ALIBABA CLOUD

Alibaba Cloud

CloudConfig

Resource Compliance Evaluation

Document Version: 20210830

Alibaba Cloud

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 because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should 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 this document based on the "status quo", "being defective", and "existing functions" of its products and services. 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 take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, 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 directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
⚠ Danger	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.
🔔 Warning	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.
📢 Notice	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.
ⓘ Note	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]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.Manage rules

1.1. Create a rule based on a managed rule

A rule is a piece of logical judgment code that is stored in a rule function of Function Compute. You can create a rule based on a managed rule that is provided by Cloud Config to audit associated resources.

Context

Before you create a rule, you must familiarize yourself with the definition of rules and how rules work. For more information, see Rule definition and implementation.

Cloud Config allows you to manage the following two types of rules:

- Managed rules

  A managed rule is a rule function that Cloud Config creates in Function Compute. If you create a rule based on a managed rule, you can directly select the managed rule in the Cloud Config console. For more information about the managed rules that Cloud Config provides, see Managed rules.

- Custom rules

  A custom rule is created based on a rule function that you create in Function Compute. To create a rule based on a rule function, you must create the rule function in Function Compute and enter the Alibaba Cloud Resource Name (ARN) of the rule function in the Cloud Config console. For more information about the code and input parameters of a custom rule function, see Custom rule functions.

Use an ordinary account

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. On the **Create Rule** page, search for a managed rule based on the rule name, tag, evaluation logic, or risk level.
5. Click **Apply Rule**.
6. In the **Properties** step, set the Rule Name, Risk Level, and Description parameters. Then, click **Next**.

   The Rule Name, Risk Level, and Trigger Type parameters have default values. You can change the values of the Rule Name and Risk Level parameters.
7. In the **Access Resource Scope** step, keep the default resource type and click **Next**.
8. In the **Parameters** step, click **Next**.

   If the managed rule has an input parameter, you must set an expected value for the input parameter.
9. In the **Modify** step, click **Next**.

   For managed rules that allow you to modify the remediation settings, you can select the check box next to **Modify** and set the remediation method, remediation type, and parameters involved. For more information, see Configure automatic remediation or Configure manual remediation.
10. In the **Preview and Save** step, check the configurations and click **Submit**.
11. Verify that the rule is created.

- Click **View Details**. On the page that appears, you can view the rule details on the **Rule Details**, **Result**, and **Correction Details** tabs.
- Click **Return to Rule List**. In the **Rules** list, you can view the status of the created rule in the Status column. In normal cases, the rule is in the **Active** state.

Use a management account

1. Log on to the Cloud Config console.
2. In the left-side navigation pane, click **Rules**.
3. On the **Rules** page, click the required account group tab.
4. On the account group tab, click **Create Rule**.
5. On the **Create Rule** page, search for a managed rule based on the rule name, tag, evaluation logic, or risk level.
6. Click **Apply Rule**.
7. In the **Properties** step, set the Rule Name, Risk Level, and Description parameters. Then, click **Next**.

   The Rule Name, Risk Level, and Trigger Type parameters have default values. You can change the values of the Rule Name and Risk Level parameters.
8. In the **Access Resource Scope** step, keep the default resource type and click **Next**.
9. In the **Parameters** step, click **Next**.

   If the managed rule has an input parameter, you must set an expected value for the input parameter.
10. In the **Modify** step, click **Next**.

    For managed rules that allow you to modify the remediation settings, you can select the check box next to **Modify** and set the remediation method, remediation type, and parameters involved. For more information, see Configure automatic remediation or Configure manual remediation.
11. In the **Preview and Save** step, check the configurations and click **Submit**.
12. Verify that the rule is created.
    - Click **View Details**. On the page that appears, you can view the rule details on the **Rule Details**, **Result**, and **Correction Details** tabs.
    - Click **Return to Rule List**. In the **Rules** list, you can view the status of the created rule in the Status column. In normal cases, the rule is in the **Active** state.

1.2. Create a rule based on Function Compute

If the managed rules provided by Cloud Config cannot meet your requirements on resource auditing, you can create rules based on Function Compute to audit associated resources. When a rule is triggered, Cloud Config invokes the corresponding rule function to evaluate the associated resources and returns the compliance evaluation results of the resources.

Prerequisites

Function Compute is activated. For more information, see Rule definition and implementation.

Context

Before you create a rule, you must familiarize yourself with the definition of rules and how rules work. For more information, see Rule definition and implementation.

