HYCU for GitLab

R-Cloud Module Guide

Table of Contents

Copyright notice

About the module

With the R-Cloud (formerly HYCU Protégé) module for GitLab, you can back up your SaaS application data securely and efficiently.

Limitations

When adding the module and while protecting the related SaaS application, the following limitations apply:

- The creator's information about the comments, discussions, and discussion notes that are related to the issues, incidents, tasks, test cases, requirements, snippets, and commits will not be preserved during the restore. Instead, the information will be added to the body of comments, discussions, or discussion notes.
- Due to the GitLab API limitations:
  - The merge requests are included in the backup but cannot be automatically restored.
  - The attachments associated with the issues, incidents, tasks, test cases, requirements, snippets, commits, body/comments, discussions, or discussion notes cannot be backed up or restored. Instead, these links will be referenced only from the original project.
  - When transitioning a project from the Premium or Ultimate subscriptions to the Free subscription during a cross-group restore, certain metadata fields of the objects will not be fully restored. For example, only one assignee ID will be restored instead of the full list, and mapping for the milestones and assignees in issue boards cannot be restored.
- The following cannot be backed up or restored:
  - The objects associated with a group or a subgroup of a project, such as milestones, epics, iterations, variables, and other objects.
  - The project repository information such as forks, watches, stars, and license information.
  - The release assets.
  - The mapping of tasks along with their issues or incidents.
- During the restore, the releases require unique tag names for the project. If a tag is unavailable or already associated with another release during the restore, the tag and release cannot be restored.

- If an archived project is backed up, the variables associated with the project will not be backed up.
- If you perform a complete restore of an archived project, it will be restored as a non-archived project.
- You cannot perform a granular restore of objects to an archived project.
- The module does not protect the following objects: reactions, linked items, child items, designs, activities, branches, metrics information associated with the issues, incidents, tasks, test cases, requirements, snippets, commits, comments, discussions, discussion notes, and some metadata fields, such as the satisfied field in the requirements object.
- The wiki pages cannot be restored as separate items. Instead, the existing wiki pages will be replaced during the restore.
- The project issue board iteration information cannot be restored.

Considerations

Before you add the module as a source, consider the following:

- GitLab imposes rate limits. Triggering parallel backups or restores of multiple repositories might extend the time required to complete the module jobs.
- You must provide the GitLab group ID. Keep in mind that the source validation will fail if you provide the subgroup ID or if you update the ID to the subgroup ID.
- If you configure the source by using a token that is not your personal token, the backup and restore tasks might fail.
- If the configured token has access to another group or a subgroup, the cross-group restore is supported. To perform the cross-group restore, update the group ID with the one to be used for the restored data. By default, if the restore configuration is not updated with another group ID, the data will be restored to the original group or subgroup.
- During the restore of issues, tasks, requirements, test cases, or incidents, the old identification number (IID) will be prepended to the title to make the tracking easier.
- If the related environment is unavailable during the granular restore of the feature flags and deployment keys, a temporary string will be generated solely

for the representation in the restored objects. The environment will not be created.

Protecting data

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

1. Create a personal access token for the GitLab application. When selecting the desired scopes, select the following:
   - `api`
   - `read_api`
   - `read_user`
   - `read_repository`
   - `write_repository`

   > **Important** The personal access token must be linked to a group and generated by using either the maintainer role, the owner role, or a custom role. The custom role must be granted the necessary permissions for the supported objects.
   >
   > For details, see GitLab documentation about permissions and roles.

2. Add the module as a source to R-Cloud. For instructions, see *HYCU R-Cloud Help*.

   > **Note** When adding the module as a source, provide the GitLab group ID and the personal (bearer) token generated in the previous step.

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

Backing up data

After adding the module, all the repositories in the specified group, as well as their issues, comments, releases, and pull requests will be automatically detected.

The supported objects are:

- Repository sources:
  - Refs
  - Branches
  - Commits
  - Tags

  - Objects
  - Log
  - LFS files
- Commit comments and discussions:
  - Comment/discussion (text, creator, creation date)
  - Discussion notes (text, creator, creation date)
- Labels:
  - Name
  - Description
  - Color
- Milestones:
  - Status
  - Name
  - Description
  - Due date
  - Start date
- Wikis:
  - Wiki pages
  - Commits
  - Logs
- Snippets:
  - Name
  - Description
  - Files
  - Metadata
  - Comment/discussion (text, creator, creation date)
  - Discussion notes (text, creator, creation date)
- Issues/Test cases/Requirements/Incidents/Tasks/Merge Requests:
  - Title
  - Description
  - Metadata (creation date, creator, status, assignee, assigned labels, assigned milestones)
  - Comment/discussion (text, creator, creation date)
  - Discussion notes (text, creator, creation date)
- Releases:

  - Tag name
  - Title
  - Metadata (assigned milestone)
  - Release date
  - Release notes
  - Releases assets (links only)
- Feature flags:
  - Name
  - Description
  - Type
  - Environment
  - Strategies
- Environments:
  - Name
  - URL
- Deployment keys:
  - Key
  - Title
  - Metadata (expires at, can push)
- Variables:
  - Type
  - Environment
  - Flags
  - Description
  - Key
  - Value
- Issue boards:
  - Name
  - Label/milestone/assignee associations

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

Restoring data

R-Cloud allows you to restore the protected GitLab data at the following levels:

- Project
- Project wiki
- Project issue
- Project task
- Project requirement
- Project test case
- Project incident
- Project feature flag
- Project snippet
- Project release
- Project variable
- Project environment
- Project deployment key
- Project issue board

For details on how to restore the SaaS application data, 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®