HYCU for Amazon Route 53

R-Cloud Module Guide

Table of Contents

Copyright notice

About the module

With the R-Cloud (formerly HYCU Protégé) module for Amazon Route 53, you can back up the current values of your created Amazon Route 53 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:

- `iam:ListAttachedRolePolicies`
- `iam:ListRolePolicies`
- `iam:GetRolePolicy`
- `iam:GetPolicy`
- `iam:GetPolicyVersion`
- `ec2:DescribeRegions`
- `ec2:DescribeVpcs`
- `route53:ListHostedZones`
- `route53:ListResourceRecordSets`
- `route53:ListHealthChecks`
- `route53:ListCidrCollections`
- `route53:ListCidrLocations`
- `route53:ListCidrBlocks`
- `route53:ListTrafficPolicies`
- `route53:ListTrafficPolicyVersions`
- `route53:ListTrafficPolicyInstances`
- `route53:ListQueryLoggingConfigs`
- `route53:GetHostedZone`
- `route53:GetDNSSEC`
- `route53:GetQueryLoggingConfig`

- `route53:GetHealthCheck`
- `route53:GetTrafficPolicy`
- `route53:GetTrafficPolicyInstance`
- `route53:CreateHostedZone`
- `route53:AssociateVPCWithHostedZone`
- `route53:ChangeResourceRecordSets`
- `route53:CreateKeySigningKey`
- `route53:EnableHostedZoneDNSSEC`
- `route53:CreateQueryLoggingConfig`
- `route53:CreateHealthCheck`
- `route53:UpdateHealthCheck`
- `route53:CreateTrafficPolicy`
- `route53:CreateTrafficPolicyVersion`
- `route53:CreateTrafficPolicyInstance`
- `route53:CreateCidrCollection`
- `route53:ChangeCidrCollection`
- `route53resolver:ListResolverEndpoints`
- `route53resolver:ListResolverRules`
- `route53resolver:ListResolverRuleAssociations`
- `route53resolver:ListResolverQueryLogConfigs`
- `route53resolver:ListResolverQueryLogConfigAssociations`
- `route53resolver:ListFirewallRules`
- `route53resolver:ListFirewallDomainLists`
- `route53resolver:ListFirewallRuleGroups`
- `route53resolver:ListFirewallRuleGroupAssociations`
- `route53resolver:GetResolverEndpoint`
- `route53resolver:GetResolverRule`
- `route53resolver:GetResolverRulePolicy`
- `route53resolver:GetResolverRuleAssociation`

- `route53resolver:GetFirewallRuleGroup`
- `route53resolver:GetFirewallDomainList`
- `route53resolver:GetFirewallRuleGroupAssociation`
- `route53resolver:GetResolverQueryLogConfig`
- `route53resolver:GetResolverQueryLogConfigPolicy`
- `route53resolver:GetResolverQueryLogConfigAssociation`
- `route53resolver:CreateResolverEndpoint`
- `route53resolver:CreateResolverRule`
- `route53resolver:AssociateResolverRule`
- `route53resolver:PutResolverRulePolicy`
- `route53resolver:CreateFirewallRuleGroup`
- `route53resolver:AssociateFirewallRuleGroup`
- `route53resolver:CreateFirewallRule`
- `route53resolver:CreateFirewallDomainList`
- `route53resolver:UpdateFirewallDomains`
- `route53resolver:CreateResolverQueryLogConfig`
- `route53resolver:AssociateResolverQueryLogConfig`
- `route53resolver:PutResolverQueryLogConfigPolicy`
- `arc-zonal-shift:ListManagedResources`
- `arc-zonal-shift:GetManagedResource`
- `arc-zonal-shift:CreatePracticeRunConfiguration`
- `arc-zonal-shift:UpdateZonalAutoshiftConfiguration`
- `route53-recovery-control-config:ListClusters`
- `route53-recovery-control-config:ListControlPanels`
- `route53-recovery-control-config:ListRoutingControls`
- `route53-recovery-control-config:ListSafetyRules`
- `route53-recovery-control-config:ListAssociatedRoute53HealthChecks`
- `route53-recovery-control-config:ListTagsForResource`
- `route53-recovery-control-config:DescribeCluster`