Cloud Config allows you to manage the following two types of rules:

- Managed rules

  A managed rule is a rule function that Cloud Config creates in Function Compute. If you create a rule based on a managed rule, you can directly select the managed rule in the Cloud Config console. For more information about the managed rules that Cloud Config provides, see Managed rules.

- Custom rules

  A custom rule is created based on a rule function that you create in Function Compute. To create a rule based on a rule function, you must create the rule function in Function Compute and enter the Alibaba Cloud Resource Name (ARN) of the rule function in the Cloud Config console. For more information about the code and input parameters of a custom rule function, see Custom rule functions.

Use an ordinary account

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. On the **Create Rule** page, click **Create Custom Rule**.
5. In the **Properties** step, set the Function ARN, Rule Name, Risk Level, Trigger Type, and Description parameters. Then, click **Next**.
    - If you have created a rule function, directly select the ARN of the function.
    - If you have not created a rule function, click **Create New Function** to create a rule function in the Function Compute console. For more information, see Overview.

      When you create a rule function, set the **Function Type** parameter to **Event Function**, the **Runtime** parameter to **Python 3**, and the **Function Handler** parameter to the default value **index.handler**.
6. In the **Assess Resource Scope** step, specify the resource types associated with the rule and click **Next**.
7. In the **Parameters** step, click **Add Rule Parameter**, specify a name and an expected value for an input parameter, and then click **Next**.
    - After you specify the resource types, Cloud Config monitors all your resources of the specified types based on the rule. Each rule can be applied to one or more resource types.
    - The names of the input parameters must be the same as those of the configuration items to be evaluated.
8. In the **Modify** step, click **Next**.
9. In the **Preview and Save** step, check the configurations and click **Submit**.
10. Verify that the rule is created.
    - Click **View Details**. On the page that appears, you can view the rule details on the **Rule Details**, **Result**, and **Correction Details** tabs.
    - Click **Return to Rule List**. In the **Rules** list, you can view the status of the created rule in the Status column. In normal cases, the rule is in the **Active** state.

Use a management account

1. Log on to the Cloud Config console.
2. In the left-side navigation pane, click **Rules**.
3. On the **Rules** page, click the required account group tab.
4. On the account group tab, click **Create Rule**.
5. On the **Create Rule** page, click **Create Custom Rule**.
6. In the **Properties** step, set the Function ARN, Rule Name, Risk Level, Trigger Type, and Description parameters. Then, click **Next**.
    - If you have created a rule function, directly select the ARN of the function.
    - If you have not created a rule function, click **Create New Function** to create a rule function in the Function Compute console. For more information, see Overview.

      When you create a rule function, set the **Function Type** parameter to **Event Function**, the **Runtime** parameter to **Python 3**, and the **Function Handler** parameter to the default value **index.handler**.
7. In the **Assess Resource Scope** step, specify the resource types associated with the rule and click **Next**.
8. In the **Parameters** step, click **Add Rule Parameter**, specify a name and an expected value for an input parameter, and then click **Next**.
    - After you specify the resource types, Cloud Config monitors all your resources of the specified types based on the rule. Each rule can be applied to one or more resource types.
    - The names of the input parameters must be the same as those of the configuration items to be evaluated.
9. In the **Modify** step, click **Next**.
10. In the **Preview and Save** step, check the configurations and click **Submit**.
11. Verify that the rule is created.
    - Click **View Details**. On the page that appears, you can view the rule details on the **Rule Details**, **Result**, and **Correction Details** tabs.
    - Click **Return to Rule List**. In the **Rules** list, you can view the status of the created rule in the Status column. In normal cases, the rule is in the **Active** state.

1.3. Modify a rule

If existing rules cannot meet your compliance requirements, you can modify the rules as needed. You can modify only the created rules in the rule list. You cannot modify the preset rules in compliance packages.

Context

After you enable a compliance package, rules whose names are prefixed with the compliance package name are automatically generated in the Cloud Config console. You cannot directly modify, delete, enable, or disable these rules. However, you can modify the compliance package to update the parameter settings of these rules. For more information, see Edit a compliance package.

Use an ordinary account

1. Log on to the Cloud Config console.
2. In the left-side navigation pane, click **Rules**.
3. On the **Rules** page, find the rule that you want to modify and click **Edit** in the **Actions** column.
4. In the **Properties** step, modify the description of the rule and click **Next**.
5. In the **Assess Resource Scope** step, click **Next**.

