HYCU

HYCU for AWS Key Management Service

R-Cloud Module Guide

Table of Contents

Copyright notice

About the module

With the R-Cloud (formerly HYCU Protégé) module for AWS Key Management Service (KMS), you can back up your cryptographic keys and data encryption configurations securely and efficiently.

Prerequisites

Before you add the module to R-Cloud as a source, the following prerequisites must be fulfilled:

- An AWS account must be created.
- The HycuPolicy JSON policy document in the AWS management console requires you to manually add two statements.

  For details, see section Editing the HycuPolicy JSON policy file.

Limitations

When adding the module to R-Cloud and while protecting the related SaaS application, the following limitations apply:

- 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.
- Because of the AWS KMS API limitations:
  - The rotation status will not be updated for the keys that are scheduled for deletion.

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

Considerations

Before you start with a restore, consider the following:

- 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.

Protecting data

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

1. Add the module as a source in R-Cloud. For instructions see *HYCU R-Cloud Help*.
2. Add your AWS account as a source in R-Cloud. For instructions see *HYCU R-Cloud Help*.

   > **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 policy file.

4. Assign a policy to the related SaaS application. For instructions, see *HYCU R-Cloud Help*.

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": "*"

         }
```

Backup

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.

For details on how to configure backups for your AWS KMS module, see *HYCU R-Cloud Help*.

The supported objects are:

- Key

- Policy
- Alias
- Tag
- Key rotation status

Restore

R-Cloud allows you to restore the protected AWS Key Management Service data at the following levels:

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

For details on how to configure the restore for your AWS KMS module, see *HYCU R-Cloud Help*.

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!

www.hycu.com

HYCU®