data on EMRFS with SSE-KMS or CSE-KMS, you choose the CMK in AWS KMS that you want Amazon S3 or the Amazon EMR cluster to use. With SSE-KMS, you can choose the AWS-managed CMK for Amazon S3 with the alias aws/s3, or a custom CMK that you create. With CSE-KMS, you must choose a custom CMK that you create. When you choose a custom CMK, you must ensure that your Amazon EMR cluster has permission to use the CMK. For more information, see Add the EMR Instance Role to an AWS KMS CMK in the Amazon EMR Release Guide.
For both SSE-KMS and CSE-KMS, the CMK you choose is the master key in an **envelope encryption** (p. 96) workflow. This means the data is encrypted with a unique data encryption key (or **data key**), and this data key is encrypted under the CMK in AWS KMS. The encrypted data and an encrypted copy of its data key are stored together as a single encrypted object in an S3 bucket. For more information about how this works, see the following topics.

**Topics**
- Process for Encrypting Data on EMRFS with SSE-KMS (p. 110)
- Process for Encrypting Data on EMRFS with CSE-KMS (p. 110)

### Process for Encrypting Data on EMRFS with SSE-KMS

When you configure an Amazon EMR cluster to use SSE-KMS, the encryption process works like this:

1. The cluster sends data to Amazon S3 for storage in an S3 bucket.
2. Amazon S3 sends a **GenerateDataKey** request to AWS KMS, specifying the key ID of the CMK that you chose when you configured the cluster to use SSE-KMS. The request includes encryption context; for more information, see **Encryption Context** (p. 111).
3. AWS KMS generates a unique data encryption key (data key) and then sends two copies of this data key to Amazon S3. One copy is unencrypted (plaintext), and the other copy is encrypted under the CMK.
4. Amazon S3 uses the plaintext data key to encrypt the data that it received in step 1, and then removes the plaintext data key from memory as soon as possible after use.
5. Amazon S3 stores the encrypted data and the encrypted copy of the data key together as a single encrypted object in an S3 bucket.

The decryption process works like this:

1. The cluster requests an encrypted data object from an S3 bucket.
2. Amazon S3 extracts the encrypted data key from the S3 object, and then sends the encrypted data key to AWS KMS with a **Decrypt** request. The request includes encryption context; for more information, see **Encryption Context** (p. 111).
3. AWS KMS decrypts the encrypted data key using the same CMK that was used to encrypt it, and then sends the decrypted (plaintext) data key to Amazon S3.
4. Amazon S3 uses the plaintext data key to decrypt the encrypted data, and then removes the plaintext data key from memory as soon as possible after use.
5. Amazon S3 sends the decrypted data to the cluster.

### Process for Encrypting Data on EMRFS with CSE-KMS

When you configure an Amazon EMR cluster to use CSE-KMS, the encryption process works like this:

1. When it’s ready to store data in Amazon S3, the cluster sends a **GenerateDataKey** request to AWS KMS, specifying the key ID of the CMK that you chose when you configured the cluster to use CSE-KMS. The request includes encryption context; for more information, see **Encryption Context** (p. 111).
2. AWS KMS generates a unique data encryption key (data key) and then sends two copies of this data key to the cluster. One copy is unencrypted (plaintext), and the other copy is encrypted under the CMK.
3. The cluster uses the plaintext data key to encrypt the data, and then removes the plaintext data key from memory as soon as possible after use.
4. The cluster combines the encrypted data and the encrypted copy of the data key together into a single encrypted object.
5. The cluster sends the encrypted object to Amazon S3 for storage.

The decryption process works like this:

1. The cluster requests the encrypted data object from an S3 bucket.
2. Amazon S3 sends the encrypted object to the cluster.
3. The cluster extracts the encrypted data key from the encrypted object, and then sends the encrypted data key to AWS KMS with a Decrypt request. The request includes encryption context; for more information, see Encryption Context (p. 111).
4. AWS KMS decrypts the encrypted data key using the same CMK that was used to encrypt it, and then sends the decrypted (plaintext) data key to the cluster.
5. The cluster uses the plaintext data key to decrypt the encrypted data, and then removes the plaintext data key from memory as soon as possible after use.

Encrypting Data on the Storage Volumes of Cluster Nodes

An Amazon EMR cluster is a collection of Amazon Elastic Compute Cloud (Amazon EC2) instances. Each instance in the cluster is called a cluster node or node. Each node can have two types of storage volumes: instance store volumes, and Amazon Elastic Block Store (Amazon EBS) volumes. You can configure the cluster to use Linux Unified Key Setup (LUKS) to encrypt both types of storage volumes on the nodes (but not the boot volume of each node). This is called local disk encryption.

When you enable local disk encryption for a cluster, you can choose to encrypt the LUKS master key with a CMK in AWS KMS. You must choose a custom CMK that you create; you cannot use an AWS-managed CMK. When you choose a custom CMK, you must ensure that your Amazon EMR cluster has permission to use the CMK. For more information, see Add the EMR Instance Role to an AWS KMS CMK in the Amazon EMR Release Guide.

When you enable local disk encryption using a CMK, the encryption process works like this:

1. When each cluster node launches, it sends a GenerateDataKey request to AWS KMS, specifying the key ID of the CMK that you chose when you enabled local disk encryption for the cluster.
2. AWS KMS generates a unique data encryption key (data key) and then sends two copies of this data key to the node. One copy is unencrypted (plaintext), and the other copy is encrypted under the CMK.
3. The node uses a base64-encoded version of the plaintext data key as the password that protects the LUKS master key. The node saves the encrypted copy of the data key on its boot volume.
4. If the node reboots, the rebooted node sends the encrypted data key to AWS KMS with a Decrypt request.
5. AWS KMS decrypts the encrypted data key using the same CMK that was used to encrypt it, and then sends the decrypted (plaintext) data key to the node.
6. The node uses the base64-encoded version of the plaintext data key as the password to unlock the LUKS master key.

Encryption Context

Each AWS service that is integrated with AWS KMS can specify encryption context when it uses AWS KMS to generate data keys or to encrypt or decrypt data. Encryption context is additional authenticated
information that AWS KMS uses to check for data integrity. When a service specifies encryption context for an encryption operation, it must specify the same encryption context for the corresponding decryption operation or decryption will fail. Encryption context is also written to AWS CloudTrail log files, which can help you understand why a given CMK was used. For more information about encryption context, see Encryption Context (p. 175).

The following section explain the encryption context that is used in each Amazon EMR encryption scenario that uses a CMK.

Encryption Context for EMRFS Encryption with SSE-KMS

With SSE-KMS, the Amazon EMR cluster sends data to Amazon S3, and then Amazon S3 uses a CMK to encrypt the data before saving it to an S3 bucket. In this case, Amazon S3 uses the Amazon Resource Name (ARN) of the S3 object as encryption context with each GenerateDataKey and Decrypt request that it sends to AWS KMS. The following example shows a JSON representation of the encryption context that Amazon S3 uses.

```
{ "aws:s3:arn" : "arn:aws:s3:::S3_bucket_name/S3_object_key" }
```

Encryption Context for EMRFS Encryption with CSE-KMS

With CSE-KMS, the Amazon EMR cluster uses a CMK to encrypt data before sending it to Amazon S3 for storage. In this case, the cluster uses the Amazon Resource Name (ARN) of the CMK as encryption context with each GenerateDataKey and Decrypt request that it sends to AWS KMS. The following example shows a JSON representation of the encryption context that the cluster uses.

```
{ "kms_cmk_id" : "arn:aws:kms:us-east-2:111122223333:key/0987ab65-43cd-21ef-09ab-87654321cdef" }
```

Encryption Context for Local Disk Encryption with LUKS

When an Amazon EMR cluster uses local disk encryption with LUKS, the cluster nodes do not specify encryption context with the GenerateDataKey and Decrypt requests that they send to AWS KMS.

How Amazon Redshift Uses AWS KMS

This topic discusses how Amazon Redshift uses AWS KMS to encrypt data.

Topics
- Amazon Redshift Encryption (p. 112)
- Encryption Context (p. 113)

Amazon Redshift Encryption

An Amazon Redshift data warehouse is a collection of computing resources called nodes, which are organized into a group called a cluster. Each cluster runs an Amazon Redshift engine and contains one or more databases.

Amazon Redshift uses a four-tier, key-based architecture for encryption. The architecture consists of data encryption keys, a database key, a cluster key, and a master key.
Data encryption keys encrypt data blocks in the cluster. Each data block is assigned a randomly-generated AES-256 key. These keys are encrypted by using the database key for the cluster.

The database key encrypts data encryption keys in the cluster. The database key is a randomly-generated AES-256 key. It is stored on disk in a separate network from the Amazon Redshift cluster and passed to the cluster across a secure channel.

The cluster key encrypts the database key for the Amazon Redshift cluster. You can use AWS KMS, AWS CloudHSM, or an external hardware security module (HSM) to manage the cluster key. See the <a href="#" class="external-link">Amazon Redshift Database Encryption</a> documentation for more details.

If the master key resides in AWS KMS, it encrypts the cluster key. You can request encryption by checking the appropriate box in the Amazon Redshift console. You can specify a customer-managed master key to use by choosing one from the list that appears below the encryption box. If you do not specify a customer-managed key, the AWS-managed key for Amazon Redshift under your account will be used.

**Encryption Context**

Each service that is integrated with AWS KMS specifies an encryption context when requesting data keys, encrypting, and decrypting. The encryption context is additional authenticated information that AWS KMS uses to check for data integrity. That is, when an encryption context is specified for an encryption operation, the service also specifies it for the decryption operation or decryption will not succeed. Amazon Redshift uses the cluster ID and the creation time for the encryption context. In the requestParameters field of a CloudTrail log file, the encryption context will look similar to this:

```
"encryptionContext": {
    "aws:redshift:createtime": "20150206T1832Z"
},
```

You can search on the cluster name in your CloudTrail logs to understand what operations were performed by using a customer master key. The operations include cluster encryption, cluster decryption, and generating data keys.

For more information, see <a href="#" class="external-link">Encryption Context (p. 175)</a>.

**How Amazon Relational Database Service (Amazon RDS) Uses AWS KMS**

You can use the <a href="#" class="external-link">Amazon Relational Database Service (Amazon RDS)</a> to set up, operate, and scale a relational database in the cloud. Optionally, you can choose to encrypt the data stored on your Amazon RDS <a href="#" class="external-link">DB instance</a> under a customer master key (CMK) in AWS KMS. To learn how to encrypt your Amazon RDS resources under a KMS CMK, see <a href="#" class="external-link">Encrypting Amazon RDS Resources</a> in the <a href="#" class="external-link">Amazon Relational Database Service User Guide</a>.

Amazon RDS builds on <a href="#" class="external-link">Amazon Elastic Block Store (Amazon EBS)</a> encryption to provide full disk encryption for database volumes. For more information about how Amazon EBS uses AWS KMS to encrypt volumes, see <a href="#" class="external-link">How Amazon Elastic Block Store (Amazon EBS) Uses AWS KMS (p. 103)</a>.

When you create an encrypted DB instance with Amazon RDS, Amazon RDS creates an encrypted EBS volume on your behalf to store the database. Data stored at rest on the volume, database snapshots, automated backups, and read replicas are all encrypted under the KMS CMK that you specified when you created the DB instance.
Amazon RDS Encryption Context

When Amazon RDS uses your KMS CMK, or when Amazon EBS uses it on behalf of Amazon RDS, the service specifies an encryption context (p. 175). The encryption context is additional authenticated information that AWS KMS uses to ensure data integrity. That is, when an encryption context is specified for an encryption operation, the service must specify the same encryption context for the decryption operation or decryption will not succeed. The encryption context is also written to your AWS CloudTrail logs to help you understand why a given CMK was used. Your CloudTrail logs might contain many entries describing the use of a CMK, but the encryption context in each log entry can help you determine the reason for that particular use.

At minimum, Amazon RDS always uses the DB instance ID for the encryption context, as in the following JSON-formatted example:

```
{ "aws:rds:db-id": "db-CQYSMDPBRZ7BPMH7Y3RTDG5QY" }
```

This encryption context can help you identify the DB instance for which your CMK was used.

When your CMK is used for a specific DB instance and a specific EBS volume, both the DB instance ID and the EBS volume ID are used for the encryption context, as in the following JSON-formatted example:

```
{
   "aws:rds:db-id": "db-BRG7VYS3SVIFQW7234EJQOM5RQ",
   "aws:ebs:id": "vol-ad8c6542"
}
```

How Amazon Simple Email Service (Amazon SES) Uses AWS KMS

You can use Amazon Simple Email Service (Amazon SES) to receive email, and (optionally) to encrypt the received email messages before storing them in an Amazon Simple Storage Service (Amazon S3) bucket that you choose. When you configure Amazon SES to encrypt email messages, you must choose the KMS customer master key (CMK) under which Amazon SES encrypts the messages. You can choose the default CMK in your account for Amazon SES with the alias `aws/ses`, or you can choose a custom CMK that you created separately in AWS KMS.

For more information about receiving email using Amazon SES, go to Receiving Email with Amazon SES in the Amazon Simple Email Service Developer Guide.

Topics

- Overview of Amazon SES Encryption Using AWS KMS (p. 114)
- Amazon SES Encryption Context (p. 115)
- Giving Amazon SES Permission to Use Your AWS KMS Customer Master Key (CMK) (p. 115)
- Retrieving and Decrypting Email Messages (p. 116)

Overview of Amazon SES Encryption Using AWS KMS

When you configure Amazon SES to receive email and encrypt the email messages before saving them to your S3 bucket, the process works like this:
1. You create a receipt rule for Amazon SES, specifying the S3 action, an S3 bucket for storage, and a KMS customer master key (CMK) for encryption.
2. Amazon SES receives an email message that matches your receipt rule.
3. Amazon SES requests a unique data key encrypted with the KMS CMK that you specified in the applicable receipt rule.
4. AWS KMS creates a new data key, encrypts it with the specified CMK, and then sends the encrypted and plaintext copies of the data key to Amazon SES.
5. Amazon SES uses the plaintext data key to encrypt the email message and then removes the plaintext data key from memory as soon as possible after use.
6. Amazon SES puts the encrypted email message and the encrypted data key in the specified S3 bucket. The encrypted data key is stored as metadata with the encrypted email message.

To accomplish Step 3 (p. 115) through Step 6 (p. 115), Amazon SES uses the AWS–provided Amazon S3 encryption client. Use the same client to retrieve your encrypted email messages from Amazon S3 and decrypt them. For more information, see Retrieving and Decrypting Email Messages (p. 116).

**Amazon SES Encryption Context**

When Amazon SES requests a data key to encrypt your received email messages (Step 3 (p. 115) in the Overview of Amazon SES Encryption Using AWS KMS (p. 114)), it includes encryption context in the request. The encryption context provides additional authenticated information that AWS KMS uses to ensure data integrity. The encryption context is also written to your AWS CloudTrail log files, which can help you understand why a given customer master key (CMK) was used. Amazon SES uses the following for the encryption context:

- The ID of the AWS account in which you’ve configured Amazon SES to receive email messages
- The rule name of the Amazon SES receipt rule that invoked the S3 action on the email message
- The Amazon SES message ID for the email message

The following example shows a JSON representation of the encryption context that Amazon SES uses:

```json
{
    "aws:ses:source-account": "111122223333",
    "aws:ses:rule-name": "example-receipt-rule-name",
    "aws:ses:message-id": "d6litobk75u44p8kdhnp7g2n800"
}
```

For more information about encryption context, go to Encryption Context (p. 175).