   For managed rules that are associated with tags and custom rules, you can modify the related resources.
6. In the **Parameters** step, modify the expected value of the input parameter and click **Next**.

   You can modify both the name and expected value of the input parameter of a custom rule.
7. In the **Modify** step, click **Next**.

   For managed rules that allow you to modify the remediation settings, you can select the check box next to **Modify** and set the remediation method, remediation type, and parameters involved. For more information, see Configure automatic remediation or Configure manual remediation.
8. In the **Preview and Save** step, check the configurations and click **Submit**.
9. View the modification result.
   - Click **View Details**. On the page that appears, you can view the rule details on the **Rule Details**, **Result**, and **Correction Details** tabs.
   - Click **Return to Rule List**. In the **Rules** list, you can view the status of the created rule in the Status column. In normal cases, the rule is in the **Active** state.

Use a management account

1. Log on to the Cloud Config console.
2. In the left-side navigation pane, click **Rules**.
3. On the **Rules** page, click the required account group tab.
4. On the account group tab, find the rule that you want to modify and click **Edit** in the **Actions** column.
5. In the **Properties** step, modify the description of the rule and click **Next**.
6. In the **Assess Resource Scope** step, click **Next**.

   For managed rules that are associated with tags and custom rules, you can modify the related resources.
7. In the **Parameters** step, modify the expected value of the input parameter and click **Next**.

   You can modify both the name and expected value of the input parameter of a custom rule.
8. In the **Modify** step, click **Next**.

   For managed rules that allow you to modify the remediation settings, you can select the check box next to **Modify** and set the remediation method, remediation type, and parameters involved. For more information, see Configure automatic remediation or Configure manual remediation.
9. In the **Preview and Save** step, check the configurations and click **Submit**.
10. View the modification result.
    - Click **View Details**. On the page that appears, you can view the rule details on the **Rule Details**, **Result**, and **Correction Details** tabs.
    - Click **Return to Rule List**. In the **Rules** list, you can view the status of the created rule in the

Status column. In normal cases, the rule is in the **Active** state.

1.4. Disable a rule

This topic describes how to disable a rule. You can disable a rule if you do not need it. You can disable only the created rules in the rule list. You cannot disable the preset rules in compliance packages.

Prerequisites

The rules that you want to disable are in the **Active** state in the **Status** column.

Context

After you enable a compliance package, rules whose names are prefixed with the compliance package name are automatically generated in the Cloud Config console. You cannot disable these rules.

Use an ordinary account

1. Log on to the Cloud Config console.
2. In the left-side navigation pane, click **Rules**.
3. Disable one or more rules as needed.
    - Disable a single rule
        a. On the **Rules** page, find the rule that you want to disable, move the pointer over the ⋮ icon in the **Actions** column, and then select **Disable Rule**.
        b. In the **Are you sure you want to terminate the rule?** message, click **OK**.
    - Disable multiple rules at a time
        a. On the **Rules** page, find the rules that you want to disable, select the check boxes next to the rules, and then click the ⏸ icon.
        b. In the **Disable Selected Rules** message, click **OK**.
4. View the status of the rules.

    On the **Rules** page, set filter conditions to search for the rules and check whether the rules are in the **Inactive** state. After a rule is disabled, it no longer takes effect. The compliance evaluation results that are returned before the rule is disabled are displayed.

Use a management account

1. Log on to the Cloud Config console.
2. In the left-side navigation pane, click **Rules**.
3. On the **Rules** page, click the required account group tab.
4. Disable one or more rules as needed.
    - Disable a single rule
        a. On the account group tab, find the rule that you want to disable, move the pointer over the ⋮ icon in the **Actions** column, and then select **Disable Rule**.

    b. In the **Are you sure you want to terminate the rule?** message, click **OK**.

  - Disable multiple rules at a time

    a. On the account group tab, find the rules that you want to disable, select the check boxes next to the rules, and then click the ⏸ icon.

    b. In the **Disable Selected Rules** message, click **OK**.

5. View the status of the rules.

   On the account group tab, set filter conditions to search for the rules and check whether the rules are in the **Inactive** state.

