# CMK Encryption on AWS (Preview)

Date published: 2021-08-05
Date modified: 2021-08-05

# Legal Notice

# Contents

# What is a Customer Master Key (CMK)

In AWS, the Key Management System (KMS) provides keys for encrypting data and file systems. Typically, KMS is used to generate and manage keys, but as an alternative, you are able to generate a key yourself and use it to encrypt data and file systems in AWS. In this case, you are responsible for generating, maintaining, and rotating keys. This is the Customer Managed Key (CMK). You have full control over CMKs, including establishing and maintaining the key policies, IAM policies, grants, enabling and disabling them, rotating their cryptographic material, adding tags, creating aliases that refer to the CMK, and scheduling the CMKs for deletion.

# Prerequisites

- The customer must create the CMK using the AWS KMS service.

# Limitations

- Only automatic key rotation is supported.
- CML only supports symmetric keys for CMK encryption

# Implementing CMK on AWS

Follow the steps below to begin using CMK.

## 1. Create a key

You create a customer-managed CMK in the Key Management System (KMS) of AWS.

1. In AWS, go to KMS > Customer managed keys.
2. Click Create key, and accept the defaults.
3. Enter an alias, which is a user-friendly name for the key.
4. Click Key ID, and copy the ARN shown there.

You use this ARN to create the workspace.

## 2. Update policies

To use CMKs in CML, ensure that the following two permission blocks are added to the policy section, in addition to the default policies:

```
{
            "Sid": "Allow Autoscaling service-linked role for
attachment of persistent resources",
            "Effect": "Allow",
            "Principal": {
                "AWS":
"arn:aws:iam::[YOUR-ACCOUNT-ID]:role/aws-service-role/autoscaling.ama
zonaws.com/AWSServiceRoleForAutoScaling"
            },
            "Action": "kms:CreateGrant",
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                }
            }
        },
        {
            "Sid": "Allow Autoscaling service-linked role use of the
CMK",
            "Effect": "Allow",
            "Principal": {
                "AWS":
"arn:aws:iam::[YOUR-ACCOUNT-ID]:role/aws-service-role/autoscaling.ama
zonaws.com/AWSServiceRoleForAutoScaling"
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        }
```

2. Update the cross account role attached to the corresponding environment.

# 3. Create a workspace in the CDP CLI

The following CLI command creates a workspace. The CMK is included as the value for “customerKMSKeyArn” in the following command skeleton. Other values are the same as you enter in the Provision ML Workspace UI.

```
cdp ml create-workspace --generate-cli-skeleton
2021-07-22 19:40:54,388 - MainThread - cdpcli.clidriver - WARNING - You are running an INTERNAL release of the CDP CLI, which has different capabilities from the standard public release. Find the public release at: https://pypi.org/project/cdpcli/
{
    "environmentName": "",
    "workspaceName": "",
    "usePublicLoadBalancer": true,
    "disableTLS": true,
    "provisionK8sRequest": {
        "instanceGroups": [
            {
                "instanceType": "",
                "instanceTier": "",
                "instanceCount": 0,
                "name": "",
                "ingressRules": [
                    ""
                ],
                "rootVolume": {
                    "size": 0
                },
                "autoscaling": {
                    "minInstances": 0,
                    "maxInstances": 0,
                    "enabled": true
                }
            }
        ],
        "environmentName": "",
        "tags": [
            {
                "key": "",
                "value": ""
            }
        ],
        "network": {
            "plugin": "",
            "options": {
                "encryption": ""
            },
            "topology": {
                "subnets": [
                    ""
                ]
```

```
        },
        "serviceCidr": ""
      },
      "useLegacyNodeLabel": true,
      "xEntitlements": [
        ""
      ]
    },
    "disableSSO": true,
    "enableMonitoring": true,
    "enableGovernance": true,
    "existingNFS": "",
    "kubeconfig": "",
    "enableYunikorn": true,
    "loadBalancerIPWhitelists": [
      ""
    ],
    "nfsVersion": "",
    "mlVersion": "",
    "kubernetesVersion": "",
    "enableModelMetrics": true,
    "namespace": "",
    "existingDatabaseConfig": {
      "existingDatabaseHost": "",
      "existingDatabasePort": "",
      "existingDatabaseName": "",
      "existingDatabaseUser": "",
      "existingDatabasePassword": ""
    },
    "useSpotInstancesForMlInfra": true,
    "useSpotInstancesForLiftieInfra": true,
    "whitelistAuthorizedIPRanges": true,
    "authorizedIPRanges": [
      ""
    ],
    "useLegacyHelm2": true,
    "useLegacyEFS": true,
    "additionalRuntimeRepo": "",
    "mlGovernancePrincipal": "",
    "skipValidation": true,
    "customerKMSKeyArn": "",
    "imageCatalog": {
      "name": "",
      "crn": ""
    }
}
```

# References

| | |
|---|---|
| Instructions for using AWS IAM restricted Role and Policy for Compute(Liftie) & CML | https://docs.google.com/document/d/1zGIcYVF4Y8b8jsA2kvss5Qhb8WkS62peFpClBAovgM8 |
| Customer master key - Concepts | https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#master_keys |
| Rotating customer master keys | https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html |
| Creating CMK | https://docs.aws.amazon.com/kms/latest/developerguide/create-keys.html |
| How to choose your CMK configuration | https://docs.aws.amazon.com/kms/latest/developerguide/symm-asymm-choose.html |