HYCU

HYCU for Amazon RDS

R-Cloud Module Guide

Table of Contents

Copyright notice

About the module

With the R-Cloud (formerly HYCU Protégé) module for Amazon RDS, you can back up your SaaS application data securely and efficiently. The module enables you to protect the data that is stored in your Amazon RDS instances.

The module currently supports the following database engines:

- Amazon Aurora (MySQL and PostgreSQL)
- MariaDB
- MySQL Community (instances and clusters)
- PostgreSQL (instances and clusters)
- SQL Server Express Edition

Prerequisites

Before you add the module to R-Cloud as a source, make sure your AWS account is assigned a role (username) that fulfills the following requirements:

- The role has the RDS permissions to create, restore, and delete the database snapshots.
- The role has the permission to call the `EC2 DescribeRegions` API (included in the `AmazonEC2ReadOnlyAccess` role or in the `ec2:DescribeRegions` permission).
- The role is permitted to read the Amazon Key Management Service (KMS) metadata. Specifically, the permission to read `kms:ListKeys` and `kms:DescribeKey` is required.

Limitations

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

- Protecting the custom database instances is not supported.
- Protecting the instances in the Amazon GovCloud is not supported.
- The maximum allocated Amazon S3 storage size for the restore is set to 1000 GiB.
- The number of snapshots that can be stored in Amazon S3 is by default limited to:
  - 100 instance snapshots per region
  - 100 cluster snapshots per region

  > **Note** You can increase the allowed number of snapshots in the AWS Management Console. For details, see AWS documentation.
- Using the Copy policy option to create the copies of backup data is not supported.

Considerations

The backup data is not copied to the Amazon S3 storage but remains in the same storage type as other snapshots in RDS. R-Cloud creates regional snapshots that are named using the following format:

`<OriginalInstanceName>-hycu-snapshot-yyyymmdd-hhmmss`

> Example
>
> The snapshot name for an instance named `db1` is: `db1-hycu-snapshot-20230301-114301`.

R-Cloud adds the following tags to the created snapshots:

Name	Value	Notes
`hycu-task-id`	UUID	Derived from the backup or restore request.
`hycu-instance-snapshot`	none	Only on database instance snapshots.
`hycu-cluster-snapshot`	none	Only on database cluster snapshots.

Protecting data

R-Cloud starts protecting the data stored in your Amazon RDS database after you add the module as a source to R-Cloud and assign a policy to the related SaaS application.

For details on how to add the module as a source, see *HYU R-Cloud Help*.

> **Note** The module backs up the data using snapshots that are stored in Amazon S3. Therefore, you cannot select a staging target when adding Amazon RDS as a source in R-Cloud.

Backing up data

R-Cloud allows you to define which Amazon RDS instances will be protected. To create the backups, R-Cloud uses the RDS snapshots.

For details on how to configure the backup for the SaaS application data, see *HYCU R-Cloud Help*.

Setting up automatic policy assignment

You can set up the automatic policy assignment for your Amazon RDS instances by applying the labels or the `hycu-policy` tag to your Amazon RDS instances or clusters in Amazon EC2. To do this, select the instance or the cluster that you want to configure, and then, in the Tags tab, click **Add**.

For details about how to set up the automatic policy assignment, see *HYCU R-Cloud Help*. For more information about adding the labels to the Amazon RDS instances or clusters, see AWS documentation.

Restoring data

You can restore your protected Amazon RDS instances by using the Restore option in R-Cloud. Keep in mind that:

- While restoring the Amazon RDS instances in R-Cloud, you can select the resources by their name or subnet group. If you are performing a cross-region restore, you can define the encryption key that will be used to copy the snapshot to the target region.
- When you restore the resource in R-Cloud, the resource retains most of its original configuration, including the default security group and the database parameter group. For more details, see AWS documentation about restoring the DB instance from a DB snapshot.

When performing a restore, R-Cloud takes the following parameters from the snapshot:

- The database engine and instance class
- The license model
- The port

The availability zone is taken from the original database if the database is being restored to the same region. Otherwise, the availability zone is chosen randomly by the module.

The VPC security group is set to the default security group for the database subnet group that was selected (or the default subnet group).

Resource tags and the Copy Tags to Snapshot property are restored.

The following Amazon RDS restore options are available in R-Cloud:

1. In-Place restore. The database instance or cluster will be restored to the original state (including their names). The in-place restore will delete any database instance or cluster with the same name. Before deletion, R-Cloud will create a final snapshot.
2. *For the MySQL Multi-AZ cluster:* The MySQL Multi-AZ cluster can be restored as a single database instance.

3. Restore to a different region. The module supports restoring a database instance or cluster to a different region. The following limitations apply:
    - The target region must define at least one RDS subnet group.
    - An encryption key suitable for being used with RDS must be available in the target region to copy the snapshot.
    - Restore to a different region is not supported for Multi-AZ clusters (PostgreSQL and MySQL).
    - For details on how to configure the restore for your Amazon RDS instances, 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®