What to do next

You can enable a rule that is in the **Inactive** state. After a rule is enabled, it enters the **Active** state again. To enable one or more disabled rules, perform the following steps:

- Use an ordinary account
  - Enable a single rule

    On the **Rules** page, find the rule that you want to enable, move the pointer over the

    ⋮

    icon in the **Actions** column, and then select **Enable Rule**.
  - Enable multiple rules at a time

    a. On the **Rules** page, find the rules that you want to enable, select the check boxes next to the rules, and then click the ▶ icon.

    b. In the **Enable Selected Rules** message, click **OK**.
- Use a management account
  - Enable a single rule

    On the account group tab, find the rule that you want to enable, move the pointer over the

    ⋮

    icon in the **Actions** column, and then select **Enable Rule**.
  - Enable multiple rules at a time

    a. On the account group tab, find the rules that you want to enable, select the check boxes next to the rules, and then click the ▶ icon.

    b. In the **Enable Selected Rules** message, click **OK**.

1.5. Delete a rule

When you no longer need a rule, you can delete it. You can delete a rule in the Cloud Config console. After you delete the rule, all of its configurations are deleted. You can delete only the rules that you create in the rule list. You cannot delete the preset rules in compliance packages.

Prerequisites

The rule that you want to delete is disabled. For more information, see Disable a rule.

Context

After you enable a compliance package, rules whose names are prefixed with the compliance package name are automatically generated in the Cloud Config console. You cannot directly delete these rules.

To delete such a rule, you must delete the compliance package of the rule or turn off the switch for the rule. For information about how to delete a compliance package, see Delete a compliance package.

Use an ordinary account

1. Log on to the Cloud Config console.
2. In the left-side navigation pane, click **Rules**.
3. On the **Rules** page, set filter conditions to find the rules in the **Inactive** state.
4. Delete one or more rules as required.
   - To delete a single rule, perform the following steps:
     a. Find the rule that you want to delete, move the pointer over the

        ⋮

        icon in the **Actions** column, and then select **Delete**.
     b. In the **Are you sure you want to delete the rule?** message, click **Delete**.
   - To delete multiple rules at a time, perform the following steps:
     a. Select the rules that you want to delete and click the 🗑 icon.
     b. In the **Delete Selected Rules** message, click **OK**.
5. Verify that the rule is deleted.

   After you delete a rule, it is no longer displayed on the **Rules** page.

Use a management account

1. Log on to the Cloud Config console.
2. In the left-side navigation pane, click **Rules**.
3. On the **Rules** page, click the required account group tab.
4. On the account group tab, set filter conditions to find the rules in the **Inactive** state.
5. Delete one or more rules as required.
   - To delete a single rule, perform the following steps:
     a. Find the rule that you want to delete, move the pointer over the

        ⋮

        icon in the **Actions** column, and then select **Delete**.
     b. In the **Are you sure you want to delete the rule?** message, click **Delete**.
   - To delete multiple rules at a time, perform the following steps:
     a. Select the rules that you want to delete and click the 🗑 icon.
     b. In the **Delete Selected Rules** message, click **OK**.

6. Verify that the rule is deleted.

   After you delete a rule, it is no longer displayed on the account group tab.

1.6. Manually re-evaluate resources

This topic describes how to manually re-evaluate resources. After you modify rules or resources, you can manually re-evaluate resources if you want to immediately view the latest compliance evaluation results. If you do not manually re-evaluate resources, you can view the compliance evaluation results only after resource configurations are changed or rules are triggered at the scheduled time.

Prerequisites

The rule that you want to use to re-evaluate resources is in the **Active** state in the **Status** column.

Context

You can re-evaluate resources based on the rules that you create. You can also re-evaluate resources based on the rules that Cloud Config creates when you enable compliance packages. The names of these rules are prefixed with the names of the compliance packages.

Use an ordinary account

1. Log on to the Cloud Config console.
2. In the left-side navigation pane, click **Rules**.
3. On the **Rules** page, find the rule that you want to use to re-evaluate resources. Then, click the rule name in the **Rule Name** column or click **Details** in the **Actions** column.
4. On the **Rule Details** tab, click **Re-evaluate** in the upper-right corner.

Use a management account

1. Log on to the Cloud Config console.
2. In the left-side navigation pane, click **Rules**.
3. On the **Rules** page, click the required account group tab.
4. On the account group tab, find the rule that you want to use to re-evaluate resources. Then, click the rule name in the **Rule Name** column or click **Details** in the **Actions** column.
5. On the **Rule Details** tab, click **Re-evaluate** in the upper-right corner.

2.Remediation settings

2.1. Overview

You can specify a remediation template for a rule when you create or edit the rule. A remediation template is a workflow in Logic Composer. If the configuration of a resource is non-compliant, the template can be automatically or manually triggered to modify the configuration.

