

Config

Getting Started

Issue 01
Date 2024-09-30



Copyright © Huawei Technologies Co., Ltd. 2024. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process*. For details about this process, visit the following web page:

<https://www.huawei.com/en/psirt/vul-response-process>

For vulnerability information, enterprise customers can visit the following web page:

<https://securitybulletin.huawei.com/enterprise/en/security-advisory>

Contents

1 Enabling the Resource Recorder.....	1
2 Filtering Resources.....	4
3 Evaluating Resource Compliance.....	8

1 Enabling the Resource Recorder

Scenarios

The resource recorder automatically detects and records changes made to your resources that are supported by Config.

If you have enabled the resource recorder and specified an OBS bucket and an SMN topic when you configure the resource recorder, Config will notify you if there is a change (creation, modification, deletion, relationship change) to the resources within the monitoring scope and periodically store your notifications and resource snapshots.

To get full functionality of Config, you need to enable the resource recorder. If the resource recorder is disabled, you may fail to update your resource data, create and use rules, or to aggregate resource data.

This section describes how to enable and configure the resource recorder.

Preparations

1. If you already have a Huawei account, skip this step. If you do not have one, follow the following steps to create one:

- a. Go to [Huawei Cloud](#) and click **Sign Up**.
- b. [Sign up for a Huawei account and enable Huawei Cloud services](#).
After your account is created, you will be directed to your personal information page.
- c. Complete real-name authentication by following the instructions in [Individual Real-Name Authentication](#) or [Enterprise Real-Name Authentication](#).

2. Topping Up Your Account


Config is free of charge, but the SMN topic and the OBS bucket that you configured for the resource recorder will be charged. For details, see [SMN billing](#) and [OBS billing](#).

Ensure your account has sufficient balance to avoid unavailability of the resource recorder and other functions of Config. For more details, see [Topping up an Account](#).

Procedure

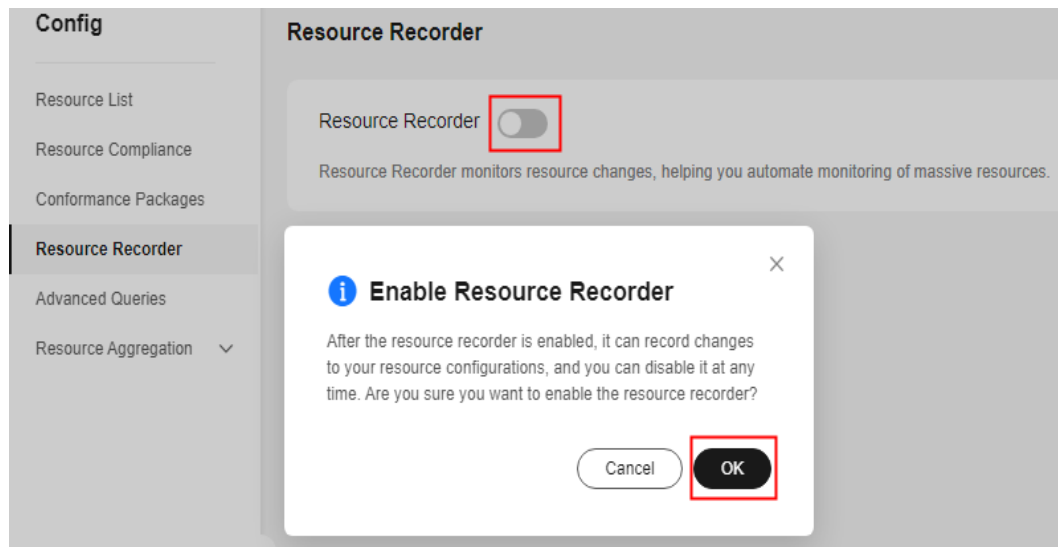
The following steps only involve mandatory parameters. For other parameters, you can keep the default configurations. For more details, see [Configuring the Resource Recorder](#).

Step 1 Log in to the management console.

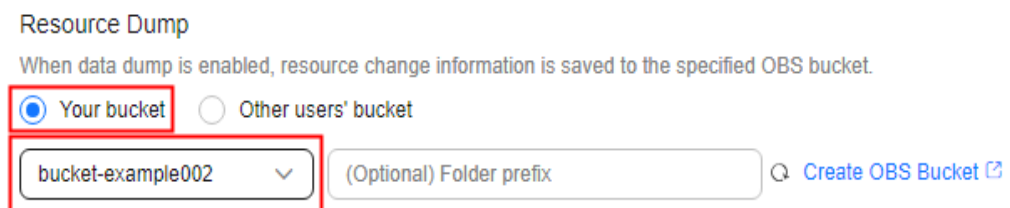
Step 2 Click  in the upper left corner of the page. In the service list that is displayed, under **Management & Governance**, select **Config**.