**Giving Amazon SES Permission to Use Your AWS KMS Customer Master Key (CMK)**

You can use the default customer master key (CMK) in your account for Amazon SES with the alias `aws/ses`, or you can use a custom CMK you create. If you use the default CMK for Amazon SES, you don’t need to perform any steps to give Amazon SES permission to use it. However, to specify a custom CMK when you add the S3 action to your Amazon SES receipt rule, you must ensure that Amazon SES has permission to use the CMK to encrypt your email messages. To give Amazon SES permission to use your custom CMK, add the following statement to your CMK’s key policy (p. 24):

```json
{
    "Effect": "Allow",
    "Action": "kms:*",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:user/AWSUser"
    },
    "Resource": "arn:aws:kms:us-east-1:111122223333:key/1234abcd-1234-1234-1234-1234abcd1234"
}
```
"Sid": "Allow SES to encrypt messages using this master 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": {
  }
}

Replace ACCOUNT-ID-WITHOUT-HYPHENS with the 12-digit ID of the AWS account in which you've configured Amazon SES to receive email messages. This policy statement allows Amazon SES to encrypt data with this CMK only under these conditions:


For more information about the encryption context that Amazon SES uses when encrypting your email messages, go to Amazon SES Encryption Context (p. 115). For general information about encryption context, go to Encryption Context (p. 175).

Retrieving and Decrypting Email Messages

Amazon SES does not have permission to decrypt your encrypted email messages and cannot decrypt them for you. You must write code to retrieve your email messages from Amazon S3 and decrypt them. To make this easier, use the Amazon S3 encryption client. The following AWS SDKs include the Amazon S3 encryption client:

- AWS SDK for Java – See AmazonS3EncryptionClient in the AWS SDK for Java API Reference.
- AWS SDK for Ruby – See Aws::S3::Encryption::Client in the AWS SDK for Ruby API Reference.
- AWS SDK for .NET – See AmazonS3EncryptionClient in the AWS SDK for .NET API Reference.
- AWS SDK for Go – See s3crypto in the AWS SDK for Go API Reference.

The Amazon S3 encryption client simplifies the work of constructing the necessary requests to Amazon S3 to retrieve the encrypted email message and to AWS KMS to decrypt the message's encrypted data key, and of decrypting the email message. For example, to successfully decrypt the encrypted data key you must pass the same encryption context that Amazon SES passed when requesting the data key from AWS KMS (Step 3 (p. 115) in the Overview of Amazon SES Encryption Using AWS KMS (p. 114)). The Amazon S3 encryption client handles this, and much of the other work, for you.

For sample code that uses the Amazon S3 encryption client in the AWS SDK for Java to do client-side decryption, see the following:

- Example: Client-Side Encryption (Option 1: Using an AWS KMS–Managed Customer Master Key (AWS SDK for Java)) in the Amazon Simple Storage Service Developer Guide.
How Amazon Simple Storage Service (Amazon S3) Uses AWS KMS

This topic discusses how to protect data at rest within Amazon S3 data centers by using AWS KMS. There are two ways to use AWS KMS with Amazon S3. You can use server-side encryption to protect your data with a customer master key or you can use a AWS KMS customer master key with the Amazon S3 encryption client to protect your data on the client side.

Topics

- Server-Side Encryption: Using SSE-KMS (p. 117)
- Using the Amazon S3 Encryption Client (p. 118)
- Encryption Context (p. 118)

Server-Side Encryption: Using SSE-KMS

You can protect data at rest in Amazon S3 by using three different modes of server-side encryption: SSE-S3, SSE-C, or SSE-KMS.

- SSE-S3 requires that Amazon S3 manage the data and master encryption keys. For more information about SSE-S3, see Protecting Data Using Server-Side Encryption with AWS-Managed Encryption Keys.
- SSE-C requires that you manage the encryption key. For more information about SSE-C, see Protecting Data Using Server-Side Encryption with Customer-Provided Encryption Keys (SSE-C).
- SSE-KMS requires that AWS manage the data key but you manage the master key in AWS KMS. The remainder of this topic discusses how to protect data by using server-side encryption with AWS KMS-managed keys (SSE-KMS).

You can request encryption and the master key you want by using the Amazon S3 console or API. In the console, check the appropriate box to perform encryption and select your key from the list. For the Amazon S3 API, specify encryption and choose your key by setting the appropriate headers in a GET or PUT request. For more information, see Protecting Data Using Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS).

You can choose a specific customer-managed master key or accept the AWS-managed key for Amazon S3 under your account. If you choose to encrypt your data, AWS KMS and Amazon S3 perform the following actions:

- Amazon S3 requests a plaintext data key and a copy of the key encrypted by using the specified customer-managed master key or the AWS-managed master key.
- AWS KMS creates a data key, encrypts it by using the master key, and sends both the plaintext data key and the encrypted data key to Amazon S3.
- Amazon S3 encrypts the data using the data key and removes the plaintext key from memory as soon as possible after use.
- Amazon S3 stores the encrypted data key as metadata with the encrypted data.

Amazon S3 and AWS KMS perform the following actions when you request that your data be decrypted.

- Amazon S3 sends the encrypted data key to AWS KMS.
AWS KMS decrypts the key by using the appropriate master key and sends the plaintext key back to Amazon S3.

Amazon S3 decrypts the ciphertext and removes the plaintext data key from memory as soon as possible.

Using the Amazon S3 Encryption Client

You can use the Amazon S3 encryption client in the AWS SDK from your own application to encrypt objects and upload them to Amazon S3. This method allows you to encrypt your data locally to ensure its security as it passes to the Amazon S3 service. The S3 service receives your encrypted data and does not play a role in encrypting or decrypting it.

The Amazon S3 encryption client encrypts the object by using envelope encryption. The client calls AWS KMS as a part of the encryption call you make when you pass your data to the client. AWS KMS verifies that you are authorized to use the customer master key and, if so, returns a new plaintext data key and the data key encrypted under the customer master key. The encryption client encrypts the data by using the plaintext key and then deletes the key from memory. The encrypted data key is sent to Amazon S3 to store alongside your encrypted data.

Encryption Context

Each service that is integrated with AWS KMS specifies an encryption context when requesting data keys, encrypting, and decrypting. The encryption context is additional authenticated information that AWS KMS uses to check for data integrity. That is, when an encryption context is specified for an encryption operation, the service also specifies it for the decryption operation or decryption will not succeed. If you are using SSE-KMS or the Amazon S3 encryption client to perform encryption, Amazon S3 uses the bucket path as the encryption context. In the requestParameters field of a CloudTrail log file, the encryption context will look similar to this.

```
"encryptionContext": {
    "aws:s3:arn": "arn:aws:s3:::bucket_name/file_name"
},
```

For more information, see Encryption Context (p. 175).

How AWS Systems Manager Parameter Store Uses AWS KMS

With AWS Systems Manager Parameter Store, you can create Secure String parameters, which are parameters that have a plaintext parameter name and an encrypted parameter value. Parameter Store uses AWS KMS to encrypt and decrypt the parameter values of Secure String parameters.

With Parameter Store you can create, store, and manage data as parameters with values. You can create a parameter in Parameter Store and use it in multiple applications and services subject to policies and permissions that you design. When you need to change a parameter value, you change one instance, rather than managing an error-prone change to numerous sources. Parameter Store supports a hierarchical structure for parameter names, so you can qualify a parameter for specific uses.

To manage sensitive data, you can create Secure String parameters. Parameter Store uses AWS KMS customer master keys (CMKs) to encrypt the parameter values of Secure String parameters when you create or change them. It also uses CMKs to decrypt the parameter values when you access them. You
Encrypting and Decrypting Secure String Parameters (p. 119)
Setting Permissions to Encrypt and Decrypt Parameter Values (p. 120)
Parameter Store Encryption Context (p. 121)
Troubleshooting CMK Issues in Parameter Store (p. 122)

Encrypting and Decrypting Secure String Parameters

Parameter Store does not perform any cryptographic operations. Instead, it relies on AWS KMS to encrypt and decrypt Secure String parameter values. When you create or change a Secure String parameter value, Parameter Store calls the AWS KMS Encrypt API operation. This operation uses an AWS KMS CMK directly to encrypt the parameter value instead of using the CMK to generate a data key (p. 2).

You can select the CMK that Parameter Store uses to encrypt the parameter value. If you do not specify a CMK, Parameter Store uses the default aws/ssm CMK that Systems Manager automatically creates in your account.

To view the default aws/ssm CMK for your account, use the DescribeKey operation in the AWS KMS API. The following example uses the describe-key command in the AWS Command Line Interface (AWS CLI) with the aws/ssm alias name.

```
aws kms describe-key --key-id alias/aws/ssm
```

To create a Secure String parameter, use the PutParameter operation in the Systems Manager API. Include a Type parameter with a value of SecureString. To specify an AWS KMS CMK, use the KeyId parameter. The default is the default aws/ssm CMK for your account.

Parameter Store then calls the AWS KMS Encrypt API with the CMK and the plaintext parameter value. AWS KMS returns the encrypted parameter value, which Parameter Store stores with the parameter name.

The following example uses the Systems Manager put-parameter command and its --type parameter in the AWS CLI to create a Secure String parameter. Because the command omits the optional --key-id parameter, Parameter Store uses the default aws/ssm CMK to encrypt the parameter value.

```
aws ssm put-parameter --name MyParameter --value "secret_value" --type SecureString
```

The following similar example uses the --key-id parameter to specify a customer managed CMK. The example uses a CMK ID to identify the CMK, but you can use any valid CMK identifier.

```
aws ssm put-parameter --name param1 --value "secret" --type SecureString --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

When you get a Secure String parameter from Parameter Store, its value is encrypted. To get a parameter, use the GetParameter operation in the Systems Manager API.

The following example uses the Systems Manager get-parameter command in the AWS CLI to get the MyParameter parameter from Parameter Store without decrypting its value.

```
$ aws ssm get-parameter --name MyParameter
```
To decrypt the parameter value before returning it, set the `WithDecryption` parameter of `GetParameter` to `true`. When you use `WithDecryption`, Parameter Store calls the AWS KMS `Decrypt` API operation on your behalf to decrypt the parameter value. As a result, the `GetParameter` request returns the parameter with a plaintext parameter value, as shown in the following example.

```
$ aws ssm get-parameter --name MyParameter --with-decryption

{
  "Parameter": {
    "Type": "SecureString",
    "Name": "MyParameter",
    "Value": "secret_value"
  }
}
```

The following workflow shows how Parameter Store uses an AWS KMS CMK.

**Encrypt in Put Parameter:**

1. When you create a Secure String parameter, Parameter Store sends an `Encrypt` request to AWS KMS that includes the plaintext parameter value and the CMK that you chose. During transmission to AWS KMS, the plaintext value in the Secure String parameter is protected by Transport Layer Security (TLS).
2. AWS KMS encrypts the parameter value with the specified CMK and returns the ciphertext to Parameter Store, which stores the parameter name and its encrypted value.

**Decrypt in Get Parameter**

1. When you include the `WithDecryption` parameter in a request to get a Secure String parameter, Parameter Store sends a `Decrypt` request to AWS KMS with the encrypted Secure String parameter value.
2. AWS KMS uses the same CMK to decrypt the encrypted value. It returns the plaintext (decrypted) parameter value to Parameter Store. During transmission, the plaintext data is protected by TLS.
3. Parameter Store returns the plaintext parameter value to you in the `GetParameter` response.

**Setting Permissions to Encrypt and Decrypt Parameter Values**

You can use IAM policies to allow or deny permission for a user to call the Systems Manager `PutParameter` and `GetParameter` operations.

Also, if you are using customer managed CMKs, you can use IAM policies and key policies to allow or deny permission to use the CMKs in calls to the AWS KMS `Encrypt` and `Decrypt` operations. However, you cannot establish access control policies for the default `aws/ssm` CMK. For detailed information about controlling access to customer managed AWS KMS CMKs, see [Authentication and Access Control for AWS KMS](p. 20).
The following example shows an IAM policy that allows the user to call the Systems Manager
GetParameter operation on all parameters in the /ReadableParameters path. The policy also allows
the user to call the AWS KMS Decrypt operation on the specified customer managed CMK.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": ["ssm:GetParameter*"],
      },
      {
         "Effect": "Allow",
         "Action": ["kms:Decrypt"],
         "Resource": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
      }
   ]
}
```

Parameter Store Encryption Context

An encryption context is a set of key–value pairs that contain arbitrary nonsecret data. When you include
an encryption context in a request to encrypt data, AWS KMS cryptographically binds the encryption
context to the encrypted data. To decrypt the data, you must pass in the same encryption context.

You can also use the encryption context to identify a cryptographic operation in audit records and logs.
The encryption context appears in plaintext in logs, such as AWS CloudTrail logs.

Parameter Store uses the following encryption context in its cryptographic operations:

- Key: PARAMETER_ARN
- Value: The Amazon Resource Name (ARN) of the parameter that is being encrypted.

The format of the encryption context is as follows:

```
"PARAMETER_ARN":"arn:aws:ssm:<REGION_NAME>:<ACCOUNT_ID>:parameter/<parameter-name>"
```

For example, Parameter Store includes this encryption context in calls to encrypt and decrypt the
MyParameter parameter.

```
```

If the parameter is in a Parameter Store hierarchical path, the path and name are included in the
encryption context. For example, this encryption context is used when encrypting and decrypting the
MyParameter parameter in the /ReadableParameters path:

```
```

You can decrypt an encrypted Secure String parameter value by calling the AWS KMS Decrypt operation
with the correct encryption context and the encrypted parameter value that the Systems Manager
GetParameter operation returns. However, we encourage you to use the GetParameter operation with the WithDecryption parameter to decrypt Parameter Store parameter values.

You can also include the encryption context in an IAM policy. For example, you can permit a user to decrypt only one particular parameter value or set of parameter values.

This example IAM policy allows the user to get the value of the MyParameter parameter and to decrypt its value using the specified CMK. However the permissions apply only when the encryption context matches specified string. These permissions do not apply to any other parameter or CMK, and the call to GetParameter fails if the encryption context does not match the string.

