



HYCU for AWS Parameter Store

R-Cloud Module Guide

Table of Contents

About the module.....	3
Prerequisites.....	3
Limitations	4
General limitations	4
Rate limiting.....	4
Known issue	5
Considerations.....	5
Protecting data.....	6
Editing the HycuPolicy JSON policy file.....	6
Backing up data	7
Restoring data	8

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.

About the module

With the R-Cloud (formerly HYCU Protégé) module for AWS Parameter Store, you can back up the current values of your created AWS parameters securely and efficiently.

Prerequisites

Before you add the module to R-Cloud as a source, your Authentication IAM account must be granted the minimum permissions set. The following permissions must be included:

- `ssm:DescribeParameters`
- `ssm:GetParameter`
- `ssm:PutParameter`
- `ssm:ListTagsForResource`
- `ssm:AddTagsToResource`
- `ssm:LabelParameterVersion`
- `kms:Decrypt`
- `kms:Encrypt`
- `ec2:DescribeRegions`
- `ec2:DescribeImages`

Instead of granting the individual permissions, you can also assign your Authentication IAM account the following policies:

- `AmazonSSMFullAccess`
- `AWSKeyManagementServicePowerUser`
- `AmazonEC2ReadOnlyAccess`


For the SecureString parameters, the corresponding KMS key alias must exist. The IAM Authentication account used when adding the module in R-Cloud must be granted the appropriate permissions.

Limitations

General limitations

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

- Only the latest parameter version is protected.
- The labels are not protected.
- Due to the API limitation, restoring a parameter value of an existing parameter whose oldest version has a label applied will fail.
- Restoring a parameter value that includes the backed-up tags to an existing parameter with a group of tags will complete with errors if the sum of the combined unique tags exceeds the maximum tag number limitation.

 **Note** Although the parameter value will be restored, the backed-up tags will not be applied.

- Restoring a SecureString parameter value for which the corresponding Key Management Service (KMS) key is no longer accessible will fail.
- When restoring a parameter that is assigned a notification expiration policy with an invalid time span according to the set expiration time, the expiration notification policies will not be restored.

Rate limiting

Parameter Store

The Parameter Store throughputs measured in transactions per second are:

- **Default throughput:** 40. The default throughput is shared by the following API calls: GetParameter, GetParameters, GetParametersByPath.
- **Higher throughput:** 10000. The higher throughput is used by the GetParameter API call.
- The SecureStrings parameters may be limited to the KMS throughput limits, depending on the region.

For the rate limiting details, see AWS documentation about the AWS Systems Manager endpoints and quotas.

KMS

The quotas vary according to the selected AWS Region, and the type of the KMS key used in the request. Each KMS quota is calculated separately. The quotas are adjustable. For details, see [AWS documentation about the request quotas](#).

Known issue

When restoring the `aws:ec2:image` data type parameter, the parameter store must validate the provided value of the Amazon EC2 AMI image ID.

The validation uses an asynchronous method. As a result, when trying to add the restored label to the version, the validation might not complete within the allocated time, and the parameter restore completes with a reported failure.

Considerations

- The restore can be configured to use the default KMS key for the SecureString parameters. If the original key is not available, the parameter value will be encrypted by using the default KMS key alias `alias/aws/ssm`.
- The AWS Systems Manager Parameter Store API interactions charges consist of interacting with the advanced parameters and using the higher throughput. Interacting with the standard parameters and using the standard throughput are available at no additional cost. For details, see [AWS Systems Manager pricing documentation](#).
- Creating a SecureString parameter is free of charge, but charges for using the AWS KMS encryption apply. For details, see [AWS KMS pricing documentation](#).
- The Parameter Store throughputs are configurable. If you see the throttling exception errors in the backup reports or if your backups take longer than expected, increase the Parameter Store throughput. Keep in mind that increasing the throughput results in additional charges. For details on configuring the throughput, see [AWS documentation on increasing or resetting the Parameter Store throughput](#). For details on pricing, see [AWS Systems Manager pricing documentation](#).

Protecting data

R-Cloud starts protecting the parameters in AWS Parameter Store 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 the following statements to the existing HycuPolicy JSON policy file:

- Statement 1:

```
{
  "Effect": "Allow",
  "Action": [
    "ssm:DescribeParameters",
    "ssm:GetParameter",
    "ssm:PutParameter",
    "ssm:ListTagsForResource",
    "ssm:AddTagsToResource",
    "ssm:LabelParameterVersion",
    "ec2:DescribeRegions"
  ],
```

```
"Resource": "*"
}
```

- Statement 2. Add this statement if you also want to protect the secured parameters:

```
{
  "Effect": "Allow",
  "Action": [
    "kms:Decrypt",
    "kms:Encrypt"
  ],
  "Resource": "*"
}
```

- Statement 3. Add this statement if you also want to protect the `aws:ec2:image` data type parameters.

```
{
  "Effect": "Allow",
  "Action": [
    "ec2:DescribeImages"
  ],
  "Resource": "*"
}
```

Backing up data

The resource type that is being backed up is Parameter.

The following configurable parameter metadata types are protected:

- Tags
- Policies

When creating a backup, the following APIs are called:

- `get_parameter`
- `list_tags_for_resource`

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

Restoring data

The module allows you to restore your protected AWS Parameter Store data on the Parameter level.

The APIs called to create a restore are:

- `put_parameter`
- `label_parameter_version`
- `add_tags_to_resource`

During the restore, the following restore configuration options are available:

- Use the default KMS key
- Create a new version if the parameter exists

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!

