Alibaba Cloud CloudConfig

Quick Start

Issue: 20200528

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.
3. The content of this document may be changed due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.
4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.
6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Document conventions

Style	Description	Example
	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 **Danger:** Resetting will result in the loss of user configuration data.
	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 **Warning:** Restarting will cause business interruption. About 10 minutes are required to restart an instance.
	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	 **Notice:** If the weight is set to 0, the server no longer receives new requests.
	A note indicates supplemental instructions, best practices, tips, and other content.	 **Note:** You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings** > **Network** > **Set network type**.
Bold	Bold formatting is used for buttons, menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands.	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`

Style	Description	Example
{} or {a|b}	This format is used for a required value, where only one item can be selected.	switch {active|stand}

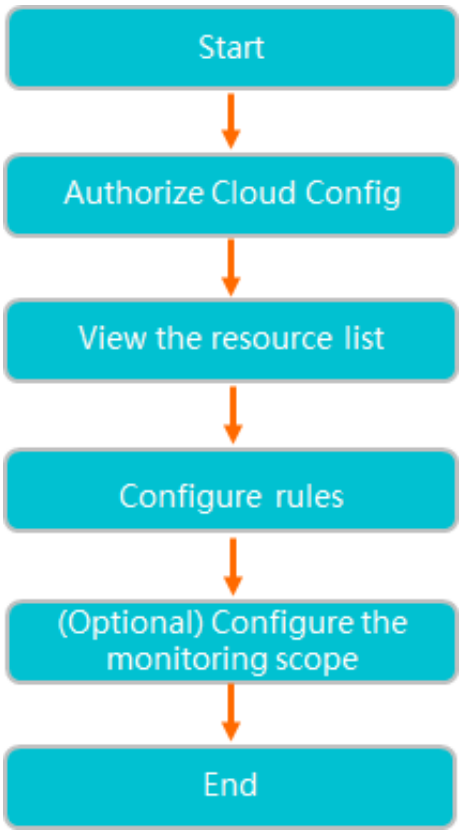
Contents

1 Overview

This topic helps you get started with the procedure for using Cloud Config, operation scenarios, and the relationship between features.

Procedure in Quick Start

By following the steps in the procedure, you can quickly authorize Cloud Config to monitor and evaluate resources.



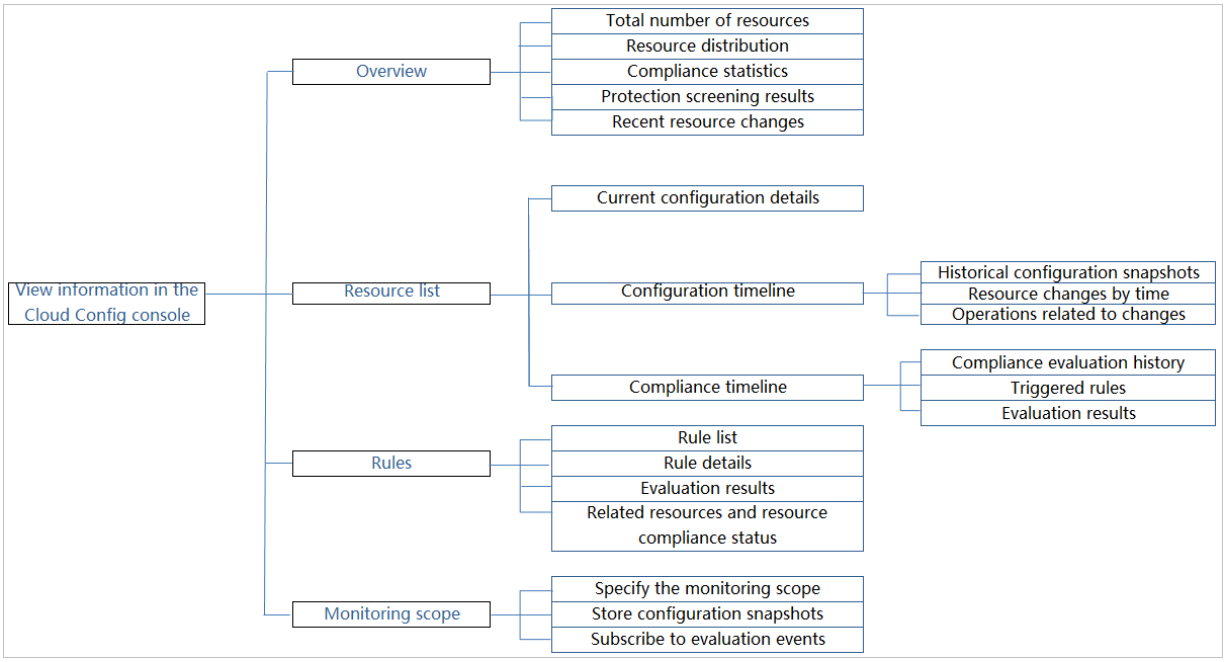
The following table describes the steps to get started with Cloud Config.