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "ssm:GetParameter"
         ],
      },
      {
         "Effect": "Allow",
         "Action": [
            "kms:Decrypt"
         ],
         "Condition": {
            "StringEquals": {
            }
         }
      }
   ]
}
```

Troubleshooting CMK Issues in Parameter Store

To perform any operation on a Secure String parameter, Parameter Store must be able to use the AWS KMS CMK that you specify for your intended operation. Most of the Parameter Store failures related to CMKs are caused by the following problems:

- The credentials that an application is using do not have permission to perform the specified action on the CMK.

  To fix this error, run the application with different credentials or revise the IAM or key policy that is preventing the operation. For help with AWS KMS IAM and key policies, see Authentication and Access Control for AWS KMS (p. 20).

- The CMK is not found.

  This typically happens when you use an incorrect identifier for the CMK. Find the correct identifiers (p. 10) for the CMK and try the command again.

- The CMK is not enabled. When this occurs, Parameter Store returns an InvalidKeyId exception with a detailed error message from AWS KMS.

  To find the status of a CMK, use the Status column (p. 7) of the Encryption keys page of the IAM console or the DescribeKey operation in the AWS KMS API. If the CMK state is disabled, enable...
it (p. 18). If it is pending import, you must complete the import procedure (p. 69). If the CMK is pending deletion, you must use a different CMK or cancel the key deletion (p. 82).

How Amazon WorkMail Uses AWS KMS

This topic discusses how Amazon WorkMail uses AWS KMS to encrypt email messages.

Topics
- Amazon WorkMail Overview (p. 123)
- Amazon WorkMail Encryption (p. 123)
- Amazon WorkMail Encryption Context (p. 125)

Amazon WorkMail Overview

Amazon WorkMail is an email service in the cloud that provides a cost-effective way for your organization to receive and send email and use calendars. Amazon WorkMail supports existing desktop and mobile clients and integrates with your existing corporate directory. Users can leverage their existing credentials to sign on to their email by using Microsoft Outlook, a mobile device, or a browser.

Using the Amazon WorkMail console, you can create an Amazon WorkMail organization and optionally assign to it one or more email domains that you own. Then you can create new email users and email distribution groups. Users can then send and receive messages. The messages are encrypted and stored until ready to be viewed.

Amazon WorkMail Encryption

Each end user you create is associated with one mailbox. Amazon WorkMail creates an asymmetric key pair for each mailbox and sends the private key portion of the key pair to AWS KMS to be encrypted under a customer master key (CMK). The CMK can be a custom key that you choose for your organization or the default Amazon WorkMail service CMK. The encrypted private key and unencrypted public key is then saved for later use.
Each message received is encrypted by using a symmetric key dynamically generated by Amazon WorkMail. The symmetric key is then encrypted by using the public key associated with the user’s mailbox. The encrypted symmetric key and the encrypted message and attachments are then stored.

In asymmetric cryptography, data that is encrypted by using the public key can be decrypted only by using the corresponding private key. As mentioned above, however, Amazon WorkMail encrypts the private key by using an AWS KMS CMK. To make the private key ready to use, it must therefore be decrypted by using the same CMK used to encrypt it. Thus, when a user is ready to retrieve email messages, Amazon WorkMail sends the private key to AWS KMS for decryption and uses the plaintext private key returned by AWS KMS to decrypt the symmetric key that was used to encrypt the email message. Amazon WorkMail then uses the symmetric key to decrypt the message before presenting it to the user.
Amazon WorkMail Encryption Context

Each service that is integrated with AWS KMS specifies an encryption context when requesting data keys, encrypting, and decrypting. The encryption context is additional authenticated information that AWS KMS uses to check for data integrity. That is, when an encryption context is specified for an encryption operation, the service also specifies it for the decryption operation or decryption will not succeed. The encryption context is written to your CloudTrail logs to help you understand why a given AWS KMS key was used. Amazon WorkMail uses the organization ID for the encryption context. In the requestParameters field of a CloudTrail log file, the encryption context will look similar to this.

```
"encryptionContext": {
}
```

The organization ID is a unique identifier that Amazon WorkMail generates when an organization is created. A customer can have multiple organizations in an AWS account. The following example shows the ARN of an organization in the us-east-2 region.

```
arn:aws:workmail:us-east-2:111122223333:organization/m-68755160c4cb4e29a2b2f8fb58f359d7
```

For more information about the encryption context, see Encryption Context (p. 175).

How Amazon WorkSpaces Uses AWS KMS

You can use Amazon WorkSpaces to provision a cloud-based desktop (a WorkSpace) for each of your end users. When you launch a new WorkSpace, you can choose to encrypt its volumes and decide which AWS KMS customer master key (CMK) to use for the encryption. You can choose your account’s default CMK for Amazon WorkSpaces (use the alias aws/workspaces), or you can choose a custom CMK that you created separately in AWS KMS.

For more information about creating WorkSpaces with encrypted volumes, go to Encrypt a WorkSpace in the Amazon WorkSpaces Administration Guide.

Topics
- Overview of Amazon WorkSpaces Encryption Using AWS KMS (p. 125)
- Amazon WorkSpaces Encryption Context (p. 126)
- Giving Amazon WorkSpaces Permission to Use A CMK On Your Behalf (p. 127)

Overview of Amazon WorkSpaces Encryption Using AWS KMS

When you create WorkSpaces with encrypted volumes, Amazon WorkSpaces uses Amazon Elastic Block Store (Amazon EBS) to create and manage those volumes. Both services use your KMS customer master key (CMK) to work with the encrypted volumes. For more information about EBS volume encryption, see the following documentation:

- How Amazon Elastic Block Store (Amazon EBS) Uses AWS KMS (p. 103) in this guide
- Amazon EBS Encryption in the Amazon EC2 User Guide for Windows Instances

When you launch WorkSpaces with encrypted volumes, the end-to-end process works like this:
1. You specify the CMK to use for encryption as well as the WorkSpace's user and directory. This action creates a grant (p. 57) that allows Amazon WorkSpaces to use your CMK only for this WorkSpace—that is, only for the WorkSpace associated with the specified user and directory.

2. Amazon WorkSpaces creates an encrypted EBS volume for the WorkSpace and specifies the CMK to use as well as the volume's user and directory (the same information that you specified at Step 1 (p. 126)). This action creates a grant (p. 57) that allows Amazon EBS to use your CMK only for this WorkSpace and volume—that is, only for the WorkSpace associated with the specified user and directory, and only for the specified volume.

3. Amazon EBS requests a volume data key that is encrypted under your CMK and specifies the WorkSpace user’s SID and directory ID as well as the volume ID as encryption context.

4. AWS KMS creates a new data key, encrypts it under your CMK, and then sends the encrypted data key to Amazon EBS.

5. Amazon WorkSpaces uses Amazon EBS to attach the encrypted volume to your WorkSpace, at which time Amazon EBS sends the encrypted data key to AWS KMS with a Decrypt request and specifies the WorkSpace user's SID and directory ID as well as the volume ID as encryption context.

6. AWS KMS uses your CMK to decrypt the data key, and then sends the plaintext data key to Amazon EBS.

7. Amazon EBS uses the plaintext data key to encrypt all data going to and from the encrypted volume. Amazon EBS keeps the plaintext data key in memory for as long as the volume is attached to the WorkSpace.

8. Amazon EBS stores the encrypted data key (received at Step 4 (p. 126)) with the volume metadata for future use in case you reboot or rebuild the WorkSpace.

9. When you use the AWS Management Console to remove a WorkSpace (or use the TerminateWorkspaces action in the Amazon WorkSpaces API), Amazon WorkSpaces and Amazon EBS retire the grants that allowed them to use your CMK for that WorkSpace.

Amazon WorkSpaces Encryption Context

Amazon WorkSpaces doesn't use your customer master key (CMK) directly for cryptographic operations (such as Encrypt, Decrypt, GenerateDataKey, etc.), which means Amazon WorkSpaces doesn't send requests to AWS KMS that include encryption context. However, when Amazon EBS requests an encrypted data key for the encrypted volumes of your WorkSpaces (Step 3 (p. 126) in the Overview of Amazon WorkSpaces Encryption Using AWS KMS (p. 125)) and when it requests a plaintext copy of that data key (Step 5 (p. 126)), it includes encryption context in the request. The encryption context provides additional authenticated information that AWS KMS uses to ensure data integrity. The encryption context is also written to your AWS CloudTrail log files, which can help you understand why a given customer master key (CMK) was used. Amazon EBS uses the following for the encryption context:

- The SID of the AWS Directory Service user that is associated with the WorkSpace
- The directory ID of the AWS Directory Service directory that is associated with the WorkSpace
- The volume ID of the encrypted volume

The following example shows a JSON representation of the encryption context that Amazon EBS uses:

```json
{
  "aws:workspaces:sid-directoryid": "[S-1-5-21-277731876-1789304096-451871588-1107]@[d-1234abcd01]",
  "aws:ebs:id": "vol-1234abcd"
}
```

For more information about encryption context, see Encryption Context (p. 175).
Giving Amazon WorkSpaces Permission to Use A CMK On Your Behalf

You can use your account’s default customer master key (CMK) for Amazon WorkSpaces with the alias `aws/workspaces`, or you can use a custom CMK that you create. If you use the default CMK for Amazon WorkSpaces, you don’t need to perform any steps to give Amazon WorkSpaces permission to use it. AWS KMS automatically specifies the necessary permissions in the key policy (p. 24) for the default CMK.

To use a custom CMK, the WorkSpaces administrators who create WorkSpaces with encrypted volumes must have permission to use the CMK. The WorkSpaces administrators don’t use the CMK directly. Simply creating a WorkSpace with encrypted volumes implicitly creates the grant (p. 57) that gives Amazon WorkSpaces permission to use the CMK on the administrator’s behalf.

Even though the WorkSpaces administrators don’t use the CMK directly, they need permission to use the CMK because they can only grant permissions that they have. To give WorkSpaces administrators permission to use a CMK, do these things:

1. Add the WorkSpaces administrators to the list of key users in the CMK’s key policy (p. 127)
2. Give the WorkSpaces administrators extra permissions with an IAM policy (p. 128)

WorkSpaces administrators also need permission to use Amazon WorkSpaces. For more information about these permissions, go to Controlling Access to Amazon WorkSpaces Resources in the Amazon WorkSpaces Administration Guide.

Part 1: Adding WorkSpaces Administrators to a CMK’s Key Users

To add WorkSpaces administrators to the list of key users in a CMK’s key policy, you can use the AWS Management Console or the AWS Command Line Interface (AWS CLI).

To add WorkSpaces administrators as key users for a CMK (console)

1. Sign in to the AWS Management Console and open the AWS Identity and Access Management (IAM) console at https://console.aws.amazon.com/iam/.
2. In the left navigation pane, choose Encryption keys.
3. For Region, choose the appropriate AWS Region. Do not use the region selector in the navigation bar (top right corner).
4. Choose the alias of the CMK that WorkSpaces administrators will use.
5. In the Key Policy section, under Key Users, choose Add.
6. In the list of IAM users and roles, select the users and roles that correspond to your WorkSpaces administrators, and then choose Attach.

To add WorkSpaces administrators as key users for a CMK (AWS CLI)

1. Use the `aws kms get-key-policy` command to retrieve the existing key policy, and then save the policy document to a file.
2. Open the policy document in your preferred text editor. Add the IAM users and roles that correspond to your WorkSpaces administrators to the policy statements that give permission to key users (p. 28). Then save the file.
3. Use the `aws kms put-key-policy` command to apply the key policy to the CMK.
Part 2: Giving WorkSpaces Administrators Extra Permissions with an IAM Policy

In addition to the permissions in the key users section of the default key policy (p. 25), WorkSpaces administrators need some permissions in an IAM user policy that applies to them. For information about creating and editing IAM user policies, go to Working with Managed Policies and Working with Inline Policies in the IAM User Guide.

At minimum, WorkSpaces administrators need permission to create grants (p. 57) for the custom CMK(s) that they will use with Amazon WorkSpaces. To use the AWS Management Console to create WorkSpaces with encrypted volumes, WorkSpaces administrators also need permission to list aliases and list keys, which are actions that the console performs on behalf of WorkSpaces administrators to display a list of available CMKs.

To give these permissions to your WorkSpaces administrators, add an IAM policy similar to the following example to your WorkSpaces administrators. Replace arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab in the first policy statement with the ARN(s) of the CMK(s) that WorkSpaces administrators will use when they create WorkSpaces with encrypted volumes. If your WorkSpaces administrators will launch WorkSpaces with only the Amazon WorkSpaces API (not with the console), you can omit the second statement with the "kms:ListAliases" and "kms:ListKeys" permissions.

```
{
    "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": "*
        }
    ]
}
```
Monitoring Customer Master Keys

Monitoring is an important part of understanding the availability, state, and usage of your customer master keys (CMKs) in AWS KMS and maintaining the reliability, availability, and performance of your AWS solutions. Collecting monitoring data from all the parts of your AWS solution will help you debug a multipoint failure if one occurs. Before you start monitoring your CMKs, however, create a monitoring plan that includes answers to the following questions:

- What are your monitoring goals?
- What resources will you monitor?
- How often will you monitor these resources?
- What monitoring tools (p. 129) will you use?
- Who will perform the monitoring tasks?
- Who should be notified when something happens?

The next step is to monitor your CMKs over time to establish a baseline for normal AWS KMS usage and expectations in your environment. As you monitor your CMKs, store historical monitoring data so that you can compare it with current data, identify normal patterns and anomalies, and devise methods to address issues.

For example, you can monitor AWS KMS API activity and events that affect your CMKs. When data falls above or below your established norms, you might need to investigate or take corrective action.

To establish a baseline for normal patterns, monitor the following items:

- AWS KMS API activity for data plane operations. These are cryptographic operations that use a CMK, such as Decrypt, Encrypt, ReEncrypt, and GenerateDataKey.
- AWS KMS API activity for control plane operations that are important to you. These operations manage a CMK, and you might want to monitor those that change a CMK's availability (such as ScheduleKeyDeletion, CancelKeyDeletion, DisableKey, EnableKey, ImportKeyMaterial, and DeleteImportedKeyMaterial) or modify a CMK's access control (such as PutKeyPolicy and RevokeGrant).
- Other AWS KMS metrics (such as the amount of time remaining until your imported key material (p. 69) expires) and events (such as the expiration of imported key material or the deletion or key rotation of a CMK).

Monitoring Tools

AWS provides various tools that you can use to monitor your CMKs. You can configure some of these tools to do the monitoring for you, while some of the tools require manual intervention. We recommend that you automate monitoring tasks as much as possible.

Automated Monitoring Tools

You can use the following automated monitoring tools to watch your CMKs and report when something has changed.

- **Amazon CloudWatch Alarms** – Watch a single metric over a time period that you specify, and perform one or more actions based on the value of the metric relative to a given threshold over a number of time periods. The action is a notification sent to an Amazon Simple Notification Service (Amazon SNS).
Monitoring with Amazon CloudWatch

You can monitor your customer master keys (CMKs) using Amazon CloudWatch, which collects and processes raw data from AWS KMS into readable, near real-time metrics. These data are recorded for a
period of two weeks so that you can access historical information and gain a better understanding of the usage of your CMKs and their changes over time. For more information about Amazon CloudWatch, see the Amazon CloudWatch User Guide.

Topics
- AWS KMS Metrics and Dimensions (p. 131)
- Creating CloudWatch Alarms to Monitor AWS KMS Metrics (p. 132)
- AWS KMS Events (p. 133)

AWS KMS Metrics and Dimensions

When you import key material into a CMK (p. 69) and set it to expire, AWS KMS sends metrics and dimensions to CloudWatch. You can view the AWS KMS metrics using the AWS Management Console and the Amazon CloudWatch API.

AWS KMS Metrics

The AWS/KMS namespace includes the following metrics.

SecondsUntilKeyMaterialExpiration

This metric tracks the number of seconds remaining until imported key material expires. This metric is valid only for CMKs whose origin is EXTERNAL and whose key material is or was set to expire. The most useful statistic for this metric is Minimum, which tells you the smallest amount of time remaining for all data points in the specified statistic period. The only valid unit for this metric is Seconds.

Use this metric to track the amount of time that remains until your imported key material expires. When that amount of time falls below a threshold that you define, you might want to take action such as reimporting the key material with a new expiration date. You can create a CloudWatch alarm to notify you when that happens. For more information, see Creating CloudWatch Alarms to Monitor AWS KMS Metrics (p. 132).

Dimensions for AWS KMS Metrics

AWS KMS metrics use the AWS/KMS namespace and have only one valid dimension: KeyId. You can use this dimension to view metric data for a specific CMK or set of CMKs.

How Do I View AWS KMS Metrics?

You can view the AWS KMS metrics using the AWS Management Console and the Amazon CloudWatch API.

To view metrics using the CloudWatch console

2. If necessary, change the region. From the navigation bar, select the region where your AWS resources reside.
3. In the navigation pane, choose Metrics.
4. In the content pane, choose the All metrics tab. Then, below AWS Namespaces, choose KMS.
5. Choose Per-Key Metrics to view the individual metrics and dimensions.
To view metrics using the Amazon CloudWatch API

To view AWS KMS metrics using the CloudWatch API, send a ListMetrics request with Namespace set to AWS/KMS. The following example shows how to do this with the AWS Command Line Interface (AWS CLI).

