HYCU

HYCU for AWS WAF

R-Cloud Module Guide

Table of Contents

Copyright notice

About the module

With the R-Cloud (formerly HYCU Protégé) module for AWS WAF, you can back up your SaaS application data securely and efficiently. The module enables you to protect the web application firewall (WAF) data that is managed by your AWS account.

Prerequisites

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

wafv2:AssociateWebACL	wafv2:UpdateManagedRuleSetVersionExpiryDate
wafv2:CreateWebACL	wafv2:CreateIPSet
wafv2:GetWebACL	wafv2:GetIPSet
wafv2:GetWebACLForResource	wafv2:ListIPSets
wafv2:GetLoggingConfiguration	wafv2:UpdateIPSet
wafv2:ListResourcesForWebACL	wafv2:CreateRegexPatternSet
wafv2:ListWebACLs	wafv2:GetRegexPatternSet
wafv2:UpdateWebACL	wafv2:ListRegexPatternSets
wafv2:CheckCapacity	wafv2:UpdateRegexPatternSet
wafv2:CreateRuleGroup	wafv2:CreateAPIKey
wafv2:DescribeManagedRuleGroup	wafv2:GetDecryptedAPIKey
wafv2:DescribeAllManagedProducts	wafv2:ListAPIKeys

wafv2:DescribeManagedProductsByVendor	wafv2:ListTagsForResource
wafv2:GetPermissionPolicy	cloudfront:ListDistributionsByWebACLId
wafv2:GetRuleGroup	cloudfront:GetDistribution
wafv2:ListAvailableManagedRuleGroupVersions	cloudfront:UpdateDistribution
wafv2:ListAvailableManagedRuleGroups	iam:ListRolePolicies
wafv2:ListRuleGroups	iam:GetRolePolicy
wafv2:PutFirewallManagerRuleGroups	iam:GetPolicy
wafv2:UpdateRuleGroup	iam:GetPolicyVersion
wafv2:GetManagedRuleSet	iam:ListAttachedRolePolicies
wafv2:ListManagedRuleSets	iam:ListRolePolicies
wafv2:PutManagedRuleSetVersions	iam:GetRolePolicy
wafv2:TagResourceiam:ListAttachedRolePolicies	iam:GetPolicy
wafv2:ListLoggingConfigurations	iam:GetPolicyVersion

Instead of granting the individual WAF permissions, you can assign your Authentication IAM account the AWSWAFFullAccess policy.

Limitations

General limitations

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

- Each API key is created with a new value, while the domains remain unchanged. This means that the captcha and the API key can be restored, but the users will have to update their application code with a newly created API key.
- To associate a restored Web ACL to a service, the service must be available (must exist). If not, the Web ACL can be restored but cannot be associated.
- To perform a successful restore, the following AWS WAF quotas must not be exceeded:
  - The fixed quotas on calls per account per region.
  - The service quotas for limiting the number of certain resources.

  For details, see AWS documentation on AWS WAF quotas.

Rate limitations

AWS WAF has the following fixed quotas on calls per account per Region. These quotas apply to the total calls to the service through any available means, including the console, CLI, AWS CloudFormation, the REST API, and the SDKs. These quotas cannot be changed.

Call type	Quota per account per Region
Maximum number of calls to AssociateWebACL	One request every two seconds
Maximum number of calls to DisassociateWebACL	One request every two seconds
Maximum number of calls to GetWebACLForResource	One request per second
Maximum number of calls to ListResourcesForWebACL	One request per second
Maximum number of calls to any individual Get or List action, if no other quota is defined for it	Five requests per second

Maximum number of calls to any individual Create, Put, or Update action, if no other quota is defined for it	One request per second

For more information on AWS request throttling and rate limits, see AWS documentation.

In addition to the above-mentioned limits, AWS also implements service quotas for limiting the number of certain resources. For more information on Amazon WAF quotas, see AWS documentation.

Consideration

To restore and enable a logging configuration, the Amazon Resource Name (ARN) of a log destination must be provided. The destination Amazon S3 bucket, CloudWatch, or Kinesis Data Firehose can be used as a log destination. If CloudWatch is used as the log destination, the ARN of a Log Group must be used. If the ARN is not available anymore, the log configuration can no longer be restored.

Protecting data

R-Cloud starts protecting the WAF data managed by your AWS account after you perform the following tasks:

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

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

2. Add your AWS account as a source in R-Cloud. For instructions, see *HYCU R-Cloud Help*.
3. Edit the WAF JSON policy document. For instructions, see Editing the HycuPolicy JSON file.
4. Assign a policy to the related SaaS application. For instructions, see *HYCU R-Cloud Help*.

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

Editing the HycuPolicy JSON file

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

```
{
   "Effect":"Allow",
   "Action":[
        "wafv2:AssociateWebACL",
        "wafv2:CreateWebACL",
        "wafv2:GetWebACL",
        "wafv2:GetWebACLForResource",
        "wafv2:ListLoggingConfigurations",
        "wafv2:GetLoggingConfiguration",
        "wafv2:ListResourcesForWebACL",
        "wafv2:ListWebACLs",
        "wafv2:UpdateWebACL",
        "wafv2:CheckCapacity",
        "wafv2:CreateRuleGroup",
        "wafv2:DescribeManagedRuleGroup",
        "wafv2:DescribeAllManagedProducts",
        "wafv2:DescribeManagedProductsByVendor",
        "wafv2:GetPermissionPolicy",
        "wafv2:GetRuleGroup",
        "wafv2:ListAvailableManagedRuleGroupVersions",
        "wafv2:ListAvailableManagedRuleGroups",
        "wafv2:ListRuleGroups",
```

```
"wafv2:PutFirewallManagerRuleGroups",
"wafv2:UpdateRuleGroup",
"wafv2:GetManagedRuleSet",
"wafv2:ListManagedRuleSets",
"wafv2:PutManagedRuleSetVersions",
"wafv2:UpdateManagedRuleSetVersionExpiryDate",
"wafv2:CreateIPSet",
"wafv2:GetIPSet",
"wafv2:ListIPSets",
"wafv2:UpdateIPSet",
"wafv2:CreateRegexPatternSet",
"wafv2:GetRegexPatternSet",
"wafv2:ListRegexPatternSets",
"wafv2:UpdateRegexPatternSet",
"wafv2:CreateAPIKey",
"wafv2:GetDecryptedAPIKey",
"wafv2:ListAPIKeys",
"wafv2:ListTagsForResource",
"wafv2:TagResourceiam:ListAttachedRolePolicies",
"cloudfront:ListDistributionsByWebACLId",
"cloudfront:GetDistribution",
"cloudfront:UpdateDistribution",
"iam:ListRolePolicies",
"iam:GetRolePolicy",
"iam:GetPolicy",
"iam:GetPolicyVersion",
```

```
    ],
   "Resource":"*"
}
```

Backing up data

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 your protected AWS WAF data at the following levels:

- Web ACL
  - Web ACL Rules
- IP Set
- Regex Pattern Set
- API Key
- Rule Group
- Logging Configuration

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®