You must grant Logic Composer and Operation Orchestration Service (OOS) the required permissions to modify the configurations of your resources based on the remediation template. For more information about Logic Composer, see What is Logic Composer?. For more information about OOS, see Introduction to OOS.

When you create or edit a rule, you can configure or skip the remediation settings. Automatic and manual execution of remediation templates have the following differences:

- Automatic execution: If the resources to which the rule is applied are evaluated as non-compliant, the configurations of the resources are automatically remediated.
- Manual execution: If the resources to which the rule is applied are evaluated as non-compliant, the configurations of the resources are not automatically remediated. You can manually run the template to remediate the resource configurations on the Correction Details tab of the rule.

Limits

- You can specify remediation templates only for specific managed rules. Cloud Config is planning to support remediation settings for more managed rules.
- You can specify only one remediation template for a rule. Default templates are applicable only to managed rules.

Related features

The following table describes the features that are related to remediation settings.

Feature	Description
Configure automatic remediation	When you create a rule, you can specify a remediation template for the rule and configure automatic execution for the template. If the configuration of a resource is non-compliant, the template automatically runs to correct the configuration.
Configure manual remediation	When you create a rule, you can specify a remediation template for the rule and configure manual execution for the template. If the configuration of a resource is non-compliant, you can manually run the template to remediate the configuration.
Delete remediation settings	Cloud Config allows you to delete remediation settings and revoke permissions.

2.2. Configure automatic remediation

When you create a rule, you can specify a remediation template for the rule and configure automatic execution for the template. If the configuration of a resource is non-compliant, the template automatically runs to correct the configuration.

Context

This topic describes how to configure automatic remediation by creating a rule based on the **required-tags** managed rule.

The **required-tags** managed rule checks whether the associated resources have all the specified tags. You may want the tag "Project=A" to be attached to all Elastic Compute Service (ECS) instances within your Alibaba Cloud account. In this case, you can create a rule based on the **required-tags** managed rule to monitor all your ECS instances. If Cloud Config detects that the tag is not attached to one or more ECS instances, these resources are evaluated to be **non-compliant** based on the rule. If you subscribe to resource non-compliance events, Cloud Config sends notifications of resource non-compliance events to a specified Message Service (MNS) topic. For more information, see Send notifications of resource events to an MNS topic.

Use an ordinary account

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. On the **Create Rule** page, find the managed rule based on which you want to create a rule.
5. Click **Apply Rule**.
6. In the **Properties** step, set the Rule Name and Risk Level parameters. Then, click **Next**.

   The Rule Name, Risk Level, and Trigger Type parameters have default values. You can change the values of the Rule Name and Risk Level parameters.
7. In the **Access Resource Scope** step, keep the default resource type and click **Next**.
8. In the **Parameters** step, enter the key and value of a tag and click **Next**.

   If you want to check multiple tags, you can specify multiple key-value pairs in sequence. You can specify up to six key-value pairs. If specific resources have all the specified tags, these resources are evaluated to be **compliant** based on the rule. If you want to check whether a specified tag is attached to specific resources, you must create a rule for each tag based on the required-tags managed rule.

   You may want the tag "Project=A" to be attached to all the resources within your Alibaba Cloud account. In this case, you can create a rule based on the **required-tags** managed rule to monitor all your resources. If Cloud Config detects that the tag is not attached to one or more of your resources, these resources are evaluated to be **non-compliant**.
9. In the **Modify** step, select the check box next to **Modify**, select **Automatic Remediation**, set the Remediation Type parameter to **Operation Orchestration Service**, enter the key-value pairs of the required tags, and then click **Next**.

   > ? **Note** You must specify the key-value pairs of the tags that you want to attach to your resources.
10. In the **Preview and Save** step, check the settings and click **Submit**.
11. View the remediation results.

    If a resource is evaluated to be **non-compliant** based on the rule, Cloud Config triggers the remediation template. The configurations of the non-compliant resource are automatically changed to the preset values.

   i. In the left-side navigation pane, click **Rules**.
   ii. On the **Rules** page, find the created rule, and click **Details** in the **Actions** column or the rule name in the **Rule Name/Rule ID** column.
   iii. On the rule details page, click the **Correction Details** tab.
   iv. On the **Correction Details** tab, view the remediation results.

Use a management account

1. Log on to the Cloud Config console.
2. In the left-side navigation pane, click **Rules**.
3. On the **Rules** page, click the required account group tab.
4. On the account group tab, click **Create Rule**.
5. On the **Create Rule** page, find the managed rule based on which you want to create a rule.
6. Click **Apply Rule**.
7. In the **Properties** step, set the Rule Name and Risk Level parameters. Then, click **Next**.