```
$ aws cloudwatch list-metrics --namespace AWS/KMS
```

Creating CloudWatch Alarms to Monitor AWS KMS Metrics

You can create a CloudWatch alarm that sends an Amazon SNS message when the value of the metric changes and causes the alarm to change state. An alarm watches a single metric over a time period you specify, and performs one or more actions based on the value of the metric relative to a given threshold over a number of time periods. The action is a notification sent to an Amazon SNS topic or Auto Scaling policy. Alarms invoke actions for sustained state changes only. CloudWatch alarms do not invoke actions simply because they are in a particular state; the state must have changed and been maintained for a specified number of periods.

Topics

- Create a CloudWatch Alarm to Monitor the Expiration of Imported Key Material (p. 132)
- Create a CloudWatch Alarm to Monitor Usage of CMKs that are Pending Deletion (p. 133)

Create a CloudWatch Alarm to Monitor the Expiration of Imported Key Material

When you import key material into a CMK (p. 69), you can optionally specify a time at which the key material expires. When the key material expires, AWS KMS deletes the key material and the CMK becomes unusable. To use the CMK again, you must reimport key material. You can create a CloudWatch alarm to notify you when the amount of time that remains until your imported key material expires falls below a threshold that you define (for example, 10 days). If you receive a notification from such an alarm, you might want to take action such as reimporting the key material with a new expiration date.

To create an alarm to monitor the expiration of imported key material (AWS Management Console)

2. If necessary, change the region. From the navigation bar, select the region where your AWS resources reside.
3. In the navigation pane, choose Alarms. Then choose Create Alarm.
4. Choose Browse Metrics and then choose KMS.
5. Select the check box next to the key ID of the CMK to monitor.
6. In the lower pane, use the menus to change the statistic to Minimum and the time period to 1 Minute. Then choose Next.
7. In the Create Alarm window, do the following:
   a. For Name, type a name such as KeyMaterialExpiresSoon.
   b. Following Whenever, for is, choose <= and then type the number of seconds for your threshold value. For example, to be notified when the time that remains until your imported key material expires is 10 days or less, type 864000.
   c. For for consecutive period(s), if necessary, type 1.
d. For **Send notification to**; do one of the following:

- To use a new Amazon SNS topic, choose **New list** and then type a new topic name. For **Email list**, type at least one email address. You can type more than one email address by separating them with commas.
- To use an existing Amazon SNS topic, choose the name of the topic to use.

e. Choose **Create Alarm**.

8. If you chose to send notifications to an email address, open the email message you receive from no-reply@sns.amazonaws.com with subject “AWS Notification - Subscription Confirmation.” Confirm your email address by choosing the **Confirm subscription** link in the email message.

**Important**

You will not receive email notifications until after you have confirmed your email address.

---

**Create a CloudWatch Alarm to Monitor Usage of CMKs that are Pending Deletion**

When you schedule key deletion (p. 81) for a CMK, AWS KMS enforces a waiting period before deleting the CMK. You can use the waiting period to ensure that you don't need the CMK now or in the future. You can also configure a CloudWatch alarm to warn you if a person or application attempts to use the CMK during the waiting period. If you receive a notification from such an alarm, you might want to cancel deletion of the CMK.

For more information, see **Creating an Amazon CloudWatch Alarm to Detect Usage of a Customer Master Key that is Pending Deletion** (p. 87).

---

**AWS KMS Events**

AWS KMS integrates with Amazon CloudWatch Events to notify you of certain events that affect your CMKs. Each event is represented in **JSON (JavaScript Object Notation)** and contains the event name, the
date and time when the event occurred, the CMK affected, and more. You can use CloudWatch Events to collect these events and set up rules that route them to one or more targets such as AWS Lambda functions, Amazon SNS topics, Amazon SQS queues, streams in Amazon Kinesis Data Streams, or built-in targets.

For more information about using CloudWatch Events with other kinds of events, including those emitted by AWS CloudTrail when it records a read/write API request, see the Amazon CloudWatch Events User Guide.

The following topics describe the CloudWatch Events that AWS KMS creates.

Topics
- KMS CMK Rotation (p. 134)
- KMS Imported Key Material Expiration (p. 134)
- KMS CMK Deletion (p. 135)

KMS CMK Rotation

When you enable annual rotation of a CMK's key material (p. 64), AWS KMS creates new key material for the CMK each year and sends a corresponding event to CloudWatch Events. The following is an example of this event.

```
{
    "version": "0",
    "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
    "detail-type": "KMS CMK Rotation",
    "source": "aws.kms",
    "account": "111122223333",
    "time": "2016-08-25T21:05:33Z",
    "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"
    }
}
```

KMS Imported Key Material Expiration

When you import key material into a CMK (p. 69), you can optionally specify a time at which the key material expires. When the key material expires, AWS KMS deletes the key material and sends a corresponding event to CloudWatch Events. The following is an example of this event.

```
{
    "version": "0",
    "id": "9da9af57-9253-4406-87cb-7cc400e43465",
    "detail-type": "KMS Imported Key Material Expiration",
    "source": "aws.kms",
    "account": "111122223333",
    "time": "2016-08-22T20:12:19Z",
    "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"
    }
}
```
KMS CMK Deletion

When you schedule key deletion (p. 81) for a CMK, AWS KMS enforces a waiting period before deleting the CMK. After the waiting period ends, AWS KMS deletes the CMK and sends a corresponding event to CloudWatch Events. The following is an example of this event.

```json
{
  "version": "0",
  "id": "e9ce3425-7d22-412a-a699-e7a5fc3fbc9a",
  "detail-type": "KMS CMK Deletion",
  "source": "aws.kms",
  "account": "111122223333",
  "time": "2016-08-19T03:23:45Z",
  "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"
  }
}
```
Logging AWS KMS API Calls Using AWS CloudTrail

AWS KMS is integrated with CloudTrail, a service that captures API calls made by or on behalf of AWS KMS in your AWS account and delivers the log files to an Amazon S3 bucket that you specify. CloudTrail captures API calls from the AWS KMS console or from the AWS KMS API. Using the information collected by CloudTrail, you can determine what request was made, the source IP address from which the request was made, who made the request, when it was made, and so on. To learn more about CloudTrail, including how to configure and enable it, see the AWS CloudTrail User Guide.

When you enable CloudTrail logging in your AWS account, API calls made to AWS KMS actions are tracked in log files. AWS KMS records are written together with other AWS service records in a log file. CloudTrail determines when to create and write to a new log file based on a time period and file size.

CloudTrail logs all of the AWS KMS actions. For example, calls to the CreateKey, Encrypt, and Decrypt actions generate entries in the CloudTrail log files.

Every log entry contains information about who generated the request. The user identity information in the log helps you determine whether the request was made with root or IAM user credentials, with temporary security credentials for a role or federated user, or by another AWS service. For more information, see CloudTrail userIdentity Element in the CloudTrail Event Reference chapter in the AWS CloudTrail User Guide.

You can store your log files in your bucket for as long as you want, but you can also define Amazon S3 lifecycle rules to archive or delete log files automatically. By default, your log files are encrypted by using Amazon S3 server-side encryption (SSE) with a key managed by the Amazon S3 service.

You can choose to have CloudTrail publish Amazon SNS notifications when new log files are delivered if you want to take quick action upon log file delivery. For more information, see Configuring Amazon SNS Notifications for CloudTrail in the AWS CloudTrail User Guide.

You can also aggregate AWS KMS log files from multiple AWS regions and multiple AWS accounts into a single Amazon S3 bucket. For more information, see Receiving CloudTrail Log Files from Multiple Regions in the AWS CloudTrail User Guide.

CloudTrail log files can contain one or more log entries where each entry is made up of multiple JSON-formatted events. A log entry represents a single request from any source and includes information about the requested action, any parameters, the date and time of the action, and so on. The log entries are not guaranteed to be in any particular order. That is, they are not an ordered stack trace of the public API calls. For more information about the fields that make up a log entry, see the CloudTrail Event Reference in the AWS CloudTrail User Guide.

For examples of what these CloudTrail log entries look like, see the following topics.

**Topics**
- CreateAlias (p. 137)
- CreateGrant (p. 138)
- CreateKey (p. 138)
- Decrypt (p. 139)
- DeleteAlias (p. 140)
- DescribeKey (p. 141)
- DisableKey (p. 142)
- EnableKey (p. 143)
CreateAlias

The following example shows a log file generated by calling CreateAlias.

```
{
   "Records": [ 
   {
      "eventVersion": "1.02",
      "userIdentity": { 
          "type": "IAMUser",
          "principalId": "EX_PRINCIPAL_ID",
          "arn": "arn:aws:iam::123456789012:user/Alice",
          "accountId": "123456789012",
          "accessKeyId": "EXAMPLE_KEY_ID",
          "userName": "Alice",
          "sessionContext": { 
              "attributes": { 
                  "mfaAuthenticated": "false",
                  "creationDate": "2014-11-04T00:52:27Z"
              },
              "attributes": { 
                  "mfaAuthenticated": "false",
                  "creationDate": "2014-11-04T00:52:27Z"
              }
          },
          "eventTime": "2014-11-04T00:52:27Z",
          "eventSource": "kms.amazonaws.com",
          "eventName": "CreateAlias",
          "awsRegion": "us-east-1",
          "sourceIPAddress": "192.0.2.0",
          "userAgent": "AWS Internal",
          "requestParameters": { 
              "aliasName": "alias/my_alias",
              "targetKeyId": "arn:aws:kms:us-east-1:123456789012:key/64e07f97-2489-4d04-bfdf-41723ad130bd",
          },
          "responseElements": null,
          "requestID": "d9472f40-63bc-11e4-bc2b-4198b6150d5c",
          "eventID": "e72d3993-864f-48d6-8f16-e26e1ae8dfff",
          "readOnly": false,
          "resources": [{ 
              "ARN": "arn:aws:kms:us-east-1:123456789012:key/64e07f97-2489-4d04-bfdf-41723ad130bd",
              "accountID": "123456789012"
          },
          { 
              "ARN": "arn:aws:kms:us-east-1:123456789012:alias/my_alias",
              "accountID": "123456789012"
          }],
          "eventType": "AwsApiCall",
   }
}
CreateGrant

The following example shows a log file generated by calling CreateGrant.

```json
{
  "Records": [
    {
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "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-east-1:123456789012:key/65f61d18-c45c-41ca-90c9-179982e9b716",
        "encryptionContextSubset": {
          "ContextKey1": "Value1"
        }
      },
      "operations": ["Encrypt", "RetireGrant"],
      "granteePrincipal": "EX_PRINCIPAL_ID"
    },
    {
      "responseElements": {
        "grantId": "f020fe7519b93991dc8491d6f19dd3cebb24ee62277a05914386724f3d48758"
      },
      "requestID": "f3c08808-63bc-11e4-bc2b-4198b6150d5c",
      "eventType": "AwsApiCall",
      "recipientAccountId": "123456789012"
    }
  ]
}
```

CreateKey

The following example shows a log file generated by calling CreateKey.
The following example shows a log file generated by calling Decrypt.

```json
{
    "Records": [
        {
            "eventVersion": "1.02",
            "userIdentity": {
                "type": "IAMUser",
                "principalId": "EX_PRINCIPAL_ID",
                "arn": "arn:aws:iam::123456789012:user/Alice",
                "accountId": "123456789012",
                "accessKeyId": "EXAMPLE_KEY_ID",
                "userName": "Alice"
            },
            "eventTime": "2014-11-04T00:52:59Z",
            "eventSource": "kms.amazonaws.com",
            "eventName": "CreateKey",
            "awsRegion": "us-east-1",
            "sourceIPAddress": "192.0.2.0",
            "userAgent": "AWS Internal",
            "requestParameters": {
                "policy": "{
                    "Version": "2012-10-17",
                    "Statement": [
                        {
                            "Effect": "Allow",
                            "Principal": {
                                "AWS": "arn:aws:iam::123456789012:user/Alice"
                            },
                            "Action": "kms:*",
                            "Resource": "*"
                        },
                        {
                            "Effect": "Allow",
                            "Principal": {
                                "AWS": "arn:aws:iam::012345678901:user/Bob"
                            },
                            "Action": "kms:CreateGrant",
                            "Resource": "*"
                        },
                        {
                            "Effect": "Allow",
                            "Principal": {
                                "AWS": "arn:aws:iam::012345678901:user/Charlie"
                            },
                            "Action": "kms:Encrypt",
                            "Resource": "*"
                        }
                    ]
                }
            }
        }
    ]
}
```
The following example shows a log file generated by calling `DeleteAlias`.

```json
{
  "Records": [
    {
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
      },
      "eventTime": "2014-11-04T00:52:20Z",
      "eventSource": "kms.amazonaws.com",
      "eventName": "DeleteAlias",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "AWS Internal",
      "errorCode": "InvalidCiphertextException",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "d5239dea-63bc-11e4-bc2b-419b6150d5c",
      "eventID": "954983cf-7da9-4adf-aeaa-261a1292c0aa",
      "readOnly": true,
      "resources": [{
        "ARN": "arn:aws:kms:us-east-1:123456789012:key/e17cebae-e7a6-4864-b92f-0365f2f2eff38",
        "accountId": "123456789012"
      }],
      "eventType": "AwsApiCall",
      "recipientAccountID": "123456789012"
    }
  ]
}
```
DescribeKey

