

CMK Encryption on AWS (Preview)

Date published: 2021-08-05

Date modified: 2021-08-05

Legal Notice

© Cloudera Inc. 2021. All rights reserved.

The documentation is and contains Cloudera proprietary information protected by copyright and other intellectual property rights. No license under copyright or any other intellectual property right is granted herein.

Copyright information for Cloudera software may be found within the documentation accompanying each component in a particular release.

Cloudera software includes software from various open source or other third party projects, and may be released under the Apache Software License 2.0 ("ASLv2"), the Affero General Public License version 3 (AGPLv3), or other license terms.

Other software included may be released under the terms of alternative open source licenses. Please review the license and notice files accompanying the software for additional licensing information.

Please visit the Cloudera software product page for more information on Cloudera software. For more information on Cloudera support services, please visit either the Support or Sales page. Feel free to contact us directly to discuss your specific needs.

Cloudera reserves the right to change any products at any time, and without notice. Cloudera assumes no responsibility nor liability arising from the use of products, except as expressly agreed to in writing by Cloudera.

Cloudera, Cloudera Altus, HUE, Impala, Cloudera Impala, and other Cloudera marks are registered or unregistered trademarks in the United States and other countries. All other trademarks are the property of their respective owners.

Disclaimer: EXCEPT AS EXPRESSLY PROVIDED IN A WRITTEN AGREEMENT WITH CLOUDERA, CLOUDERA DOES NOT MAKE NOR GIVE ANY REPRESENTATION, WARRANTY, NOR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, IN CONNECTION WITH CLOUDERA TECHNOLOGY OR RELATED SUPPORT PROVIDED IN CONNECTION THEREWITH. CLOUDERA DOES NOT WARRANT THAT CLOUDERA PRODUCTS NOR SOFTWARE WILL OPERATE UNINTERRUPTED NOR THAT IT WILL BE FREE FROM DEFECTS NOR ERRORS, THAT IT WILL PROTECT YOUR DATA FROM LOSS, CORRUPTION NOR UNAVAILABILITY, NOR THAT IT WILL MEET ALL OF CUSTOMER'S BUSINESS REQUIREMENTS. WITHOUT LIMITING THE FOREGOING, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, CLOUDERA EXPRESSLY DISCLAIMS ANY AND ALL IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, QUALITY, NON-INFRINGEMENT, TITLE, AND FITNESS FOR A PARTICULAR PURPOSE AND ANY REPRESENTATION, WARRANTY, OR COVENANT BASED ON COURSE OF DEALING OR USAGE IN TRADE.

This document has been released as part of a technical preview for features described herein. Technical preview components are provided as a convenience to our customers for their evaluation and trial usage. These components are provided 'as is' without warranty or support. Further, Cloudera assumes no liability for the usage of technical preview components, which should be used by customers at their own risk.

Contents

Legal Notice	2
What is a Customer Master Key (CMK)	4
Prerequisites	4
Limitations	4
Implementing CMK on AWS	4
1. Create a key	4
2. Update policies	5
3. Create a workspace in the CDP CLI	6
References	8
How to choose your CMK configuration	8

This document has been released as part of a technical preview for features described herein. Technical preview components are provided as a convenience to our customers for their evaluation and trial usage. These components are provided 'as is' without warranty or support. Further, Cloudera assumes no liability for the usage of technical preview components, which should be used by customers at their own risk.

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.

This document has been released as part of a technical preview for features described herein. Technical preview components are provided as a convenience to our customers for their evaluation and trial usage. These components are provided 'as is' without warranty or support. Further, Cloudera assumes no liability for the usage of technical preview components, which should be used by customers at their own risk.

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.

This document has been released as part of a technical preview for features described herein. Technical preview components are provided as a convenience to our customers for their evaluation and trial usage. These components are provided 'as is' without warranty or support. Further, Cloudera assumes no liability for the usage of technical preview components, which should be used by customers at their own risk.

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": [
          ""
        ]
      }
    ]
  }
}
```

This document has been released as part of a technical preview for features described herein. Technical preview components are provided as a convenience to our customers for their evaluation and trial usage. These components are provided 'as is' without warranty or support. Further, Cloudera assumes no liability for the usage of technical preview components, which should be used by customers at their own risk.

CLUDERA TECHNICAL PREVIEW DOCUMENTATION

```
    },
    "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,
"useSpotInstancesForLiftiInfra": true,
"whitelistAuthorizedIPRanges": true,
"authorizedIPRanges": [
  ""
],
"useLegacyHelm2": true,
"useLegacyEFS": true,
"additionalRuntimeRepo": "",
"mlGovernancePrincipal": "",
"skipValidation": true,
"customerKMSKeyArn": "",
"imageCatalog": {
  "name": "",
  "crn": ""
}
}
```

This document has been released as part of a technical preview for features described herein. Technical preview components are provided as a convenience to our customers for their evaluation and trial usage. These components are provided 'as is' without warranty or support. Further, Cloudera assumes no liability for the usage of technical preview components, which should be used by customers at their own risk.

References

<p>Instructions for using AWS IAM restricted Role and Policy for Compute(Liftie) & CML</p>	<p>https://docs.google.com/document/d/1zGlcYVF4Y8b8jsA2kvss5Qhb8WkS62peFpCIBAovgM8</p>
<p>Customer master key - Concepts</p>	<p>https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#master_keys</p>
<p>Rotating customer master keys</p>	<p>https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html</p>
<p>Creating CMK</p>	<p>https://docs.aws.amazon.com/kms/latest/developerguide/create-keys.html</p>
<p>How to choose your CMK configuration</p>	<p>https://docs.aws.amazon.com/kms/latest/developerguide/symm-asymm-choose.html</p>

This document has been released as part of a technical preview for features described herein. Technical preview components are provided as a convenience to our customers for their evaluation and trial usage. These components are provided 'as is' without warranty or support. Further, Cloudera assumes no liability for the usage of technical preview components, which should be used by customers at their own risk.