No.	Step	Scenario
1	Authorize Cloud Config to access your resources	Before you use Cloud Config, authorize Cloud Config to read the data of your resources.
2	View the resource list	After you authorize Cloud Config, Cloud Config automatically scans resources in each region under your account and generates an aggregated list of resources in multiple regions. You can view and manage the resources under your account.

No.	Step	Scenario
3	Create rules	Cloud Config checks the validity of resources based on rules. You can configure rules to evaluate resources as needed.
4	(Optional) Set the monitoring scope	After you activate Cloud Config, the monitoring scope of the service includes all supported resource types by default. During initialization, Cloud Config scans all resources under your account. If you have other monitoring schemes, select resource types to be monitored as needed.

Relationship between features

The core elements of Cloud Config include resources, rules, configuration information, configuration history, configuration changes, compliance evaluation results, rule information, and compliance evaluation history. The following figure shows the relationship between features.



2 Authorize Cloud Config to access your resources

You must authorize Cloud Config to access your resources before you can use it to track configuration changes of your resources and evaluate configuration compliance.

Prerequisites

Make sure that you have completed account registration and real-name verification with Alibaba Cloud.

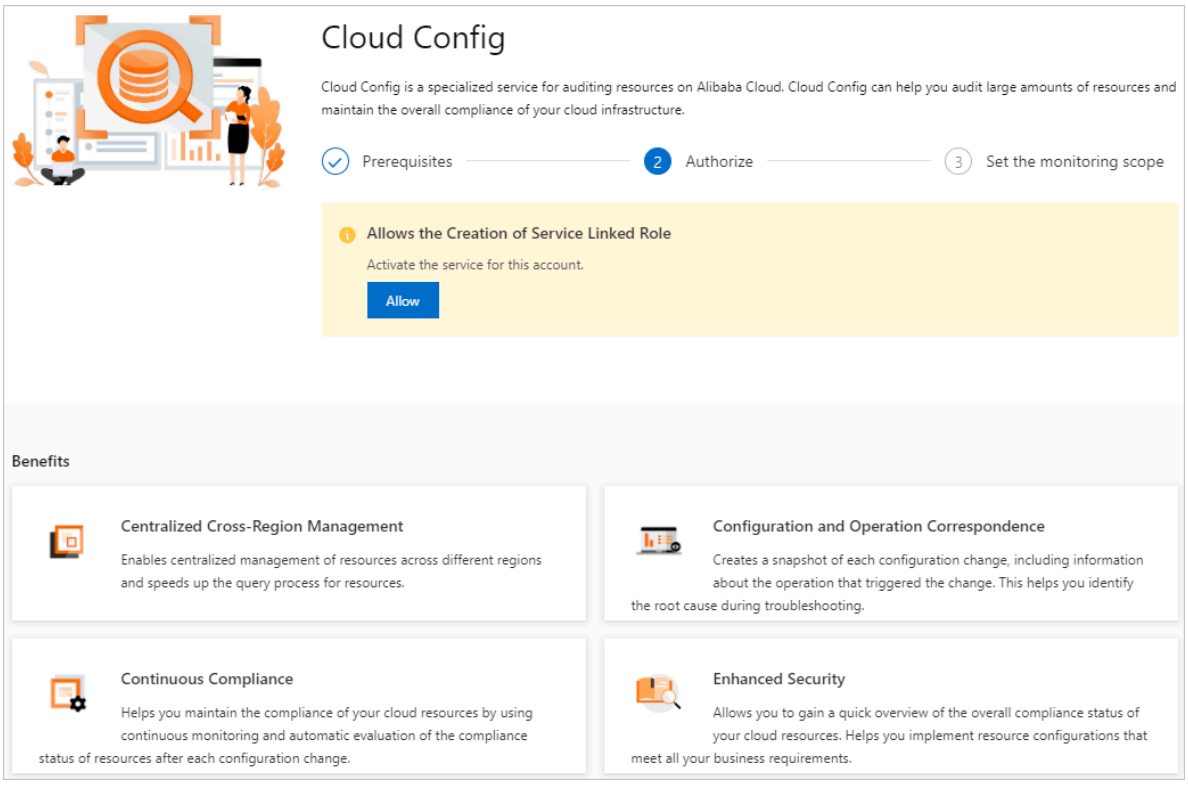
Context

When you authorize Cloud Config to access data in other Alibaba Cloud services, the running of these services is not affected. Only the read-only permissions on resource configurations are granted to Cloud Config.

Procedure

1. Log on to the Cloud Config console.

2. In the Authorize step, click **Allow** to create the service linked role that authorizes Cloud Config to access your resources.



Note:

Cloud Config needs 2 to 10 minutes to scan your resources and generate a resource list.

3 View the resource list

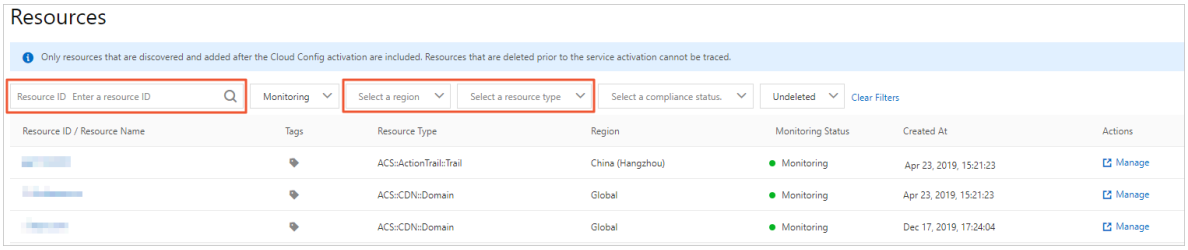
After you authorize Cloud Config, Cloud Config automatically scans resources in each region under your account and generates an aggregated list of resources in multiple regions.

Prerequisites

Make sure that you have authorized Cloud Config. For more information, see Authorize Cloud Config to access your resources.

Procedure

1. Log on to the Cloud Config console.
2. In the left-side navigation pane, click **Resources**.
3. You can set filters, such as region and resource type, or enter a resource ID in the search box to search for resources.