The following example shows a log file generated by multiple calls to DescribeKey in response to viewing keys in the IAM management console.

```json
{
    "Records": [
        {
            "eventVersion": "1.02",
            "userIdentity": {
                "type": "IAMUser",
                "principalId": "EX_PRINCIPAL_ID",
                "arn": "arn:aws:iam::123456789012:user/Alice",
                "accountId": "123456789012",
                "accessKeyId": "EXAMPLE_KEY_ID",
                "userName": "Alice",
                "sessionContext": {
                    "attributes": {
                        "mfaAuthenticated": "false",
                        "creationDate": "2014-11-05T20:51:21Z"
                    }
                }
            },
            "invokedBy": "signin.amazonaws.com",
            "eventTime": "2014-11-05T20:51:34Z",
            "eventSource": "kms.amazonaws.com",
            "eventName": "DescribeKey",
            "awsRegion": "us-east-1",
            "sourceIPAddress": "192.0.2.0",
            "userAgent": "signin.amazonaws.com",
            "requestParameters": {
                "keyId": "30a9a1e7-2a84-459d-9c61-04cbeaebab95"
            },
            "responseElements": null,
            "requestID": "874d4823-652d-11e4-0af2addecb",
            "eventType": "AwsApiCall",
            "recipientAccountId": "123456789012"
        }
    ]
}
```
The following example shows a log file generated by calling `DisableKey`.

```json
{
  "Records": [
    {
      "eventVersion": "1.02",
      "userIdentity": { "type": "IAMUser",
                        "principalId": "EX_PRINCIPAL_ID",
                        "arn": "arn:aws:iam::123456789012:user/Alice",
                        "accountId": "123456789012",
                        "accessKeyId": "EXAMPLE_KEY_ID",
                        "userName": "Alice",
                        "sessionContext": { "attributes": { "mfaAuthenticated": "false",
                                                           "creationDate": "2014-11-05T20:51:21Z" } },
                        "invokedBy": "signin.amazonaws.com"
      },
      "eventTime": "2014-11-05T20:51:55Z",
      "eventSource": "kms.amazonaws.com",
      "eventName": "DescribeKey",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "signin.amazonaws.com",
      "requestParameters": { "keyId": "e7b6d35a-b551-4c8f-b51a-0460ebc04565" },
      "responseElements": null,
      "requestId": "9400c720-652d-11e4-9a87-01af2a1ddec8",
      "eventID": "939fcefb-dc14-4a52-b918-73045fe97af3",
      "readOnly": true,
      "resources": [
        { "ARN": "arn:aws:kms:us-east-1:123456789012:key/e7b6d35a-b551-4c8f-b51a-0460ebc04565",
          "accountId": "123456789012"
        }
      ],
      "eventType": "AwsApiCall",
      "recipientAccountId": "123456789012"
    }
  ]
}
```
EnableKey

The following example shows a log file generated by calling EnableKey.

```
{
  "Records": [
    {
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "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": "e17cebae-e7a6-4864-b92f-0365f2feff38"
      },
      "responseElements": null,
      "requestID": "e17cebae-e7a6-4864-b92f-0365f2feff38",
      "eventID": "be39928-3629-4370-9634-567f9274d52e",
      "readOnly": false,
      "resources": [{
        "ARN": "arn:aws:kms:us-east-1:123456789012:key/e17cebae-e7a6-4864-b92f-0365f2feff38",
        "accountId": "123456789012"
      }]
    }
  ]
}```
The following example shows a log file generated by calling Encrypt.

```json
{
   "Records": [
      {
         "eventVersion": "1.02",
         "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice"
         },
         "eventTime": "2014-11-04T00:53:11Z",
         "eventSource": "kms.amazonaws.com",
         "eventName": "Encrypt",
         "awsRegion": "us-east-1",
         "sourceIPAddress": "192.0.2.0",
         "userAgent": "AWS Internal",
         "requestParameters": {
            "encryptionContext": {
               "ContextKey1": "Value1"
            },
            "keyId": "arn:aws:kms:us-east-1:012345678901:key/8d3acf57-6bba-480a-9459-ed1b8e79d3d0"
         },
         "responseElements": null,
         "requestID": "f3423043-63bc-11e4-bc2b-4198b6150d5c",
         "readOnly": true,
         "resources": [
            {
               "ARN": "arn:aws:kms:us-east-1:012345678901:key/8d3acf57-6bba-480a-9459-ed1b8e79d3d0",
               "accountId": "012345678901"
            }
         ],
         "eventType": "AwsServiceEvent",
         "recipientAccountId": "012345678901"
      }
   ]
}
```

```

The following example shows a log file created by calling GenerateDataKey.

```json
{
   "Records": [
      {
         "eventVersion": "1.02",
         "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice"
         },
         "eventTime": "2014-11-04T00:53:11Z",
         "eventSource": "kms.amazonaws.com",
         "eventName": "GenerateDataKey",
         "awsRegion": "us-east-1",
         "sourceIPAddress": "192.0.2.0",
         "userAgent": "AWS Internal",
         "requestParameters": {
            "encryptionContext": {
               "ContextKey1": "Value1"
            },
            "keyId": "arn:aws:kms:us-east-1:012345678901:key/8d3acf57-6bba-480a-9459-ed1b8e79d3d0"
         },
         "responseElements": null,
         "requestID": "f3423043-63bc-11e4-bc2b-4198b6150d5c",
         "readOnly": true,
         "resources": [
            {
               "ARN": "arn:aws:kms:us-east-1:012345678901:key/8d3acf57-6bba-480a-9459-ed1b8e79d3d0",
               "accountId": "012345678901"
            }
         ],
         "eventType": "AwsServiceEvent",
         "recipientAccountId": "012345678901"
      }
   ]
}
```
GenerateDataKeyWithoutPlaintext

The following example shows a log file created by calling GenerateDataKeyWithoutPlaintext.

```json
{
  "Records": [
    {
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "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": "d4f2a88d-5f9c-4807-b71d-4d0ee5225156",
        "numberOfBytes": 16
      },
      "responseElements": null,
      "requestID": "d6b8e411-63bc-11e4-bc2b-4198b6150d5c",
      "eventID": "d6f7734272-9ec5-4c80-9f36-528ebbe35e4a",
      "readOnly": true,
      "resources": [null],
      "eventType": "AwsApiCall",
      "recipientAccountId": "123456789012"
    }
  ]
}
```
The following example shows a log file created by calling GenerateRandom.

```json
{
  "Records": [
    {
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "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": "123456789012"
    }
  ]
}
```

### GetKeyPolicy

The following example shows a log file generated by calling GetKeyPolicy.

```json
{
  "Records": [
    {
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::123456789012:user/Alice",
```
ListAliases

The following example shows a log file generated by calling ListAliases.

```json
{
  "Records": [
    {
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "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": "eyJiIjoiYWxpYXMvZTU0Y2MxOTMtYTMwNC00YzEwLTliZWItYTJjZjA3NjJzd0ttLTE0OTg0LWZtNiI6IiIsImNsaWFzL2U1NGNjMTJkLWEzMTliMDUtMzQzLTI1YjYtZDQ0Mzg5YmNlYjU3IiwiYSI6IjY1MyIsImluaXRjaWQiOiIyNjQ1MDMyMDAtMDcyMC00OTI1LTMxYmUtODc0MDc2MzA5ZjctMzY2IiwiYW5kIjoiMzgwZjk2MzZmMy0xOWY1LTQzMDctYzU4Yy00NzI3NjQ1ZjUxOTQiLCJzY29kZSI6IjI0MjQwY2Y5MC01MTQyLTQ2Y2ItYzJlYS03ZjUxMjQ2MjA4MjY5Iiwic2VjcmV0aW9uIjoiOTI1NjQ1MzI2N2YtMDYwOS00Y2Q1LTkwYzAtYTEzNzIzNzU4ZDZhLTIwZGQ1ZjYwMTQyOCJ9",
        "requestID": "bfe6c190-63bc-11e4-bc2b-4198b6150d5c",
        "eventID": "a27dda7b-76f1-4ac3-8b40-42dfba77bdc6",
        "readOnly": true,
        "resources": []
      }
    }
  ]
}
```
ListGrants

The following example shows a log file generated by calling ListGrants.

```json
{
   "Records": [
      {
         "eventVersion": "1.02",
         "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "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": "arn:aws:kms:us-east-1:123456789012:key/ea22a751-e707-40d0-92ac-13a28fa9eb11",
            "marker": "eyJncmFudElkIjoiMWY4M2U2MzY2MDgxYjQ2Yzc4MTdhM2Y4YmQwMDM0YzNiY2NlY2RmOWFiNWMyYWY1Nzc1NDNjYmNlMjMlNHkiLCJuYW1lIjoiYXNzZXRzIiwiY29tIjoieSIsInVzZXJzIjoidmFsdWViX2ZvcmQifQ",
            "limit": 10
         },
         "responseElements": null,
         "requestID": "e5c23960-63bc-11e4-bc2b-4198b6150d5c",
         "eventID": "2d4380f5-1b20-4253-8e92-dd0492b3bd3d",
         "readOnly": true,
         "resources": [{
            "accountId": "123456789012"
         }],
         "eventType": "AwsApiCall",
         "recipientAccountId": "123456789012"
      }
   ]
}
```

ReEncrypt

The following example shows a log file generated by calling ReEncrypt.

```json
{
   "Records": [
      {
         "eventVersion": "1.02",
         "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice"
         },
         "eventTime": "2014-11-04T00:52:49Z",
         "eventSource": "kms.amazonaws.com",
         "eventName": "ReEncrypt",
         "awsRegion": "us-east-1",
         "sourceIPAddress": "192.0.2.0",
         "userAgent": "AWS Internal",
         "requestParameters": {
            "keyId": "arn:aws:kms:us-east-1:123456789012:key/ea22a751-e707-40d0-92ac-13a28fa9eb11",
            "marker": "eyJncmFudElkIjoiMWY4M2U2MzY2MDgxYjQ2Yzc4MTdhM2Y4YmQwMDM0YzNiY2NlY2RmOWFiNWMyYWY1Nzc1NDNjYmNlMjMlNHkiLCJuYW1lIjoiYXNzZXRzIiwiY29tIjoieSIsInVzZXJzIjoidmFsdWViX2ZvcmQifQ",
            "limit": 10
         },
         "responseElements": null,
         "requestID": "e5c23960-63bc-11e4-bc2b-4198b6150d5c",
         "eventID": "2d4380f5-1b20-4253-8e92-dd0492b3bd3d",
         "readOnly": true,
         "resources": [{
            "accountId": "123456789012"
         }],
         "eventType": "AwsApiCall",
         "recipientAccountId": "123456789012"
      }
   ]
}
```
Amazon EC2 Example One

The following example demonstrates an IAM user creating an encrypted volume using the default volume key in the Amazon EC2 management console.

The following example shows a CloudTrail log entry that demonstrates the user Alice creating an encrypted volume using a default volume key in AWS EC2 Management Console. The EC2 log file record includes a `volumeId` field with a value of "vol-13439757". The AWS KMS record contains an `encryptionContext` field with a value of "aws:ebs:id": "vol-13439757". Similarly, the `principalId` and `accountId` between the two records match. The records reflect the fact that creating an encrypted volume generates a data key that is used to encrypt the volume content.
"userName": "Alice",
"sessionContext": {
  "attributes": {
    "mfaAuthenticated": "false",
    "creationDate": "2014-11-05T20:40:44Z"
  }
},
"invokedBy": "signin.amazonaws.com"
},
"eventTime": "2014-11-05T20:50:18Z",
"eventSource": "ec2.amazonaws.com",
"eventName": "CreateVolume",
"awsRegion": "us-east-1",
"sourceIPAddress": "72.72.72.72",
"userAgent": "signin.amazonaws.com",
"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::123456789012:user/Alice",
    "accountId": "123456789012",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2014-11-05T20:40:44Z"
      }
    },
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2014-11-05T20:50:19Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "GenerateDataKeyWithoutPlaintext",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "requestParameters": {
    "encryptionContext": {
      "aws:ebs:id": "vol-13439757"
    },
    "numberOfBytes": 64,
    "keyId": "alias/aws/ebs"
  },
}
Amazon EC2 Example Two

The following example shows an IAM user running an Amazon EC2 instance that mounts a data volume encrypted by using a default volume key. The action taken by the user generates multiple AWS KMS log records. Creating the encrypted volume generates a data key, and the Amazon EC2 service generates a grant, on behalf of the customer, that enables it to decrypt the data key. The `instanceId`, "i-81e2f56c", is referred to in the `granteePrincipal` field of the `CreateGrant` record as "123456789012:aws:ec2-infrastructure:i-81e2f56c" as well as in the identity of the principal calling Decrypt, "arn:aws:sts::123456789012:assumed-role/aws:ec2-infrastructure/i-81e2f56c". The key identified by the UUID "e29ddfd4-1bf6-4e1b-8ecb-08216bd70d07" is common across all three KMS calls.

```json
{
  "Records": [
    {
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2014-11-05T21:34:36Z"
          }
        },
        "invokedBy": "signin.amazonaws.com"
      },
      "eventTime": "2014-11-05T21:35:27Z",
      "eventSource": "ec2.amazonaws.com",
      "eventName": "RunInstances",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "72.72.72.72",
      "userAgent": "signin.amazonaws.com",
      "requestParameters": {
        "instancesSet": {
          "items": [
            {
              "imageId": "ami-b66ed3de",
              "minCount": 1,
              "maxCount": 1
            }
          ]
        }
      }
    }
  ]
}
```
AWS Key Management Service Developer Guide
Amazon EC2 Example Two

{  
  "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": "123456789012",  
  "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-b847-9c3d330e6aae",  
"eventType": "AwsApiCall",  
"recipientAccountId": "123456789012"  
}
"encryptionContextSubset": {
  "aws:ebs:id": "vol-f67bafbb2"
}
},
"granteePrincipal": "123456789012:aws:ec2-infrastructure:i-81e2f56c",
"KeyId": "arn:aws:kms:us-east-1:123456789012:key/e29ddf4d4-1bf6-4e1b-8ecb-08216bd70d07"
},
"responseElements": {
  "grantId": "6caf442b4ff8a27511fbde1e12cc5342f5312112247f75c191db2721ec356fe"
},
"requestID": "41c4b4f7-8bce-4773-bf0e-5ae3bb5cbce2",
"eventID": "c1ad79e3-0d3f-402a-b119-d5c3d7c6a6c",
"readOnly": false,
"resources": [
  {
    "ARN": "arn:aws:kms:us-east-1:123456789012:key/e29ddf4d4-1bf6-4e1b-8ecb-08216bd70d07",
    "accountId": "123456789012"
  }
],
"eventType": "AwsApiCall",
"recipientAccountId": "123456789012"
},
{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::123456789012:user/Alice",
    "accountId": "123456789012",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2014-11-05T13:34:36Z"
      }
    }
  },
  "invokedBy": "AWS Internal"
},
"eventTime": "2014-11-05T13:35:32Z",
"eventSource": "kms.amazonaws.com",
"eventName": "GenerateDataKeyWithoutPlaintext",
"awsRegion": "us-east-1",
"sourceIpAddress": "AWS Internal",
"userAgent": "AWS Internal",
"requestParameters": {
  "encryptionContext": {
    "aws:ebs:id": "vol-f67bafbb2"
  },
  "numberOfBytes": 64,
  "KeyId": "alias/aws/ebs"
},
"responseElements": null,
"requestID": "create-123456789012-758247346-1415223332",
"eventID": "ac3cab10-ce93-4953-9d62-0b6e5c9a651d",
"readOnly": true,
"resources": [
  {
    "ARN": "arn:aws:kms:us-east-1:123456789012:key/e29ddf4d4-1bf6-4e1b-8ecb-08216bd70d07",
    "accountId": "123456789012"
  }
],
"eventType": "AwsApiCall"
"recipientAccountId": "123456789012"
},
"eventVersion": "1.02",
"userIdentity": {
"type": "AssumedRole",
"principalId": "123456789012:aws:ec2-infrastructure:i-81e2f56c",
"arn": "arn:aws:sts::123456789012:assumed-role/aws:ec2-infrastructure/i-81e2f56c",
"accountId": "123456789012",
"accessKeyId": "",
"sessionContext": {
"attributes": {
"mfaAuthenticated": "false",
"creationDate": "2014-11-05T21:35:38Z"
},
"sessionIssuer": {
"type": "Role",
"principalId": "123456789012:aws:ec2-infrastructure",
"arn": "arn:aws:iam::123456789012:role/aws:ec2-infrastructure",
"accountId": "123456789012",
"userName": "aws:ec2-infrastructure"
}
},
"eventTime": "2014-11-05T21:35:47Z",
"eventSource": "kms.amazonaws.com",
"eventName": "Decrypt",
"awsRegion": "us-east-1",
"sourceIPAddress": "172.172.172.172",
"requestParameters": {
"encryptionContext": {
"aws:ebs:id": "vol-f67baf2b"
}
},
"responseElements": null,
"requestID": "b4b27883-6533-11e4-b4d9-751f1761e9e5",
"eventID": "ed65380-0a3e-4123-bbc8-3d1b7cfe49b0",
"readOnly": true,
"resources": [
{
"ARN": "arn:aws:kms:us-east-1:123456789012:key/e29ddf4d4-1bf6-4e1b-8ec8-08216bd70d07",
"accountId": "123456789012"
}
],
"eventType": "AwsApiCall",
"recipientAccountId": "123456789012"}
Connecting to AWS KMS Through a VPC Endpoint

You can connect directly to AWS KMS through a private endpoint in your VPC instead of connecting over the internet. When you use a VPC endpoint, communication between your VPC and AWS KMS is conducted entirely within the AWS network.