   The Rule Name, Risk Level, and Trigger Type parameters have default values. You can change the values of the Rule Name and Risk Level parameters.
8. In the **Access Resource Scope** step, keep the default resource type and click **Next**.
9. In the **Parameters** step, enter the key and value of a tag and click **Next**.

   If you want to check multiple tags, you can specify multiple key-value pairs in sequence. You can specify up to six key-value pairs. If specific resources have all the specified tags, these resources are evaluated to be **compliant** based on the rule. If you want to check whether a specified tag is attached to specific resources, you must create a rule for each tag based on the required-tags managed rule.

   You may want the tag "Project=A" to be attached to all the resources within your Alibaba Cloud account. In this case, you can create a rule based on the **required-tags** managed rule to monitor all your resources. If Cloud Config detects that the tag is not attached to one or more of your resources, these resources are evaluated to be **non-compliant**.
10. In the **Modify** step, select the check box next to **Modify**, select **Automatic Remediation**, set the Remediation Type parameter to **Operation Orchestration Service**, enter the key-value pairs of the required tags, and then click **Next**.

    > **Note** You must specify the key-value pairs of the tags that you want to attach to your resources.
11. In the **Preview and Save** step, check the settings and click **Submit**.
12. View the remediation results.

    If a resource is evaluated to be **non-compliant** based on the rule, Cloud Config triggers the remediation template. The configurations of the non-compliant resource are automatically changed to the preset values.

   i. In the left-side navigation pane, click **Rules**.
   ii. On the **Rules** page, find the created rule, and click **Details** in the **Actions** column or the rule name in the **Rule Name/Rule ID** column.
   iii. On the rule details page, click the **Correction Details** tab.

iv. On the **Correction Details** tab, view the remediation results.

Related operations

Manage the AliyunServiceRoleForConfigRemediation service-linked role

2.3. Configure manual remediation

When you create a rule, you can specify a remediation template for the rule and configure manual execution for the template. If the configuration of a resource is non-compliant, you can manually run the template to remediate the configuration.

Context

This topic describes how to configure manual remediation by creating a rule based on the **required-tags** managed rule.

The **required-tags** managed rule checks whether the associated resources have all the specified tags. You may want the tag "Project=A" to be attached to all Elastic Compute Service (ECS) instances within your Alibaba Cloud account. In this case, you can create a rule based on the **required-tags** managed rule to monitor all your ECS instances. If Cloud Config detects that the tag is not attached to one or more ECS instances, these resources are evaluated to be **non-compliant** based on the rule. If you subscribe to resource non-compliance events, Cloud Config sends notifications of resource non-compliance events to a specified Message Service (MNS) topic. For more information, see Send notifications of resource events to an MNS topic.

Use an ordinary account

1. Configure the manual remediation settings.
   i. Log on to the Cloud Config console.
   ii. In the left-side navigation pane, click **Rules**.
   iii. On the **Rules** page, click **Create Rule**.
   iv. On the **Create Rule** page, find the managed rule based on which you want to create a rule.
   v. Click **Apply Rule**.
   vi. In the **Properties** step, set the Rule Name and Risk Level parameters. Then, click **Next**.

      The Rule Name, Risk Level, and Trigger Type parameters have default values. You can change the values of the Rule Name and Risk Level parameters.
   vii. In the **Access Resource Scope** step, keep the default resource type and click **Next**.
   viii. In the **Parameters** step, enter the key and value of a tag and click **Next**.

      If you want to check multiple tags, you can specify multiple key-value pairs in sequence. You can specify up to six key-value pairs. If specific resources have all the specified tags, these resources are evaluated to be **compliant** based on the rule. If you want to check whether a specified tag is attached to specific resources, you must create a rule for each tag based on the required-tags managed rule.

      You may want the tag "Project=A" to be attached to all the resources within your Alibaba Cloud account. In this case, you can create a rule based on the **required-tags** managed rule to monitor all your resources. If Cloud Config detects that the tag is not attached to one or more of your resources, these resources are evaluated to be **non-compliant**.

ix. In the **Modify** step, select the check box next to **Modify**, select **Manual Remediation**, set the Remediation Type parameter to **Operation Orchestration Service**, enter the key-value pairs of the required tags, and then click **Next**.

> ? **Note** You must specify the key-value pairs of the tags that you want to attach to your resources.

x. In the **Preview and Save** step, check the settings and click **Submit**.