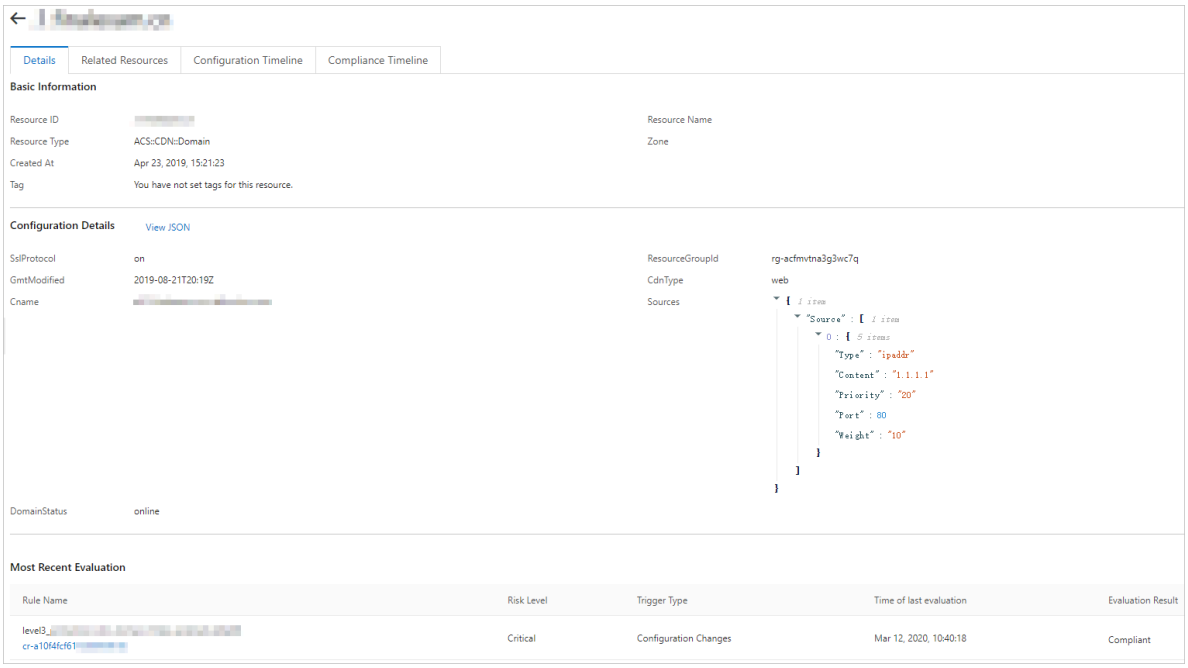
4. Click the resource ID in the **Resource ID / Resource Name** column.

   On the **Details** page that appears, you can view the following information:

   - On the **Details** tab that appears, view the basic information, core configurations, and latest compliance evaluation result of the resource.
   - Click the **Related Resources** tab. On the Related Resources tab that appears, view the resources related to the selected resource.
   - Click the **Configuration Timeline** tab. On the Configuration Timeline tab that appears, view the configuration timeline of the selected resource.
   - Click the **Compliance Timeline** tab. On the Compliance Timeline tab that appears, view the compliance history of the selected resource.

Note:

Cloud Config is increasing the number of supported resource types. The current resource list displays the resources of the types supported by Cloud Config.