AWS KMS supports Amazon Virtual Private Cloud (Amazon VPC) interface endpoints that are powered by AWS PrivateLink. Each VPC endpoint is represented by one or more Elastic Network Interfaces (ENIs) with private IP addresses in your VPC subnets.

The VPC interface endpoint connects your VPC directly to AWS KMS without an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. The instances in your VPC do not need public IP addresses to communicate with AWS KMS.

You can specify the VPC endpoint in AWS KMS API operations and AWS CLI commands. For example, the following command uses the `endpoint-url` parameter to specify a VPC endpoint in an AWS CLI command to AWS KMS.

```bash
$ aws kms list-keys --endpoint-url https://vpce-0295a3caf8414c94a-dfm9tr04.kms.us-east-1.vpce.amazonaws.com
```

If you enable private DNS hostnames for your VPC endpoint, you do not even need to specify the endpoint URL. The standard AWS KMS DNS hostname that the AWS KMS CLI and SDKs use by default (`https://kms.<region>.amazonaws.com`) resolves to your VPC endpoint.

You can also use AWS CloudTrail logs to audit your use of KMS keys through the VPC endpoint. And you can use the conditions in IAM and key policies to deny access to any request that does not come from a specified VPC or VPC endpoint.

**Note**
Use caution when creating IAM and key policies based on your VPC endpoint. If a policy statement requires that requests come from a particular VPC or VPC endpoint, requests from integrated AWS services that use the CMK on your behalf might fail. For help, see Using VPC Endpoint Conditions in Policies with AWS KMS Permissions (p. 48).

**Regions**
AWS KMS supports VPC endpoints in all AWS regions where both Amazon VPC and AWS KMS are available, except for AWS GovCloud (US) and EU (Paris).

**Topics**
- Create an AWS KMS VPC Endpoint (p. 156)
- Connecting to an AWS KMS VPC Endpoint (p. 159)
- Using a VPC Endpoint in a Policy Statement (p. 160)
- Audit the CMK Use for your VPC (p. 162)

Create an AWS KMS VPC Endpoint

You create an interface endpoint in your VPC by using the KMS VPC endpoint service in each region. You can create a VPC endpoint in the AWS Management Console, or by using the AWS CLI or Amazon EC2 API.
Creating an AWS KMS VPC Endpoint (Console)

1. Sign in to the AWS Management Console and open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation bar, use the region selector to choose your region.
3. In the navigation pane, choose Endpoints. In the main pane, Create Endpoint.
4. For Service category, choose AWS services.
5. In the Service Name list, choose the entry for AWS KMS interface endpoint in the region. For example, in the US East (N.Virginia) Region, the entry name is com.amazonaws.us-east-1.kms.
6. For VPC, select a VPC. The endpoint is created in the VPC that you select.
7. For Subnets, choose a subnet from each Availability Zone that you want to include.

   The VPC endpoint can span multiple Availability Zones. An elastic network interface (ENI) for the VPC endpoint is created in each subnet that you choose. Each ENI has a DNS hostname and a private IP address.

8. In this step, you can enable a private DNS hostname for your VPC endpoint. If you select the Enable Private DNS Name option, the standard AWS KMS DNS hostname (https://kms.<region>.amazonaws.com) resolves to your VPC endpoint.

   This option makes it easier to use the VPC endpoint. The AWS KMS CLI and SDKs use the standard AWS KMS DNS hostname by default, so you do not need to specify the VPC endpoint URL in applications and commands.

   This feature works only when the enableDnsHostnames and enableDnsSupport attributes of your VPC are set to true. To set these attributes, use the ModifyVpcAttribute API.

   To enable a private DNS hostname, for Enable Private DNS Name, select Enable for this endpoint.

9. For Security group, select or create a security group.

   You can use security groups to control access to your endpoint, much like you would use a firewall.

10. Choose Create endpoint.

    The results show the VPC endpoint, including the VPC endpoint ID and the DNS names that you use to connect to your VPC endpoint (p. 159).

    You can also use the Amazon VPC tools to view and manage your endpoint, including creating a notification for an endpoint, changing properties of the endpoint, and deleting the endpoint. For instructions, see Interface VPC Endpoints.
Creating an AWS KMS VPC Endpoint (AWS CLI)

You can use the create-vpc-endpoint command in the AWS CLI to create a VPC endpoint that connects to AWS KMS.

Be sure to use interface as the VPC endpoint type and a service name value that includes kms and the region where your VPC is located.

The command does not include the PrivateDnsNames parameter because its default value is true. To disable this option, you can include the parameter with a value of false. Private DNS names are available only when the enableDnsHostnames and enableDnsSupport attributes of your VPC are set to true. To set these attributes, use the ModifyVpcAttribute API.

The following diagram shows the syntax of the command.

```
aws ec2 create-vpc-endpoint --vpc-id <vpc id> \
  --vpc-endpoint-type Interface \
  --service-name com.amazonaws.<region>.kms \
  --subnet-ids <subnet id> \
  --security-group-id <security group id>
```

For example, this command creates a VPC endpoint in the VPC with VPC ID vpc-1a2b3c4d, which is in the us-east-1 region. It specifies just one subnet ID to represent the Availability Zones, but you can specify many. The security group ID is also required.
Connecting to an AWS KMS VPC Endpoint

You can connect to AWS KMS through the VPC endpoint by using the AWS CLI or an AWS SDK. To specify the VPC endpoint, use its DNS name.

For example, this `list-keys` command uses the `endpoint-url` parameter to specify the VPC endpoint. To use a command like this, replace the example VPC endpoint ID with one in your account.
If you enabled private hostnames when you created your VPC endpoint, you do not need to specify the VPC endpoint URL in your CLI commands or application configuration. The standard AWS KMS DNS hostname (https://kms.<region>.amazonaws.com) resolves to your VPC endpoint. The AWS CLI and SDKs use this hostname by default, so you can begin using the VPC endpoint without changing anything in your scripts and application.

To use private hostnames, the `enableDnsHostnames` and `enableDnsSupport` attributes of your VPC must be set to true. To set these attributes, use the `ModifyVpcAttribute` API.

### Using a VPC Endpoint in a Policy Statement

You can use IAM policies and AWS KMS key policies to control access to your AWS KMS customer master keys (CMKs). You can also use global condition keys to restrict these policies based on VPC endpoint or VPC in the request.

- Use the `aws:sourceVpce` condition key to grant or restrict access to an AWS KMS CMK based on the VPC endpoint.
- Use the `aws:sourceVpc` condition key to grant or restrict access to an AWS KMS CMK based on the VPC that hosts the private endpoint.

**Note**

Use caution when creating IAM and key policies based on your VPC endpoint. If a policy statement requires that requests come from a particular VPC or VPC endpoint, requests from integrated AWS services that use the CMK on your behalf might fail. For help, see Using VPC Endpoint Conditions in Policies with AWS KMS Permissions (p. 48).

Also, the `aws:sourceIP` condition key is not effective when the request comes from an Amazon VPC endpoint. To restrict requests to a VPC endpoint, use the `aws:sourceVpce` or `aws:sourceVpc` condition keys. For more information, see VPC Endpoints - Controlling the Use of Endpoints in the **Amazon VPC User Guide**.

For example, the following sample key policy allows a user to perform encryption operations with a CMK only when the request comes through the specified VPC endpoint.

When a user makes a request to AWS KMS, the VPC endpoint ID in the request is compared to the `aws:sourceVpce` condition key value in the policy. If they do not match, then the request is denied.

To use a policy like this one, replace the placeholder AWS account ID and VPC endpoint IDs with valid values for your account.

```json
{
   "Id": "example-key-1",
   "Version": "2012-10-17",
   "Statement": [
   {
      "Sid": "Enable IAM user permissions",
      "Effect": "Allow",
      "Principal": {"AWS": ["111122223333"]},
      "Action": ["kms:*"],
      "Resource": "*
   },
   {
      "Sid": "Restrict usage to my VPC endpoint",
      "Effect": "Deny",
   }
]```
You can also use the `aws:sourceVpc` condition key to restrict access to your CMKs based on the VPC in which VPC endpoint resides.

The following sample key policy allows commands that manage the CMK only when they come from `vpc-12345678`. In addition, it allows commands that use the CMK for cryptographic operations only when they come from `vpc-2b2b2b2b`. You might use a policy like this one if an application is running in one VPC, but you use a second, isolated VPC for management functions.

To use a policy like this one, replace the placeholder AWS account ID and VPC endpoint IDs with valid values for your account.

```json
{
   "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"
            }
         }
      }
   ]
}
```
Audit the CMK Use for your VPC

When a request to AWS KMS uses a VPC endpoint, the VPC endpoint ID appears in the AWS CloudTrail log (p. 136) entry that records the request. You can use the endpoint ID to audit the use of your AWS KMS VPC endpoint.

For example, this sample log entry records a GenerateDataKey request that used the VPC endpoint. The vpcEndpointId field appears at the end of the log entry.

```
{
  "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-0295a3caf8414c94a"
}
```
Programming the AWS KMS API

You can use the AWS KMS API to perform the following actions, and more.

- Create, describe, list, enable, and disable keys.
- Create, delete, list, and update aliases.
- Encrypt, decrypt, and re-encrypt content.
- Set, list, and retrieve key policies.
- Create, retire, revoke, and list grants.
- Retrieve key rotation status.
- Update key descriptions.
- Generate data keys with or without plaintext.
- Generate random data.

For example code in Java that uses the AWS SDK for Java to call the AWS KMS API, see the following topics.

**Topics**

- Creating a Client (p. 163)
- Working With Keys (p. 163)
- Encrypting and Decrypting Data Keys (p. 165)
- Working with Key Policies (p. 167)
- Working with Grants (p. 168)
- Working with Aliases (p. 170)

Creating a Client

To use the AWS SDK for Java to write code that uses the AWS Key Management Service (AWS KMS) API, you start by creating a client. The following code snippet shows you how to do this using the SDK's client builder. For more information about using the client builder, see the following resources.

- Fluent Client Builders on the AWS Developer Blog
- Creating Service Clients in the AWS SDK for Java Developer Guide
- AWSKMSClientBuilder in the AWS SDK for Java API Reference

The client object, `kms`, is used in the example code in the topics that follow.

```java
AWSKMS kms = AWSKMSClientBuilder.defaultClient();
```

Working With Keys

This topic discusses how to create, describe, list, enable, and disable keys in Java. For detailed information, see the AWS SDK for Java API Reference.
Creating a Customer Master Key

To create a customer master key (p. 2), use the CreateKey operation. For details about the Java implementation, see the createKey method in the AWS SDK for Java API Reference.

```
// Create a CMK

String desc = "Key for protecting critical data";
CreateKeyRequest req = new CreateKeyRequest().withDescription(desc);
CreateKeyResult result = kms.createKey(req);
```

Creating a Data Key

To generate a data key, use the GenerateDataKey operation. This operation returns plaintext and encrypted copies of the data key that it creates. For details about the Java implementation, see the generateDataKey method in the AWS SDK for Java API Reference.

```
// Generate a data key

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_128");

GenerateDataKeyResult dataKeyResult = kmsClient.generateDataKey(dataKeyRequest);
ByteBuffer plaintextKey = dataKeyResult.getPlaintext();
ByteBuffer encryptedKey = dataKeyResult.getCiphertextBlob();
```

Getting Information About a Custom Master Key

To get detailed information about a CMK, including the key ARN and key state, use the DescribeKey operation. For details about the Java implementation of DescribeKey, see the describeKey method in the AWS SDK for Java API Reference.

DescribeKey does not get aliases. To get aliases, use the ListAliases operation.

```
// Describe a CMK

// Replace the fictitious key ARN with a valid one.
String keyId = "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
```
Getting Key IDs and Key ARNs of Customer Master Keys

To get the key IDs and key ARNs of the customer master keys, use the `ListKeys` operation. For details about the Java implementation, see the `ListKeys` method in the AWS SDK for Java API Reference.

```java
// List CMKs in this account
//
Integer limit = 10;
String marker = null;
ListKeysRequest req = new ListKeysRequest().withMarker(marker).withLimit(limit);
ListKeysResult result = kms.listKeys(req);
```

Enabling Customer Master Keys

To enable a disabled CMK, use the `EnableKey` operation. For details about the Java implementation, see the `EnableKey` method in the AWS SDK for Java API Reference.

```java
// Enable a CMK
//
String keyId = "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
EnableKeyRequest req = new EnableKeyRequest().withKeyId(keyId);
kms.enableKey(req);
```

Disabling Customer Master Keys

To disable a CMK, use the `DisableKey` operation. Disabling a CMK prevents it from being used. For details about the Java implementation, see the `DisableKey` method in the AWS SDK for Java API Reference.

```java
// Disable a CMK
//
String keyId = "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
DisableKeyRequest req = new DisableKeyRequest().withKeyId(keyId);
kms.disableKey(req);
```

Encrypting and Decrypting Data Keys

This topic shows how to use the `Encrypt`, `Decrypt`, and `ReEncrypt` operations in the AWS KMS API.

These operations are designed to encrypt and decrypt data keys (p. 2). They use an AWS KMS customer master key (p. 2) (CMK) in the encryption operations and they cannot accept more than 4 KB (4096 bytes) of data. Although you might use them to encrypt small amounts of data, such as a password or RSA key, they are not designed to encrypt application data.
To encrypt application data, use the server-side encryption features of an AWS service, or a client-side encryption library, such as the AWS Encryption SDK or the Amazon S3 encryption client.

**Topics**
- Encrypting a Data Key (p. 166)
- Decrypting a Data Key (p. 166)
- Re-Encrypting a Data Key Under a Different Customer Master Key (p. 166)

### Encrypting a Data Key

The Encrypt operation is designed to encrypt data keys, but it is not frequently used. The GenerateDataKey and GenerateDataKeyWithoutPlaintext operations return encrypted data keys. You might use this method when you are moving encrypted data to a new region and want to encrypt its data key with a CMK in the new region.

For details about the Java implementation of the Encrypt operation, see the encrypt method in the AWS SDK for Java API Reference.