2. Perform manual remediation.

   If you receive notifications of resource non-compliance events or find non-compliant resources, you can manually trigger the remediation template on the **Correction Details** tab of the details page for the specified rule. Then, the configurations of the non-compliant resources are changed to the preset values. To manually remediate non-compliant resources, perform the following steps:

   i. In the left-side navigation pane, click **Rules**.

   ii. On the **Rules** page, find the created rule, and click **Details** in the **Actions** column or the rule name in the **Rule Name/Rule ID** column.

   iii. On the rule details page, click the **Correction Details** tab.

   iv. On the **Correction Details** tab, click **Perform Manual Correction** next to **Remediation Method**.

3. On the **Correction Details** tab, view the remediation results.

Use a management account

1. Configure the manual remediation settings.

   i. Log on to the Cloud Config console.

   ii. In the left-side navigation pane, click **Rules**.

   iii. On the **Rules** page, click the required account group tab.

   iv. On the account group tab, click **Create Rule**.

   v. On the **Create Rule** page, find the managed rule based on which you want to create a rule.

   vi. Click **Apply Rule**.

   vii. In the **Properties** step, set the Rule Name and Risk Level parameters. Then, click **Next**.

   The Rule Name, Risk Level, and Trigger Type parameters have default values. You can change the values of the Rule Name and Risk Level parameters.

   viii. In the **Access Resource Scope** step, keep the default resource type and click **Next**.

ix. In the **Parameters** step, enter the key and value of a tag and click **Next**.

If you want to check multiple tags, you can specify multiple key-value pairs in sequence. You can specify up to six key-value pairs. If specific resources have all the specified tags, these resources are evaluated to be **compliant** based on the rule. If you want to check whether a specified tag is attached to specific resources, you must create a rule for each tag based on the required-tags managed rule.

You may want the tag "Project=A" to be attached to all the resources within your Alibaba Cloud account. In this case, you can create a rule based on the **required-tags** managed rule to monitor all your resources. If Cloud Config detects that the tag is not attached to one or more of your resources, these resources are evaluated to be **non-compliant**.

x. In the **Modify** step, select the check box next to **Modify**, select **Manual Remediation**, set the Remediation Type parameter to **Operation Orchestration Service**, enter the key-value pairs of the required tags, and then click **Next**.

> **Note** You must specify the key-value pairs of the tags that you want to attach to your resources.

xi. In the **Preview and Save** step, check the settings and click **Submit**.

2. Perform manual remediation.

   If you receive notifications of resource non-compliance events or find non-compliant resources, you can manually trigger the remediation template on the **Correction Details** tab of the details page for the specified rule. Then, the configurations of the non-compliant resources are changed to the preset values. To manually remediate non-compliant resources, perform the following steps:

   i. In the left-side navigation pane, click **Rules**.

   ii. On the **Rules** page, click the required account group tab.

   iii. On the account group tab, find the created rule, and click **Details** in the **Actions** column or the rule name in the **Rule Name/Rule ID** column.

   iv. On the rule details page, click the **Correction Details** tab.

   v. On the **Correction Details** tab, click **Perform Manual Correction** next to **Remediation Method**.

3. On the **Correction Details** tab, view the remediation results.

Related operations

Manage the AliyunServiceRoleForConfigRemediation service-linked role

2.4. Delete remediation settings

Cloud Config allows you to delete remediation settings and revoke permissions.

Use an ordinary account

1. Log on to the Cloud Config console.
2. In the left-side navigation pane, click **Rules**.
3. On the **Rules** page, find the required rule, and click **Details** in the **Actions** column or the rule name in the **Rule Name/Rule ID** column.

4. On the rule details page, click the **Correction Details** tab.
5. On the **Correction Details** tab, click **Delete** in the Correction Details section.

Use a management account

1. Log on to the Cloud Config console.
2. In the left-side navigation pane, click **Rules**.
3. On the **Rules** page, click the required account group tab.
4. On the account group tab, find the required rule, and click **Details** in the **Actions** column or the rule name in the **Rule Name/Rule ID** column.
5. On the rule details page, click the **Correction Details** tab.
6. On the **Correction Details** tab, click **Delete** in the Correction Details section.

Related operations

Manage the AliyunServiceRoleForConfigRemediation service-linked role

3.View compliance evaluation results

3.1. View the compliance evaluation results

This topic describes how to view the compliance evaluation results that are generated based on a rule in the Cloud Config console.