4 Create rules

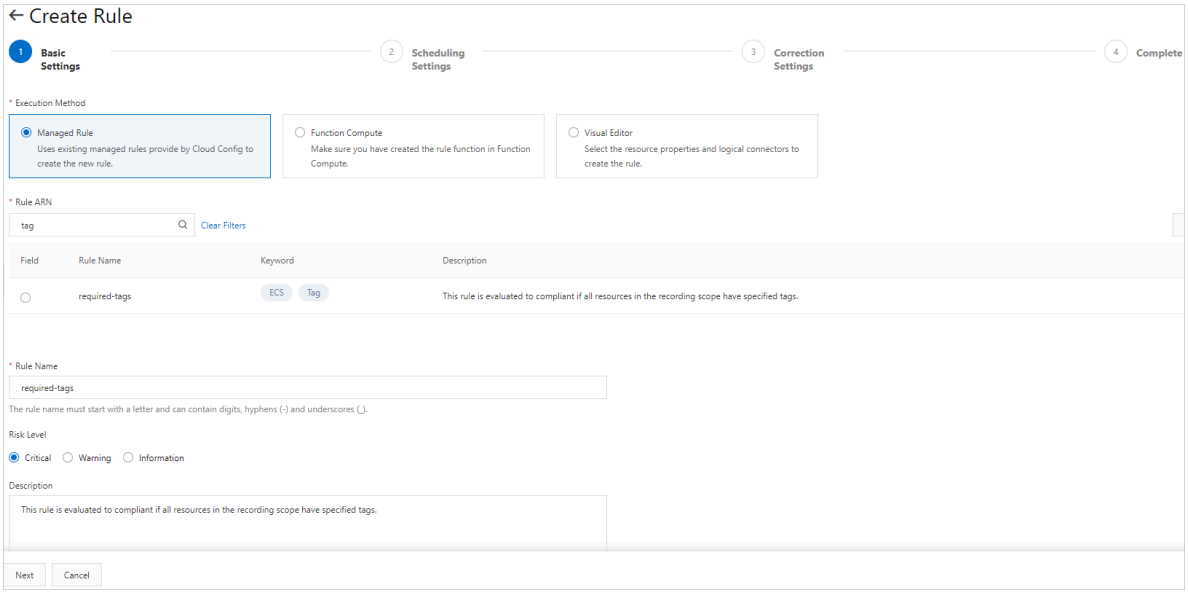
Cloud Config checks the validity of resources based on rules. You can create rules to evaluate resources as needed.

Context

Before creating a rule, you can learn about the rule definition and principles. For more information, see #unique_8.

Procedure