```java
// Encrypt a data key
// Replace the fictitious keyID value with a valid key ID, key ARN, or alias of an AWS CMK.
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 = kms.encrypt(req).getCiphertextBlob();
```

### Decrypting a Data Key

To decrypt a data key, use the Decrypt operation. For details about the Java implementation, see the decrypt method in the AWS SDK for Java API Reference.

The ciphertextBlob must be a byte buffer that was returned by the GenerateDataKey, GenerateDataKeyWithoutPlaintext, or Encrypt operations.

```java
// Decrypt a data key
//
ByteBuffer ciphertextBlob = Place your ciphertext here;
DecryptRequest req = new DecryptRequest().withCiphertextBlob(ciphertextBlob);
ByteBuffer plainText = kms.decrypt(req).getPlaintext();
```

### Re-Encrypting a Data Key Under a Different Customer Master Key

To decrypt an encrypted data key, and then immediately re-encrypt the data key under a different customer master key (CMK), use the ReEncrypt operation. The operations are performed entirely on the server side within AWS KMS, so they never expose your plaintext outside of AWS KMS.

The ciphertextBlob must be a byte buffer that was returned by the GenerateDataKey, GenerateDataKeyWithoutPlaintext, or Encrypt operations.
For details about the Java implementation, see the `reEncrypt method` in the `AWS SDK for Java API Reference`.

```
// Re-encrypt a data key
ByteBuffer sourceCiphertextBlob = Place your ciphertext here;

// Replace the fictitious keyID value with a valid key ID, key ARN, or alias of an AWS CMK.
String destinationKeyId = "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321";

ReEncryptRequest req = new ReEncryptRequest();
req.setCiphertextBlob(sourceCiphertextBlob);
req.setDestinationKeyId(destinationKeyId);
ByteBuffer destinationCipherTextBlob = kms.reEncrypt(req).getCiphertextBlob();
```

## Working with Key Policies

Use the AWS SDK for Java and the following sample code to list, get, and set key policies for AWS KMS customer master keys (CMKs). This sample code requires that you previously instantiated an AWSKMSClient as `kms`.

### Topics
- Listing Key Policy Names (p. 167)
- Getting a Key Policy (p. 167)
- Setting a Key Policy (p. 168)

### Listing Key Policy Names

To list the names of key policies for a customer master key, use the `ListKeyPolicies` operation. Currently, the only key policy name it returns is `default`. For details about the Java implementation, see the `listKeyPolicies method` in the `AWS SDK for Java API Reference`.

```
// List key policy names

String keyId = "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";

ListKeyPoliciesRequest req = new ListKeyPoliciesRequest().withKeyId(keyId);
ListKeyPoliciesResult result = kms.listKeyPolicies(req);
```

### Getting a Key Policy

To get information about a particular key policy of a customer master key, use the `GetKeyPolicy` operation. For details about the Java implementation, see the `getKeyPolicy method` in the `AWS SDK for Java API Reference`.

`GetKeyPolicy` requires a policy name. You can use the `ListKeyPolicies` operation to get the policy name, but currently, the only policy name is `default`.

```
// Get the policy for a CMK
```
Setting a Key Policy

To establish or change a key policy for a CMK, use the PutKeyPolicy operation. For details about the Java implementation, see the putKeyPolicy method in the AWS SDK for Java API Reference.

PutKeyPolicy requires a policy name. You can use the ListKeyPolicies operation to get the policy name, but currently, the only policy name is default.

Working with Grants

This topic discusses how to create, retire, revoke, and list grants on AWS KMS customer master keys (CMKs).

Topics

- Creating a Grant (p. 169)
- Retiring a Grant (p. 169)
- Revoking a Grant (p. 169)
- Get Information about Grants (p. 169)
Creating a Grant

To create a grant for an AWS KMS customer master key, use the CreateGrant operation. For details about the Java implementation, see the createGrant method in the AWS SDK for Java API Reference.

```java
// Create a grant
//
// Replace the following fictitious key ARN with a valid key ID
String keyId = "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
String granteePrincipal = "arn:aws:iam::111122223333:user/Alice";
String operation = GrantOperation.Encrypt;

CreateGrantRequest req = new CreateGrantRequest();
req.setKeyId(keyId);
req.setGranteePrincipal(granteePrincipal);
req.setOperation(operation);

CreateGrantResult result = kms.createGrant(req);
```

Retiring a Grant

To retire a grant for an AWS KMS customer master key, use the RetireGrant operation. You should retire a grant to clean up after you are done using it. For details about the Java implementation, see the retireGrant method in the AWS SDK for Java API Reference.

```java
// Retire a grant
//
String grantToken = Place your grant token here;

RetireGrantRequest req = new RetireGrantRequest().withGrantToken(grantToken);
kms.reireGrant(req);
```

Revoking a Grant

To revoke a grant to an AWS KMS customer master key, use the RevokeGrant operation. You can revoke a grant to explicitly deny operations that depend on it. For details about the Java implementation, see the revokeGrant method in the AWS SDK for Java API Reference.

```java
// Revoke a grant on a CMK
//
// Replace the following fictitious key ARN with a valid key ID
String keyId = "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
String grantId = "grant1";

RevokeGrantRequest req = new RevokeGrantRequest().withKeyId(keyId).withGrantId(grantId);
kms.revokeGrant(req);
```

Get Information about Grants

To get detailed information about the grants on an AWS KMS customer master key, use the ListGrants operation. For details about the Java implementation, see the listGrants method in the AWS SDK for Java API Reference.

```java
// Listing grants on a CMK
```
Working with Aliases

This topic explains how to create, delete, list, and update aliases.

An alias is an optional display name for a customer master key (CMK) (p. 2).

Each CMK can have multiple aliases, but each alias points to only one CMK. The alias name must be unique in the AWS account and region. To simplify code that runs in multiple regions, you can use the same alias name, but point it to a different CMK in each region.

You can use AWS KMS API operations to list, create, and delete aliases. You can also update an alias, which associates an existing alias with a different CMK. There is no operation to edit or change an alias name. If you create an alias for a CMK that already has an alias, the operation creates another alias for the same CMK. To change an alias name, delete the current alias and then create a new alias for the CMK.

Because an alias is not a property of a CMK, it can be associated with and disassociated from an existing CMK without changing the properties of the CMK. Deleting an alias does not delete the underlying CMK.

You can use an alias as the value of the KeyId parameter only in the following operations:

- DescribeKey
- Encrypt
- GenerateDataKey
- GenerateDataKeyWithoutPlaintext
- ReEncrypt

Aliases are created in an AWS account and are known only to the account in which you create them. You cannot use an alias name or alias ARN to identify a CMK in a different AWS account.

To specify an alias, use the alias name or alias ARN, as shown in the following example. In either case, be sure to prepend "alias/" to the alias name.

// Fully specified ARN

// Alias name (prefixed with "alias/")
alias/ExampleAlias

Topics

- Creating an Alias (p. 171)
- Deleting an Alias (p. 171)
- Listing Aliases (p. 171)
- Updating an Alias (p. 171)
Creating an Alias

To create an alias, use the `CreateAlias` operation. The alias must be unique in the account and region. If you create an alias for a CMK that already has an alias, `CreateAlias` creates another alias to the same CMK. It does not replace the existing alias.

For details about the Java implementation, see the `createAlias` method in the AWS SDK for Java API Reference.

```java
// Create an alias for a CMK
String aliasName = "alias/projectKey1";
String targetKeyId = "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
CreateAliasRequest req = new CreateAliasRequest().withAliasName(aliasName).withTargetKeyId(targetKeyId);
kms.createAlias(req);
```

Deleting an Alias

To delete an alias, use the `DeleteAlias` operation. Deleting an alias has no effect on the underlying CMK. For details about the Java implementation, see the `deleteAlias` method in the AWS SDK for Java API Reference.

```java
// Delete an alias for a CMK
String aliasName = "alias/projectKey1";
DeleteAliasRequest req = new DeleteAliasRequest().withAliasName(aliasName);
kms.deleteAlias(req);
```

Listing Aliases

To list all aliases, use the `ListAliases` operation. The response includes aliases that are defined by AWS services, but are not associated with a CMK. For details about the Java implementation, see the `listAliases` method in the AWS SDK for Java API Reference.

```java
// List the aliases in this AWS account
Integer limit = 10;
ListAliasesRequest req = new ListAliasesRequest().withLimit(limit);
ListAliasesResult result = kms.listAliases(req);
```

Updating an Alias

To associate an existing alias with a different CMK, use the `UpdateAlias` operation. For details about the Java implementation, see the `updateAlias` method in the AWS SDK for Java API Reference.