Use an ordinary account

- Method 1: View the value in the **Compliance** column in the **Rules** list. You can perform the following steps:

  i. Log on to the Cloud Config console.

  ii. In the left-side navigation pane, click **Rules**.

- Method 2: Go to the **Result** tab. You can perform the following steps:

  i. Log on to the Cloud Config console.

  ii. In the left-side navigation pane, click **Rules**.

  iii. On the **Rules** page, find the rule for which you want to view the compliance evaluation results. Then, click the rule name in the **Rule Name** column or click **Detail** in the **Actions** column.

  iv. Click the **Result** tab.

Use a management account

- Method 1: View the value in the **Compliance** column in the **Rules** list. You can perform the following steps:

  i. Log on to the Cloud Config console.

  ii. In the left-side navigation pane, click **Rules**.

  iii. On the **Rules** page, click the required account group tab.

- Method 2: Go to the **Result** tab. You can perform the following steps:

  i. Log on to the Cloud Config console.

  ii. In the left-side navigation pane, click **Rules**.

  iii. On the **Rules** page, click the required account group tab.

  iv. On the account group tab, find the rule for which you want to view the compliance evaluation results. Then, click the rule name in the **Rule Name** column or click **Detail** in the **Actions** column.

  v. Click the **Result** tab.

3.2. View the compliance timeline of a resource

In Cloud Config, each resource has its own compliance timeline. Cloud Config generates a compliance evaluation record for a resource each time the resource is evaluated by a rule, and displays the compliance evaluation records over time in a compliance timeline.

Context

The compliance timeline of a resource indicates the compliance evaluation history of the resource. The following table describes the elements included in the compliance timeline.

Element	Description
Points on a compliance timeline	- Start point: the time when a resource is evaluated by a rule for the first time. You can configure Cloud Config to run a rule to periodically evaluate a resource at the specified time or each time you change the resource configuration. You can also manually run a rule to evaluate a resource. - Node: A node is generated on the compliance timeline of a resource each time the resource is evaluated. One or more rules may be used to evaluate a resource at a time. - Breakpoint: A compliance timeline does not have breakpoints. If you remove a resource type from the monitoring scope of Cloud Config, Cloud Config stops monitoring this type of resources and does not update the compliance timeline of each resource of this type. Cloud Config monitors this type of resources again only after you add the resource type to the monitoring scope. Cloud Config does not record the changes of the resources before you add the resource type to the monitoring scope.
Content on a compliance timeline	- Time: the time when a compliance evaluation is performed. - Trigger type: the reason that triggers the compliance evaluation on a resource. A compliance evaluation can be manually or periodically triggered, and can also be triggered based on real-time configuration changes. - Compliance evaluation results: On the left side of the **Compliance Timeline** tab, the evaluation result for each node can be marked as Compliant or Non-compliant. This helps you find non-compliant resources. - Evaluation details of each node: You can view the basic information about the resource and the current evaluation result. If the evaluation is periodically triggered, or triggered based on real-time configuration changes, the change details of core resource configuration are also displayed for you to find non-compliant configuration items.

Use an ordinary account

1. Log on to the Cloud Config console.
2. In the left-side navigation pane, click **Resources**.
3. On the **Resources** page, set filter conditions or enter a resource ID to search for the resource for which you want to view the compliance timeline.
4. Click the resource ID in the **Resource ID / Resource Name** column.
5. Click the **Compliance Timeline** tab to view the compliance timeline of the resource.
   - In the **Basic Information** section, you can view the ID, name, type, and tags of the resource, the time when the resource was created, and the region and zone where the resource resides.
   - In the **Evaluation Result** section, you can view the latest compliance evaluation result of the resource.
   - In the **Change Details** section, you can view the relevant resource configurations before and after the current configuration change in the JSON format.

Use a management account

1. Log on to the Cloud Config console.
2. In the left-side navigation pane, click **Resources**.
3. On the **Resources** page, click the required account group tab.
4. On the account group tab, set filter conditions or enter a resource ID to search for the resource for which you want to view the compliance timeline.
5. Click the resource ID in the **Resource ID / Resource Name** column.
6. Click the **Compliance Timeline** tab to view the compliance timeline of the resource.
    - In the **Basic Information** section, you can view the ID, name, type, and tags of the resource, the time when the resource was created, and the region and zone where the resource resides.
    - In the **Evaluation Result** section, you can view the latest compliance evaluation result of the resource.
    - In the **Change Details** section, you can view the relevant resource configurations before and after the current configuration change in the JSON format.