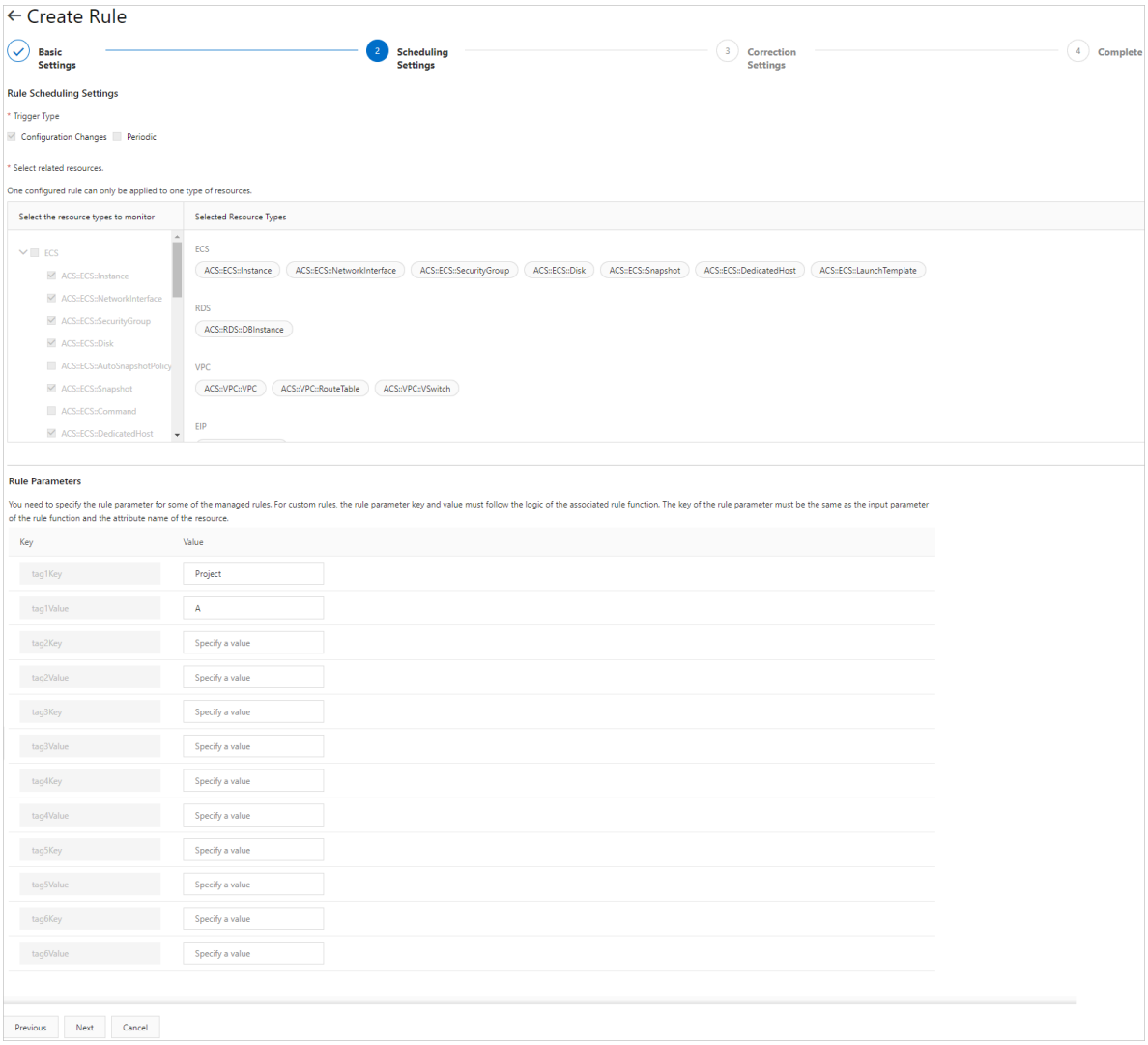
1. Log on to the Cloud Config console.
2. In the left-side navigation pane, click **Rules**.
3. On the Rules page, click **Create Rule**.
4. In the **Basic Settings** step of the **Create Rule** wizard, set **Execution Method**, set relevant parameters, and then click **Next**.