```java
// Updating an alias
String aliasName = "alias/projectKey1";
String targetKeyId = "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321";
```
UpdateAliasRequest req = new UpdateAliasRequest()
    .withAliasName(aliasName)
    .withTargetKeyId(targetKeyId);

kms.updateAlias(req);
Cryptography Basics

Following are some basic terms and concepts in cryptography that you’ll encounter when you work with AWS KMS.

Plaintext and Ciphertext

Plaintext refers to information or data in an unencrypted, or unprotected, form. Ciphertext refers to the output of an encryption algorithm operating on plaintext. Ciphertext is unreadable without knowledge of the algorithm and a secret key.

Algorithms and Keys

An encryption algorithm is a step-by-step set of instructions that specifies precisely how plaintext is transformed into ciphertext. Encryption algorithms require a secret key. AWS KMS uses the Advanced Encryption Standard (AES) algorithm in Galois/Counter Mode (GCM), known as AES-GCM. AWS KMS uses this algorithm with 256-bit secret keys.

Symmetric and Asymmetric Encryption

Encryption algorithms are either symmetric or asymmetric. Symmetric encryption uses the same secret key to perform both the encryption and decryption processes. Asymmetric encryption, also known as public-key encryption, uses two keys, a public key for encryption and a corresponding private key for decryption. The public key and private key are mathematically related so that when the public key is used for encryption, the corresponding private key must be used for decryption. AWS KMS uses only symmetric encryption.

For a more detailed introduction to cryptography and AWS KMS, see the following topics.

Topics

- How Symmetric Key Cryptography Works (p. 173)
- Authenticated Encryption (p. 174)
- Encryption Context (p. 175)
- Reference: AWS KMS and Cryptography Terminology (p. 176)

How Symmetric Key Cryptography Works

This topic provides a high-level introduction to how symmetric key cryptography uses algorithms to encrypt and decrypt data, the difference between block and stream ciphers, and how block ciphers use encryption modes to expand the effectiveness of the generic encryption schemes.

Encryption and Decryption

AWS KMS uses symmetric key cryptography to perform encryption and decryption. Symmetric key cryptography uses the same algorithm and key to both encrypt and decrypt digital data. The unencrypted data is typically called plaintext whether it is text or not. The encrypted data is typically called ciphertext. The following illustration shows a secret (symmetric) key and a symmetric algorithm being used to turn plaintext into ciphertext.
Authenticated Encryption

*Authenticated encryption* provides confidentiality, data integrity, and authenticity assurances on encrypted data. The *Encrypt* API takes plaintext, a customer master key (CMK) identifier, and an *encryption context* (p. 175) and returns ciphertext. The encryption context represents additional authenticated data (AAD). The encryption process uses the AAD only to generate an authentication tag. The tag is included with the output ciphertext and used as input to the decryption process. This means that the encryption context that you supply to the *Decrypt* API must be the same as the encryption context you supply to the *Encrypt* API. Otherwise, the encryption and decryption tags will not match, and the decryption process will fail to produce plaintext. Further, if any one of the parameters has been tampered with—specifically if the ciphertext has been altered—the authentication tag will not compute to the same value that it did during encryption. The decryption process will fail and the ciphertext will not be decrypted.

*Encryption context* (p. 175) is AWS KMS’s implementation of authenticated encryption or AAD. To learn how to use encryption context to protect the integrity of encrypted data, see the post *How to Protect the Integrity of Your Encrypted Data by Using AWS Key Management Service and EncryptionContext* on the AWS Security Blog.
Encryption Context

Encryption context is a set of key-value pairs that you can pass to AWS KMS when you call the Encrypt, Decrypt, ReEncrypt, GenerateDataKey, and GenerateDataKeyWithoutPlaintext APIs. It is checked for integrity but not stored as part of the ciphertext that is returned. Although the encryption context is not included in the ciphertext, it is cryptographically bound to the ciphertext during encryption and must be passed again when you call the Decrypt (or ReEncrypt) API. Decryption only succeeds if the encryption context you pass for decryption is exactly the same as the encryption context you passed during encryption. The encryption context is logged by AWS CloudTrail.

To learn how to use encryption context to protect the integrity of encrypted data, see the post How to Protect the Integrity of Your Encrypted Data by Using AWS Key Management Service and EncryptionContext on the AWS Security Blog.

Encryption context can consist of any values that you want. However, because it is not encrypted and because it is logged if CloudTrail logging is turned on, your encryption context should not include sensitive information. We further recommend that your encryption context describe the data being encrypted or decrypted so that you can better understand the CloudTrail log entries produced by AWS KMS. For example, Amazon EBS uses the ID of the encrypted volume as the encryption context for server-side encryption. If you are encrypting a file, you might use part of the file path as encryption context.

Topics

- Encryption Context in Grants and Key Policies (p. 175)
- Logging Encryption Context (p. 175)
- Storing Encryption Context (p. 175)

Encryption Context in Grants and Key Policies

In addition to using encryption context to check ciphertext integrity and authenticity, AWS KMS supports authorization by using grants and key policies that incorporate encryption context. Authorization that uses encryption context more tightly controls access to encrypted resources. When you create a grant, for example, you can optionally specify a set of constraints that specify an encryption context that unambiguously identifies the resource to which long-term access is being granted. For example, consider encrypted volumes with Amazon EBS and Amazon EC2: When an EBS volume is attached to an EC2 instance, a grant is created that allows only that instance to decrypt only that volume. This is accomplished by encoding the volume ID as the encryption context in the Constraint that is passed to the CreateGrant API. Without the encryption context in the constraint, the Amazon EC2 instance would obtain access to all volumes encrypted under the customer master key (CMK) rather than a specific volume.

Logging Encryption Context

AWS KMS uses AWS CloudTrail to log the encryption context so you can determine which CMKs and data have been accessed. That is, the log entry shows exactly which CMK was used to encrypt or decrypt specific data referenced by the encryption context in the log entry.

Important

Because the encryption context is logged, it must not contain sensitive information.

Storing Encryption Context

You should store the encryption context alongside the encrypted data to simplify using it when you call the Decrypt (or ReEncrypt) API. One security enhancement you might consider is to store only
enough of the encryption context to help you create the full encryption context on the fly when needed for encryption or decryption. For example, if you are encrypting a file and decide that the encryption context should be the full file path, store only part of that path alongside the encrypted file contents. Then, when you need the full encryption context, reconstruct it from the stored fragment. If someone then moves the file to a different location, when you recreate the encryption context, the context will be different and the decryption process will fail, indicating that your data has been tampered with.

Reference: AWS KMS and Cryptography Terminology

This section provides a brief glossary of terms for working with encryption in AWS KMS.

- **Additional authenticated data (AAD)**
  Offers both data-integrity and authenticity by using additional authenticated data during the encryption process. The AAD is authenticated but not encrypted. Using AAD with authenticated encryption enables the decryption process to detect any changes that may have been made to either the ciphertext or the additional authenticated data after encryption.

- **Authentication**
  The process of determining whether an entity is who it claims to be, or that information has not been manipulated by unauthorized entities.

- **Authorization**
  Specifies an entity’s legitimate access to a resource.

- **Block cipher modes**
  Encrypts plaintext to ciphertext where the plaintext and cipher text are of arbitrary length. Modes are typically used to encrypt something that is longer than one block.

- **Block ciphers**
  An algorithm that operates on blocks of data, one block at a time.

- **Data key**
  A symmetric key generated by AWS KMS for your service. Inside of your service or custom application, the data key is used to encrypt or decrypt data. It can be considered a resource by a service or application, or it can simply be metadata associated with the encrypted data.

- **Decryption**
  The process of turning ciphertext back into the form it had before encryption. A decrypted message is called plaintext.

- **Encryption**
  The process of providing data confidentiality to a plaintext message. An encrypted message is called ciphertext.

- **Encryption context**
  AWS KMS specific AAD in the form of a "key":"value" pair. Although not encrypted, it is bound to the ciphertext during encryption and must be passed again during decryption. If the encryption context passed for encryption is not the same as the encryption context passed for decryption or the ciphertext has been changed, the decryption process will fail.

- **Master key**
A key created by AWS KMS that can only be used within the AWS KMS service. The master key is commonly used to encrypt data keys so that the encrypted key can be securely stored by your service. However, AWS KMS master keys can also be used to encrypt or decrypt arbitrary chunks of data that are no greater than 4 KiB. Master keys are categorized as either customer managed keys or AWS managed keys. Customer managed keys are created by a customer for use by a service or application. AWS managed keys are the default keys used by AWS services that support encryption.

- **Symmetric key cryptography**

  Uses a single secret key to encrypt and decrypt a message.
Document History

The following table describes the important changes to the documentation since the last release of AWS Key Management Service.

- **Current API version:** 2014-11-01
- **Latest documentation update:** February 15, 2017

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Release Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>New content</td>
<td>Added documentation about Tagging Keys (p. 16).</td>
<td>February 15, 2017</td>
</tr>
<tr>
<td>New content</td>
<td>Added documentation about Monitoring Customer Master Keys (p. 129) and Monitoring with Amazon CloudWatch (p. 130).</td>
<td>August 31, 2016</td>
</tr>
<tr>
<td>New content</td>
<td>Added documentation about Importing Key Material (p. 69).</td>
<td>August 11, 2016</td>
</tr>
<tr>
<td>New content</td>
<td>Added the following documentation: Overview of Managing Access (p. 21), Using IAM Policies (p. 40), AWS KMS API Permissions Reference (p. 43), and Using Policy Conditions (p. 47).</td>
<td>July 5, 2016</td>
</tr>
<tr>
<td>Update</td>
<td>Updated portions of the documentation in the Authentication and Access Control (p. 20) chapter.</td>
<td>July 5, 2016</td>
</tr>
<tr>
<td>Update</td>
<td>Updated the Limits (p. 181) page to reflect new default limits.</td>
<td>May 31, 2016</td>
</tr>
<tr>
<td>Update</td>
<td>Updated the Limits (p. 181) page to reflect new default limits, and updated the Grant Tokens (p. 4) documentation to improve clarity and accuracy.</td>
<td>April 11, 2016</td>
</tr>
<tr>
<td>New content</td>
<td>Added documentation about Allowing Multiple IAM Users to Access a CMK (p. 36) and Using the IP Address Condition (p. 48).</td>
<td>February 17, 2016</td>
</tr>
<tr>
<td>Update</td>
<td>Updated the Using Key Policies in AWS KMS (p. 24) and Modifying a Key Policy (p. 34) pages to improve clarity and accuracy.</td>
<td>February 17, 2016</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Release Date</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Update</td>
<td>Updated the Getting Started (p. 5) topic pages to improve clarity.</td>
<td>January 5, 2016</td>
</tr>
<tr>
<td>New content</td>
<td>Added documentation about How AWS CloudTrail Uses AWS KMS (p. 98).</td>
<td>November 18, 2015</td>
</tr>
<tr>
<td>New content</td>
<td>Added instructions for Modifying a Key Policy (p. 34).</td>
<td>November 18, 2015</td>
</tr>
<tr>
<td>Update</td>
<td>Updated the documentation about How Amazon Relational Database Service (Amazon RDS) Uses AWS KMS (p. 113).</td>
<td>November 18, 2015</td>
</tr>
<tr>
<td>New content</td>
<td>Added documentation about How Amazon WorkSpaces Uses AWS KMS (p. 125).</td>
<td>November 6, 2015</td>
</tr>
<tr>
<td>Update</td>
<td>Updated the Using Key Policies in AWS KMS (p. 24) page to improve clarity.</td>
<td>October 22, 2015</td>
</tr>
<tr>
<td>New content</td>
<td>Added documentation about Deleting Customer Master Keys (p. 81), including supporting documentation about Creating an Amazon CloudWatch Alarm (p. 87) and Determining Past Usage of a Customer Master Key (p. 89).</td>
<td>October 15, 2015</td>
</tr>
<tr>
<td>New content</td>
<td>Added documentation about Determining Access to an AWS KMS Customer Master Key (p. 57).</td>
<td>October 15, 2015</td>
</tr>
<tr>
<td>New content</td>
<td>Added documentation about How Key State Affects Use of a Customer Master Key (p. 93).</td>
<td>October 15, 2015</td>
</tr>
<tr>
<td>New content</td>
<td>Added documentation about How Amazon Simple Email Service (Amazon SES) Uses AWS KMS (p. 114).</td>
<td>October 1, 2015</td>
</tr>
<tr>
<td>Update</td>
<td>Updated the Limits (p. 181) page to explain the new requests per second limits.</td>
<td>August 31, 2015</td>
</tr>
<tr>
<td>New content</td>
<td>Added information about the charges for using AWS KMS. See AWS KMS Pricing (p. 1).</td>
<td>August 14, 2015</td>
</tr>
<tr>
<td>New content</td>
<td>Added requests per second to the AWS KMS Limits (p. 181).</td>
<td>June 11, 2015</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Release Date</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>New content</td>
<td>Added a new Java code sample demonstrating use of the <code>UpdateAlias</code> API. See Updating an Alias (p. 171).</td>
<td>June 1, 2015</td>
</tr>
<tr>
<td>Update</td>
<td>Moved the AWS Key Management Service regions table to the AWS General Reference.</td>
<td>May 29, 2015</td>
</tr>
<tr>
<td>New content</td>
<td>Added documentation about How Amazon WorkMail Uses AWS KMS (p. 123).</td>
<td>January 28, 2015</td>
</tr>
<tr>
<td>New content</td>
<td>Added documentation about How Amazon Relational Database Service (Amazon RDS) Uses AWS KMS (p. 113).</td>
<td>January 6, 2015</td>
</tr>
<tr>
<td>New content</td>
<td>Added documentation about How Amazon Elastic Transcoder Uses AWS KMS (p. 105).</td>
<td>November 24, 2014</td>
</tr>
<tr>
<td>New guide</td>
<td>Introduced the AWS Key Management Service Developer Guide.</td>
<td>November 12, 2014</td>
</tr>
</tbody>
</table>
Limits

All AWS KMS objects have limits that apply to each region and each AWS account. If you need to exceed these limits, please visit the AWS Support Center and create a case.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Default Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Master Keys (CMKs) (p. 181)</td>
<td>1000</td>
</tr>
<tr>
<td>Aliases (p. 181)</td>
<td>1100</td>
</tr>
<tr>
<td>Grants per CMK (p. 181)</td>
<td>2500</td>
</tr>
<tr>
<td>Grants for a given principal per CMK (p. 182)</td>
<td>500</td>
</tr>
<tr>
<td>Requests per second (p. 182)</td>
<td>Varies by API operation; see table (p. 183).</td>
</tr>
</tbody>
</table>

**Note**

If you are exceeding the requests per second (p. 182) limit, consider using the data key caching feature of the AWS Encryption SDK. Reusing data keys, rather than requesting a new data key for every encryption operation, might reduce the frequency of your requests to AWS KMS.

Customer Master Keys (CMKs): 1000

You can have up to 1000 CMKs per region. All CMKs count towards this limit regardless of their status (enabled, disabled, or pending deletion). You can request more CMKs in a region; however, managing a large number of CMKs from the AWS Management Console may be slower than acceptable. If you have a large number of CMKs in a region, we recommend managing them programmatically with the AWS SDKs or AWS Command Line Tools.

Aliases: 1100

An alias is an independent display name that you can map to a CMK. It is not a property of a CMK. You can map multiple aliases to a single CMK, so the limit for aliases is higher than the limit for CMKs. If you request an increase in the number of CMKs, you might also need to request an increase in the number of aliases.

Grants per CMK: 2500

Grants (p. 57) are advanced mechanisms for specifying permissions that you or an AWS service integrated with AWS KMS can use to limit how and when a CMK can be used. Grants are attached to a CMK, and each grant contains the principal who receives permission to use the CMK, the ID of the CMK, and a list of operations that can be performed. Grants are an alternative to the key policy (p. 24).

Each CMK can have up to 2500 grants, including the grants created by AWS services that are integrated with AWS KMS. For a list of these services, see How AWS Services use AWS KMS (p. 96). One effect of
Grants for a given principal per CMK: 500

For a given CMK, no more than 500 grants can specify the same grantee principal. For example, assume that you want to encrypt multiple Amazon EBS volumes and attach them to a single Amazon Elastic Compute Cloud (Amazon EC2) instance. In this case, a unique grant is created for each encrypted volume and all of these grants have the same grantee principal (an IAM assumed-role user associated with the EC2 instance). Each grant gives permission to use the specified CMK to decrypt an EBS volume's unique data encryption key. For each CMK, you can have up to 500 grants that specify the same EC2 instance as the grantee principal. This effectively means that you can have no more than 500 encrypted EBS volumes per EC2 instance for a given CMK.

Requests per second: varies

AWS KMS throttles API requests at different limits depending on the API operation. Throttling means that AWS KMS rejects an otherwise valid request because the request exceeds the limit for the number of requests per second. When a request is throttled, AWS KMS returns a ThrottlingException error. The following table lists each API operation and the point at which AWS KMS throttles requests for that operation.

Note
If you are exceeding the requests per second limit for the GenerateDataKey API operation, consider using the data key caching feature of the AWS Encryption SDK. Reusing data keys might reduce the frequency of your requests to AWS KMS.

Shared limit

The API operations in the first row of the following table share a limit of 1200 requests per second. For example, when you make 600 GenerateDataKey and 400 Decrypt requests per second, AWS KMS doesn't throttle your requests. However, when you make 200 Encrypt and 1100 GenerateDataKey requests per second, AWS KMS throttles your requests because you are making more than 1200 requests per second for operations with the shared limit.

The remaining API operations have a unique limit for requests per second, which means the limit is not shared.

API requests made on your behalf

You can make API requests directly or by using an integrated AWS service that makes API requests to AWS KMS on your behalf. The limit applies to both kinds of requests.

For example, you might store data in Amazon S3 using server-side encryption with AWS KMS (SSE-KMS). Each time you upload or download an S3 object that's encrypted with SSE-KMS, Amazon S3 makes a GenerateDataKey (for uploads) or Decrypt (for downloads) request to AWS KMS on your behalf. These requests count toward your limit, so AWS KMS throttles the requests if you exceed a combined total of 1200 uploads or downloads per second of S3 objects encrypted with SSE-KMS.

Cross-account requests

When an application in one AWS account uses a CMK owned by a different account, that's known as a cross-account request. For cross-account requests, AWS KMS throttles the account that makes the requests, not the account that owns the CMK. For example, you might have applications in accounts
A and B that both use a CMK in account C. In this scenario, the limit for requests per second applies separately to accounts A and B, not to account C.

**Requests per second limit for each AWS KMS API operation**

<table>
<thead>
<tr>
<th>API operation</th>
<th>Requests per second limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decrypt</td>
<td>1200 (shared)</td>
</tr>
<tr>
<td>Encrypt</td>
<td></td>
</tr>
<tr>
<td>GenerateDataKey</td>
<td></td>
</tr>
<tr>
<td>GenerateDataKeyWithoutPlaintext</td>
<td></td>
</tr>
<tr>
<td>GenerateRandom</td>
<td></td>
</tr>
<tr>
<td>ReEncrypt</td>
<td></td>
</tr>
<tr>
<td>CancelKeyDeletion</td>
<td>5</td>
</tr>
<tr>
<td>CreateAlias</td>
<td>5</td>
</tr>
<tr>
<td>CreateGrant</td>
<td>50</td>
</tr>
<tr>
<td>CreateKey</td>
<td>5</td>
</tr>
<tr>
<td>DeleteAlias</td>
<td>5</td>
</tr>
<tr>
<td>DeleteImportedKeyMaterial</td>
<td>5</td>
</tr>
<tr>
<td>DescribeKey</td>
<td>30</td>
</tr>
<tr>
<td>DisableKey</td>
<td>5</td>
</tr>
<tr>
<td>DisableKeyRotation</td>
<td>5</td>
</tr>
<tr>
<td>EnableKey</td>
<td>5</td>
</tr>
<tr>
<td>EnableKeyRotation</td>
<td>5</td>
</tr>
<tr>
<td>GetKeyPolicy</td>
<td>30</td>
</tr>
<tr>
<td>GetKeyRotationStatus</td>
<td>30</td>
</tr>
<tr>
<td>GetParametersForImport</td>
<td>0.25 (AWS KMS throttles requests when the rate is more than 1 per 4 seconds)</td>
</tr>
<tr>
<td>ImportKeyMaterial</td>
<td>5</td>
</tr>
<tr>
<td>ListAliases</td>
<td>5</td>
</tr>
<tr>
<td>ListGrants</td>
<td>5</td>
</tr>
<tr>
<td>ListKeyPolicies</td>
<td>5</td>
</tr>
<tr>
<td>ListKeys</td>
<td>5</td>
</tr>
<tr>
<td>ListResourceTags</td>
<td>5</td>
</tr>
<tr>
<td>ListRetirableGrants</td>
<td>5</td>
</tr>
<tr>
<td>PutKeyPolicy</td>
<td>5</td>
</tr>
<tr>
<td>API operation</td>
<td>Requests per second limit</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>RetireGrant</td>
<td>15</td>
</tr>
<tr>
<td>RevokeGrant</td>
<td>15</td>
</tr>
<tr>
<td>ScheduleKeyDeletion</td>
<td>5</td>
</tr>
<tr>
<td>TagResource</td>
<td>5</td>
</tr>
<tr>
<td>UntagResource</td>
<td>5</td>
</tr>
<tr>
<td>UpdateAlias</td>
<td>5</td>
</tr>
<tr>
<td>UpdateKeyDescription</td>
<td>5</td>
</tr>
</tbody>
</table>