- `route53-recovery-control-config:DescribeControlPanel`
- `route53-recovery-control-config:DescribeRoutingControl`
- `route53-recovery-control-config:DescribeSafetyRule`
- `route53-recovery-control-config:CreateCluster`
- `route53-recovery-control-config:CreateControlPanel`
- `route53-recovery-control-config:CreateRoutingControl`
- `route53-recovery-control-config:CreateSafetyRule`
- `route53-recovery-readiness:ListCells`
- `route53-recovery-readiness:ListRecoveryGroups`
- `route53-recovery-readiness:ListReadinessChecks`
- `route53-recovery-readiness:ListResourceSets`
- `route53-recovery-readiness:ListTagsForResources`
- `route53-recovery-readiness:GetCell`
- `route53-recovery-readiness:GetRecoveryGroup`
- `route53-recovery-readiness:GetReadinessCheck`
- `route53-recovery-readiness:GetResourceSet`
- `route53-recovery-readiness:CreateCell`
- `route53-recovery-readiness:CreateRecoveryGroup`
- `route53-recovery-readiness:CreateReadinessCheck`
- `route53-recovery-readiness:CreateResourceSet`
- `route53-recovery-readiness:UpdateCell`
- `route53-recovery-readiness:UpdateRecoveryGroup`
- `route53-recovery-readiness:UpdateReadinessCheck`
- `route53profiles:ListProfiles`
- `route53profiles:ListProfileAssociations`
- `route53profiles:ListProfileResourceAssociations`
- `route53profiles:ListTagsForResource`
- `route53profiles:GetProfile`
- `route53profiles:GetProfileAssociation`

- `route53profiles:GetProfileResourceAssociation`
- `route53profiles:CreateProfile`
- `route53profiles:AssociateProfile`
- `route53profiles:AssociateResourceToProfile`

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

- AmazonRoute53FullAccess
- AmazonRoute53ResolverFullAccess
- AmazonRoute53RecoveryControlConfigFullAccess
- AmazonRoute53RecoveryReadinessFullAccess
- AmazonRoute53ProfilesFullAccess
- ElasticLoadBalancingFullAccess (or any other policy that includes the arc-zonal-shift permissions)

Limitations

General limitations

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

- The following resources are not protected due to the API limitations:
  - Domain management data (registration and transferring of the domains)
  - Reusable delegation sets
  - Resolver outpost resources
  - Profile configuration data
  - Application Recovery Controller (ARC) manual zonal shifts
- Protecting the shared configuration data for various resources is not supported.
- The restore tags will not be created after the maximum number of tags defined for the related resource is reached.
- To run a successful restore of the related resources, the VPC associations related to the profiles, the resolver rules, the resolver query logging config, and the DNS firewall rule groups must be removed.

- The query logging configuration for the hosted zone and the DNSSEC data for the hosted zone cannot be restored if the related resources already exist.
- To restore a DNSSEC, the KMS customer-managed key related to the DNSSEC key-signing keys (KSK) records must be available.
- A hosted zone created by the Cloud Map service cannot be restored if it already exists because the resource is managed by the Cloud Map service. If the hosted zone created by the Cloud Map service is deleted, it can be restored by the Route 53 service and will be marked as managed by Route 53.
- To restore the query logging configuration, the CloudWatch log group related to the query logging configuration must be available.
- The CloudWatch alarms created for the health checks cannot be protected.
- The CIDR location restore will fail if there is another CIDR location with overlapping blocks.
- Only the latest traffic policy version is protected.
- The failed traffic policy records are not restored to avoid any conflicting operations.
- The traffic policy records that already exist cannot be restored.
- The corresponding traffic policy version must be available to restore the related traffic policy record.
- After the granular restore of a health check resource, the related resources using the restored health check must be updated with the newly restored health check ID.

