HYCU for Amazon VPC

R-Cloud Module Guide

Table of Contents

Copyright notice

About the module

With the R-Cloud (formerly HYCU Protégé) module for Amazon VPC, you can back up your SaaS application data securely and efficiently. The module enables you to protect the content of the virtual private clouds (VPCs) that are managed by your AWS account.

Prerequisites

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

- `ec2:AcceptVpcPeeringConnection`
- `ec2:AllocateAddress`
- `ec2:AssignIpv6Addresses`
- `ec2:AssignPrivateIpAddresses`
- `ec2:AssociateAddress`
- `ec2:AssociateDhcpOptions`
- `ec2:AssociateRouteTable`
- `ec2:AttachInternetGateway`
- `ec2:AuthorizeSecurityGroupEgress`
- `ec2:AuthorizeSecurityGroupIngress`
- `ec2:CreateDefaultSubnet`
- `ec2:CreateDefaultVpc`
- `ec2:CreateDhcpOption`
- `ec2:CreateEgressOnlyInternetGateway`
- `ec2:CreateInternetGateway`
- `ec2:CreateNatGateway`
- `ec2:CreateNetworkAcl`
- `ec2:CreateNetworkAclEntry`
- `ec2:CreateNetworkInterface`

- ec2:CreateRoute
- ec2:CreateRouteTable
- ec2:CreateSecurityGroup
- ec2:CreateSubnet
- ec2:CreateVpc
- ec2:CreateVpcPeeringConnection
- ec2:DescribeAddresses
- ec2:DescribeDhcpOptions
- ec2:DescribeEgressOnlyInternetGateways
- ec2:DescribeInternetGateways
- ec2:DescribeIpamPools
- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeNetworkInterfaces
- ec2:DescribeRegions
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroupReferences
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- ec2:DescribeVpcAttribute
- ec2:DescribeVpcPeeringConnections
- ec2:DescribeVpcs
- ec2:GetIpamPoolCidrs
- ec2:ModifyNetworkInterfaceAttribute
- ec2:ModifyVpcAttribute
- ec2:ReplaceNetworkAssociation
- ec2:RevokeSecurityGroupEgress
- iam:GetPolicy
- iam:GetPolicyVersion

- `iam:GetRolePolicy`
- `iam:ListAttachedRolePolicies`
- `iam:ListRolePolicies`

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

- AmazonVPCFullAccess

Limitations

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

- Protecting the Bring Your Own IP (BYOIP) is not supported.
- Only the following types of the elastic network interface can be protected: Interface, EFA, and Trunk.
- An Elastic IP address cannot be restored if the address is not allocated to the AWS account anymore or if the address is associated with another resource.
- Default VPCs and subnets will be restored as non-default.
- A default subnet cannot be restored to a non-default VPC.
- A default subnet cannot be restored if the given Availability Zone already has the default subnet defined.
- A subnet cannot be restored if its CIDR overlaps with the CIDR of another subnet.
- The resources with the following states cannot be restored: deleted, deleting, failed, failing, and expired.
- When restoring a resource, the AWS quotas must not be exceeded.
- The VPC peering connection cannot be restored in the following cases:
  - If two of the VPCs already have the peering connection defined.
  - If the connection was originally requested from the VPC that belongs to a different AWS account.

Considerations

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

- For the resource types that do not support equally named objects, the module appends the following string to the name of the restored resource: `<objectname>_timestamp`.
- Amazon throttles the API requests for each AWS account on the per-region basis. Throttling ensures that the calls to the Amazon API do not exceed the maximum allowed API request limits. For more information, see AWS documentation about the AWS request throttling and rate limits.
- AWS implements service quotas for limiting the number of certain resources. For more information, see documentation about the Amazon VPC quotas.

Protecting data

R-Cloud starts protecting the content of the Amazon VPCs after you perform the following tasks:

1. Add the module as a source to 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 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.
3. Edit the AWS 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*.

Note The R-Cloud module for Amazon VPC backs up data by using a staging target. Select the preferred staging target when adding the module as a source to R-Cloud.

Editing the HycuPolicy JSON 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 file:

```
{
   "Effect":"Allow",
   "Action":[
            "ec2:DescribeRegions",
            "ec2:AssociateDhcpOptions",
            "ec2:CreateDhcpOption",
            "ec2:DescribeDhcpOptions",
            "ec2:CreateInternetGateway",
            "ec2:CreateEgressOnlyInternetGateway",
            "ec2:DescribeInternetGateways",
            "ec2:DescribeEgressOnlyInternetGateways",
            "ec2:AttachInternetGateway",
            "ec2:CreateNatGateway",
            "ec2:DescribeNatGateways",
            "ec2:CreateNetworkAcl",
            "ec2:CreateNetworkAclEntry",
            "ec2:DescribeNetworkAcls",
            "ec2:ReplaceNetworkAssociation",
            "ec2:CreateRoute",
            "ec2:CreateRouteTable",
            "ec2:DescribeRouteTables",
            "ec2:AssociateRouteTable",
            "ec2:DescribeSubnets",
            "ec2:CreateSubnet",
            "ec2:CreateDefaultSubnet",
            "ec2:GetIpamPoolCidrs",
            "ec2:DescribeIpamPools",
            "ec2:DescribeVpcs",
            "ec2:CreateVpc",
            "ec2:CreateDefaultVpc",
            "ec2:ModifyVpcAttribute",
            "ec2:DescribeVpcAttribute",
            "ec2:DescribeVpcPeeringConnections",
            "ec2:CreateVpcPeeringConnection",
```

```
            "ec2:AcceptVpcPeeringConnection",
            "ec2:CreateSecurityGroup",
            "ec2:DescribeSecurityGroups",
            "ec2:DescribeSecurityGroupReferences",
            "ec2:AuthorizeSecurityGroupEgress",
            "ec2:AuthorizeSecurityGroupIngress",
            "ec2:RevokeSecurityGroupEgress",
            "ec2:DescribeNetworkInterfaces",
            "ec2:CreateNetworkInterface",
            "ec2:ModifyNetworkInterfaceAttribute",
            "ec2:AllocateAddress",
            "ec2:AssociateAddress",
            "ec2:DescribeAddresses",
            "ec2:AssignPrivateIpAddresses",
            "ec2:AssignIpv6Addresses",
            "iam:ListAttachedRolePolicies",
            "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 Amazon VPC data at the following levels:

- DHCP Options
- Elastic IP
- VPC
- VPC Peering Connection

- Internet Gateway
- Egress Only Internet Gateway
- Security Group
- Network ACL
- Subnet
- NAT Gateway
- Elastic Network Interface

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®