- If you set Execution Method to **Managed Rule**, you can select one from more than 40 managed rules provided by Cloud Config and specify the rule name.
- If you set Execution Method to **Function Compute**, specify the rule name and select the Alibaba Cloud Resource Name (ARN) of a function.

  You must create a rule function in Function Compute before using the function to create a rule. For more information about how to create a function, see Create a function.
- If you set Execution Method to **Visual Editor**, you only need to specify the rule name.

5. In the **Scheduling Settings** step of the **Create Rule** wizard, set relevant parameters and click **Next**.

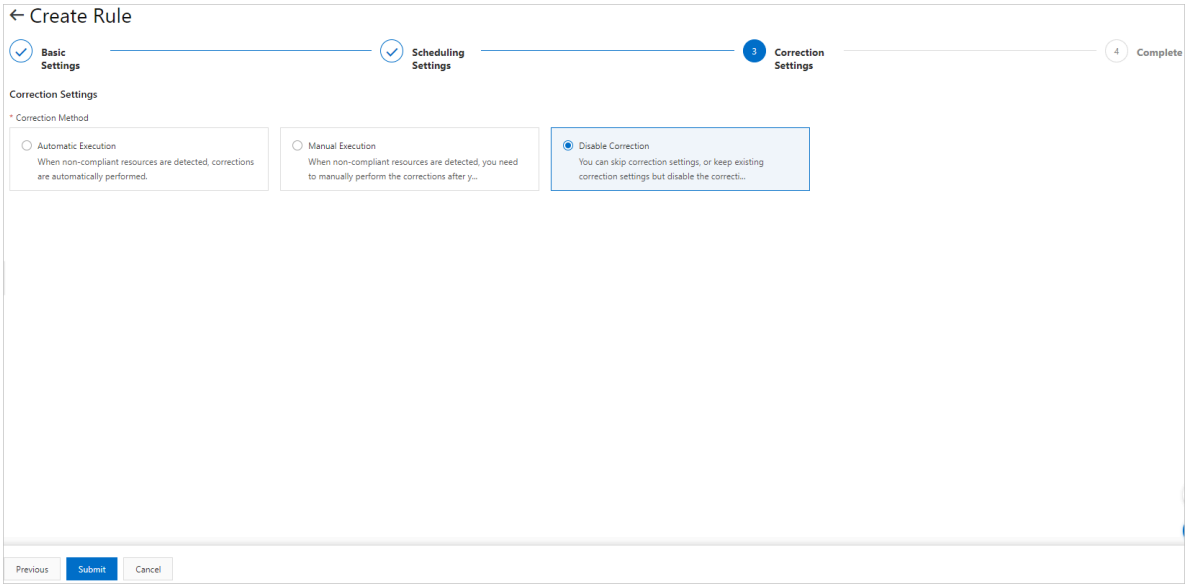


- If you set Execution Method to **Managed Rule**, you can only specify the values for the input parameters of the rule.
- If you set Execution Method to **Function Compute** or **Visual Editor**, specify the trigger type, select the resource types to be monitored, set input parameters of the rule, and then specify the values for the input parameters.

  Set the key and value for an input parameter by following the logic of the associated rule function. Note that the key must be the same as the name of the input parameter of the rule function and the attribute name of the resource.

6. In the **Correction Settings** step of the **Create Rule** wizard, set Correction Method to **Disable Correction** and click **Submit**.

   You can bind a correction template to the current rule. For more information, see #unique_9 or #unique_10.



7. View the rule creation result.

   In the **Complete** step of the **Create Rule** wizard, you can view the rule creation result.

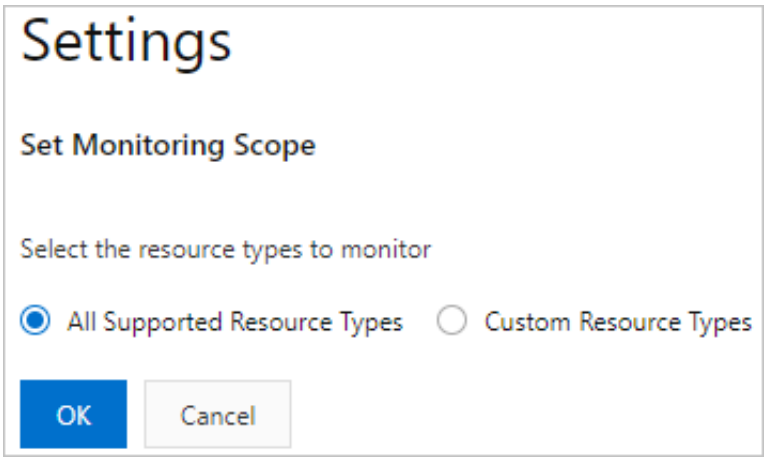
   - Click **View Details**. On the page that appears, you can view the basic information of the current rule, correction details, trigger of the rule, and compliance results of resources evaluated by the rule.
   - Click **Return to Rule List**. On the **Rules** page that appears, you can view the rule, the status of which is **Active**.

5 Set the monitoring scope

After you activate Cloud Config, the monitoring scope of the service includes all resource types by default. During initialization, Cloud Config scans all resources in your account. If you have other monitoring schemes, follow the steps described in this topic to set the resource types to be monitored.

Procedure

1. Log on to the Cloud Config console.
2. In the left-side navigation pane, click **Settings**.
3. In the **Set Monitoring Scope** section, click **Edit**.
4. Select the resource types to be monitored.



   - If you select **All Supported Resource Types** and more services are connected to Cloud Config, new resource types supported by Cloud Config are automatically added to the monitoring scope by default.
   - If you select **Custom Resource Types**, you can select resource types as needed.
5. Click **OK**.