Route 53 Resolver limitations

When adding the module to R-Cloud and protecting the related SaaS application, the following Route 53 Resolver limitations apply:

- To restore the Route 53 Resolver inbound and outbound endpoints, the backed-up IP address must be available. In this case, either the original endpoints must be deleted, or the IP addresses must be changed.
- The empty domain lists cannot be restored. At least one domain is required for a restore.

Route 53 ARC limitations

When adding the module to R-Cloud and protecting the related SaaS application, the following Route 53 ARC limitations apply:

- The endpoints of an ARC cluster cannot be protected.
- The ARC resource set granular restore will not recreate the missing ARC readiness check resources.

API call rate limitations

The Amazon Route 53 API call rate limitations are the following:

- *For the Route 53 API requests:* five requests per second per AWS account
- *For the Route 53 Resolver API requests:* five requests per second per AWS account per region
- *For the Route 53 ARC API requests:* three mutating requests per second to a cluster endpoint

For more information about the Amazon Route 53 service quotas, see AWS documentation.

Considerations

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

- The original hosted zone NS and SOA records are not restored by default. You can enable the restore of the original NS and SOA records to an existing hosted zone in R-Cloud.
- To restore a resource, the AWS quotas must not be exceeded. For more information about the Amazon Route 53 service quotas, see AWS documentation.
- The restored state of the ARC routing controls is always set to off.
- The VPC resources associated with any other Route 53 resource (private hosted zones, resolver endpoints, resolver rules, or DNS firewall rule groups) must be available for a successful restore of the corresponding resource.

- The restore of an existing DNSSEC key-signing key (KSK) will be completed with the `KeySigningKeyAlreadyExists` error. If a KSK must be returned to the backed-up state, the related KSK must be deleted before restoring.
- Restoring some of the existing resources may finish with the “The source already exists” errors. To restore the affected resources, delete them before restoring.

Protecting data

R-Cloud starts protecting the Amazon Route 53 service resources after you complete the following steps:

