



AWS Key Management Service data protection

R-Cloud Module Guide

Copyright notice

© 2024 HYCU. All rights reserved.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, distributed, transmitted, stored in a retrieval system, modified or translated to another language in any form by any means, without the prior written consent of HYCU.

Contents

Preparing for SaaS application data protection	4
Getting familiar with your SaaS application specifics	4
Backing up data	5
Configuring the SaaS application for backup operations	5
Editing the HycuPolicy JSON policy file	6
Restoring data	7

Preparing for SaaS application data protection

Before you start protecting your AWS KMS data, complete the following steps:

1. Getting familiar with ...
2. *AUTOMATICALLY GENERATED BY THE HELP SYSTEM*



Getting familiar with your SaaS application specifics

Before you start protecting your AWS KMS data, you must get familiar with all prerequisites, limitations, considerations, and/or recommendations in this topic to make sure that your module is prepared and configured correctly.

Prerequisite

An AWS account must be created.

Limitations

- When restoring, any policies added after the backup will be replaced with the policies that were effective during the backup.
- If a key is generated using the Import key material option:
 - The key material cannot be backed up and restored because of the API limitations. However, the configuration settings associated with the key can be restored.
 - In the Pending import key state, the restore will fail because of the key being in an inconsistent state.
- Backup and restore of the AWS-managed keys is not supported.
- If you restore a deleted single-Region key or a deleted multi-Region primary key, the keys are treated by AWS as new keys that cannot be used for decrypting the data that was encrypted by using the original keys. However, the module creates new key with all the metadata details of the original key.   Because of the AWS KMS API limitations:
 - The key that is scheduled for deletion cannot be updated.

- Backup and restore of the custom keystores is not supported.

Considerations

- If a key was in the pending deletion state during a backup, and still exists after a restore, the key state remains unaltered. If the key no longer exists after the restore, the key will be restored in the Disabled state.
- In the process of tag and alias restoring, the backed-up tags and aliases will be restored. The newly created tags and aliases that are added after the backup will also be available.
- An alias cannot be restored if the specified alias name is already assigned to another key within the same region.
- If the CloudHSM configuration is deleted or disconnected from the AWS CloudHSM key stores, the restore of the key associated with CloudHSM will fail.
- If an external key of the external keystore is deleted or disconnected from the external key stores, the restore of the key associated with the external key store will fail.
- Both external keystore keys and CloudHSM keystore keys can be backed up and restored if the custom keystore configurations are available and connected.

Backing up data

R-Cloud enables you to back up your AWS KMS data securely and efficiently.

Prerequisite

The HycuPolicy JSON policy document in the AWS management console requires you to manually add two statements.

For details, see [Editing the HycuPolicy JSON policy file](#).

Configuring the SaaS application for backup operations


After configuring the AWS Account and adding the AWS KMS module as a source in R-Cloud, all AWS KMS Custom Managed Keys and their properties will be automatically detected.

The supported objects are:

- Key
- Policy
- Alias
- Tag
- Key rotation status

R-Cloud starts protecting your AWS KMS data after you complete the following tasks:

1. Add the module as a source to R-Cloud. For instructions on how to add the module as a source, see [Adding the module to R-Cloud](#).
2. Add your AWS account as a source in R-Cloud. For instructions on how to add your AWS account as a source, see [Managing AWS accounts](#).

 **Note** When adding the AWS account as a source, make sure you sign into your AWS account by using the account root user or an IAM user with administrative permissions.

3. Edit the AWS JSON policy document. For instructions, see [Editing the HycuPolicy JSON file](#).
4. Assign a policy to the related SaaS application. For instructions, see [Defining your backup strategy](#).

Editing the HycuPolicy JSON policy file

In the IAM Management Console, click **Roles**, and then **HycuRole**. Click **HycuPolicy** to edit the policy. Append these statements to the existing HycuPolicy JSON policy file:

- Statement 1:

```
{
  "Effect": "Allow",
  "Action": [
    "kms:ListKeys",
    "kms:ListAliases",
    "kms:ListResourceTags",
    "kms:ListKeyPolicies",
    "kms:DescribeKey",
    "kms:GetKeyPolicy",
```

```

        "kms:GetKeyRotationStatus",
        "kms:CreateKey",
        "kms:CreateAlias",
        "kms:DisableKey",
        "kms:DisableKeyRotation",
        "kms:EnableKey",
        "kms:EnableKeyRotation",
        "kms:UpdateAlias",
        "kms:UpdateCustomKeyStore",
        "kms:UpdateKeyDescription",
        "kms:UpdatePrimaryRegion",
        "kms:PutKeyPolicy",
        "kms:TagResource",
        "kms:UntagResource",
        "kms:ReplicateKey"
    ],
    "Resource": "*"
}

```

- Statement 2:

```

{
    "Effect": "Allow",
    "Action": [
        "iam:PassRole",
        "iam:GetRole",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:GetPolicyVersion",
        "iam:GetRolePolicy"
    ],
    "Resource": "*"
}

```

Restoring data

R-Cloud enables you to restore an entire SaaS application or its resources to a specific point in time.

The protected AWS Key Management Service data can be restored on the following levels:

- Key
- Policy

- Alias
- Tag
- Key rotation status

Provide feedback

For any suggestions and comments regarding this product or its documentation, send us an e-mail to:

info@hycu.com

We will be glad to hear from you!