6 Manage the service linked role

The service linked role for Cloud Config, AliyunServiceRoleForConfig, is the Resource Access Management (RAM) role that authorizes Cloud Config to access other Alibaba Cloud services in certain scenarios.

Note:
For more information, see #unique_12.

Scenarios

The AliyunServiceRoleForConfig role is applicable to the following scenarios:

- When Cloud Config calls the APIs of other Alibaba Cloud services to query the resource configurations of the current account, Cloud Config uses the AliyunServiceRoleForConfig role to obtain the permission to read the configurations.
- If you specify an Object Storage Service (OSS) bucket to store snapshots of resource configuration changes, Cloud Config uses the AliyunServiceRoleForConfig role to obtain the permission to write snapshots to the OSS bucket.

Create the AliyunServiceRoleForConfig role

You can create the AliyunServiceRoleForConfig role in the Cloud Config console.

- Cloud Config for individuals

  You must allow Cloud Config to create the AliyunServiceRoleForConfig role before you can use Cloud Config to manage resource configurations of your Alibaba Cloud account. For more information, see Authorize Cloud Config to access your resources.
- Cloud Config for Enterprise

  When you use the master account to upgrade Cloud Config to Cloud Config for Enterprise , Cloud Config automatically creates the AliyunServiceRoleForConfig role for all member accounts.

  For more information, see #unique_13.

Delete the AliyunServiceRoleForConfig role

Currently, Cloud Config does not support deleting the AliyunServiceRoleForConfig role. If you want to delete the role, submit a ticket.

Role description

The details of the AliyunServiceRoleForConfig role are as follows:

- Name: AliyunServiceRoleForConfig
- Permission policy attached to the role: AliyunServiceRolePolicyForConfig
- This permission policy grants Cloud Config the permissions to read the resource configurations of the current account and to write snapshots of resource configuration changes to an OSS bucket.

```
"Action": [
            "ecs:Describe*",
            "ess:Describe*",
            "vpc:Describe*",
            "rds:DescribeDBInstance*",
            "rds:DescribeRegions",
            "rds:DescribeBackup*",
            "slb:Describe*",
            "*:DescribeTags",
            "oss:GetService",
            "oss:GetBucket*",
            "oss:ListBuckets",
            "oss:ListObjects",
            "ram:List*",
            "ram:Get*",
            "actiontrail:LookupEvents",
            "actiontrail:Describe*",
            "actiontrail:Get*",
            "ots:BatchGet*",
            "ots:Describe*",
            "ots:Get*",
            "ots:List*",
            "ocs:Describe*",
            "cms:Get*",
            "cms:List*",
            "cms:Query*",
            "cms:BatchQuery*",
            "cms:Describe*",
            "kvstore:Describe*",
            "fc:Get*",
            "fc:List*",
            "kms:DescribeKey",
            "kms:DescribeRegions",
            "kms:ListAliases",
            "kms:ListAliasesByKeyId",
            "kms:ListKeys",
            "cdn:Describe*",
            "yundun*:Get*",
            "yundun*:Describe*",
            "yundun*:Query*",
            "yundun*:List*",
            "polardb:Describe*",
            "dds:Describe*",
            "cen:Describe*",
            "mns:ListTopic",
            "mns:GetTopicAttributes",
            "resourcemanager:GetAccount",
            "resourcemanager:ListAccountsForParent",
            "resourcemanager:ListAccounts",
```

```
            "resourcemanager:GetFolder",
            "resourcemanager:ListFoldersForParent",
            "resourcemanager:ListAncestors",
            "resourcemanager:GetResourceDirectory",
            "composer:GetFlow",
            "composer:DescribeFlow"
        ],
        "Resource": "*",
        "Effect": "Allow"
    },
    {
        "Action": [
            "oss:PutObject",
            "fc:InvokeFunction",
            "mns:PublishMessage",
            "composer:GroupInvokeFlow"
        ],
        "Resource": "*",
        "Effect": "Allow"
    }
```