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 to 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:

```
{
   "Effect":"Allow",
   "Action":[
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "ec2:DescribeRegions",
        "ec2:DescribeVpcs"
        "route53:ListHostedZones",
        "route53:ListResourceRecordSets",
        "route53:ListHealthChecks",
        "route53:ListCidrCollections",
        "route53:ListCidrLocations",
        "route53:ListCidrBlocks",
        "route53:ListTrafficPolicies",
        "route53:ListTrafficPolicyVersions",
        "route53:ListTrafficPolicyInstances",
        "route53:ListQueryLoggingConfigs",
        "route53:GetHostedZone",
        "route53:GetDNSSEC",
        "route53:GetQueryLoggingConfig",
        "route53:GetHealthCheck",
        "route53:GetTrafficPolicy"
        "route53:GetTrafficPolicyInstance",
        "route53:CreateHostedZone",
        "route53:AssociateVPCWithHostedZone",
        "route53:ChangeResourceRecordSets",
        "route53:CreateKeySigningKey",
        "route53:EnableHostedZoneDNSSEC",
        "route53:CreateQueryLoggingConfig",
        "route53:CreateHealthCheck",
        "route53:UpdateHealthCheck",
        "route53:CreateTrafficPolicy",
        "route53:CreateTrafficPolicyVersion",
        "route53:CreateTrafficPolicyInstance",
        "route53:CreateCidrCollection",
        "route53:ChangeCidrCollection",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverRules",
        "route53resolver:ListResolverRuleAssociations",
        "route53resolver:ListResolverQueryLogConfigs",
        "route53resolver:ListResolverQueryLogConfigAssociations",
        "route53resolver:ListFirewallRules",
        "route53resolver:ListFirewallDomainLists",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:GetResolverEndpoint",
        "route53resolver:GetResolverRule",
        "route53resolver:GetResolverRulePolicy",
        "route53resolver:GetResolverRuleAssociation",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetFirewallDomainList",
        "route53resolver:GetFirewallRuleGroupAssociation",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:GetResolverQueryLogConfigPolicy",
        "route53resolver:GetResolverQueryLogConfigAssociation",
        "route53resolver:CreateResolverEndpoint",
        "route53resolver:CreateResolverRule",
        "route53resolver:AssociateResolverRule",
        "route53resolver:PutResolverRulePolicy",
        "route53resolver:CreateFirewallRuleGroup",
        "route53resolver:AssociateFirewallRuleGroup",
        "route53resolver:CreateFirewallRule",
        "route53resolver:CreateFirewallDomainList",
        "route53resolver:UpdateFirewallDomains",
        "route53resolver:CreateResolverQueryLogConfig",
        "route53resolver:AssociateResolverQueryLogConfig",
        "route53resolver:PutResolverQueryLogConfigPolicy",
        "arc-zonal-shift:ListManagedResources",
        "arc-zonal-shift:GetManagedResource",
        "arc-zonal-shift:CreatePracticeRunConfiguration",
        "arc-zonal-shift:UpdateZonalAutoshiftConfiguration",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-control-config:ListSafetyRules",
        "route53-recovery-control-config:ListAssociatedRoute53HealthChecks",
        "route53-recovery-control-config:ListTagsForResource"
        "route53-recovery-control-config:DescribeCluster",
        "route53-recovery-control-config:DescribeControlPanel",
        "route53-recovery-control-config:DescribeRoutingControl",
        "route53-recovery-control-config:DescribeSafetyRule",
        "route53-recovery-control-config:CreateCluster",
        "route53-recovery-control-config:CreateControlPanel",
        "route53-recovery-control-config:CreateRoutingControl",
        "route53-recovery-control-config:CreateSafetyRule",
        "route53-recovery-readiness:ListCells",
        "route53-recovery-readiness:ListRecoveryGroups",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53-recovery-readiness:ListResourceSets",
        "route53-recovery-readiness:ListTagsForResources",
        "route53-recovery-readiness:GetCell",
        "route53-recovery-readiness:GetRecoveryGroup",
        "route53-recovery-readiness:GetReadinessCheck",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:CreateCell",
        "route53-recovery-readiness:CreateRecoveryGroup",
        "route53-recovery-readiness:CreateReadinessCheck",
        "route53-recovery-readiness:CreateResourceSet",
        "route53-recovery-readiness:UpdateCell",
        "route53-recovery-readiness:UpdateRecoveryGroup",
        "route53-recovery-readiness:UpdateReadinessCheck"
        "route53profiles:ListProfiles",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations"
        "route53profiles:ListTagsForResource",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:CreateProfile",
        "route53profiles:AssociateProfile",
        "route53profiles:AssociateResourceToProfile"
   ],
   "Resource":"*"
}
```

Backing up data

After completing the steps in section Protecting data, the following main groups of resources can be backed up:

- Route 53 resources:
    - Hosted zones with their records
    - CIDR locations
    - Health checks
    - Traffic policies with their records

    - Profile resources with their associations

- Route 53 Resolver resources:
    - Outbound and inbound endpoints with their rules
    - VPC associations
    - Logging configurations with their VPC associations
    - DNS firewall resources with their domain lists, rules, and VPC associations

- Route 53 Application Recovery resources:
    - Routing controls resources
    - Readiness checks resources
    - Zonal autoshift resources

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 Route 53 data at the following levels:

- Route 53 resources:
    - Hosted zone
        - Record
        - Query logging config
        - DNSSEC
    - CIDR collections
        - CIDR location
    - Health check
    - Traffic policy
        - Traffic policy record
    - Profile
        - Profile association
        - Profile resource association

- Route 53 Resolver resources:
    - Resolver inbound endpoint
    - Resolver outbound endpoint
        - Resolver rules
        - Resolver rule VPC association

  - Resolver query logging config
    - Resolver query logging config VPC association
  - DNS firewall domain list
  - DNS firewall rule groups
    - DNS firewall rule
    - DNS firewall rules group VPC association

- Route 53 Application Recovery Controller resources:
  - ARC zonal autoshift
  - ARC cluster
    - ARC control panel
      - ARC safety rule
      - ARC routing control
        - ARC health check
  - ARC readiness resources
    - ARC recovery group
    - ARC cell
    - ARC resource set
    - ARC readiness check

> **Important** Granular restore is not available for the ARC recovery group and the ARC cell.

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®