Step 3 In the navigation pane on the left, choose **Resource Recorder**.

Step 4 Toggle on the resource recorder and in the displayed dialog box, click **OK**.



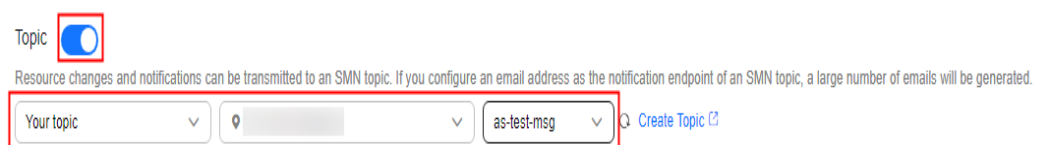
Step 5 Specify an OBS bucket.



Select an OBS bucket from the current account or another account to store resource change messages and snapshots.

If there are no OBS buckets in the current account, create one first. For details, see [Creating a Bucket](#).

Step 6 Configure an SMN topic.



Toggle on the SMN topic, select **Your topic**, and select a region and an SMN topic.

If there are no SMN topics available in the current account, create one first. For details, see [Creating a Topic](#).

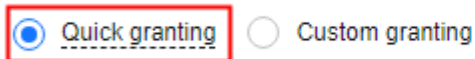
 **NOTE**

To send notifications with an SMN topic, you not only need to create the topic, but also [add subscriptions](#) and [request subscription confirmations](#).

Step 7 Grant permissions.

Grant Permissions

After the permissions are granted, resource change information can be sent to your specified SMN topic and O



Quick granting will automatically create an agency named **rms_tracker_agency** to grant the required permissions for the resource recorder to work properly. The agency contains permissions, including the **SMN Administrator** for sending notifications and the **OBS OperateAccess** permission for writing data into an OBS bucket.

Step 8 Click **Save**.

Step 9 In the displayed dialog box, click **OK**.

----End

Related Information

You can modify or disable the resource recorder at any time. You can enable or modify the resource recorder for up to 10 times per day. The number of times will be reset at 00:00 every day.

- When configuring the resource recorder, if you select an OBS bucket or SMN topic from another account, you need to be authorized by the account. For details, see [Cross-Account Authorization](#).
- If you select **Custom granting** to customize authorization for the resource recorder, you need to create an agency with IAM, and the agency must include either the permissions for sending notifications using an SMN topic or the permissions for writing data into an OBS bucket based on related configurations. To store resource changes and snapshots to an encrypted OBS bucket, you need the **KMS Administrator** permission. For details, see [Storing Resource Change Notifications and Resource Snapshots to an Encrypted OBS Bucket](#). For details about how to create an agency, see .

2 Filtering Resources

Scenario

This section describes how to filter resources on the Config console. You can get details about resources, such as the region and state.

NOTE

To use the resource list, you must enable the resource recorder. If no resources are displayed on the resource list page, check if the resource recorder is enabled, if the resource type is within the configured monitoring scope, or if the service or resource is supported by Config.

There is a delay in synchronizing data to Config, so if there is a resource change, the change may not be updated in the resource list immediately. If the resource recorder is enabled, Config will update resource changes within 24 hours.

Preparations

1. If you already have a Huawei account, skip this step. If you do not have one, follow the following steps to create one:

- a. Go to [Huawei Cloud](#) and click **Sign Up**.
- b. [Sign up for a Huawei account and enable Huawei Cloud services](#).
After your account is created, you will be directed to your personal information page.
- c. Complete real-name authentication by following the instructions in [Individual Real-Name Authentication](#) or [Enterprise Real-Name Authentication](#).

2. Topping Up Your Account

Config is free of charge, but the SMN topic and the OBS bucket that you configured for the resource recorder will be charged. For details, see [SMN billing](#) and [OBS billing](#).


Ensure your account has sufficient balance to avoid unavailability of the resource recorder and other functions of Config. For more details, see [Topping up an Account](#).

3. [Enabling the Resource Recorder](#)

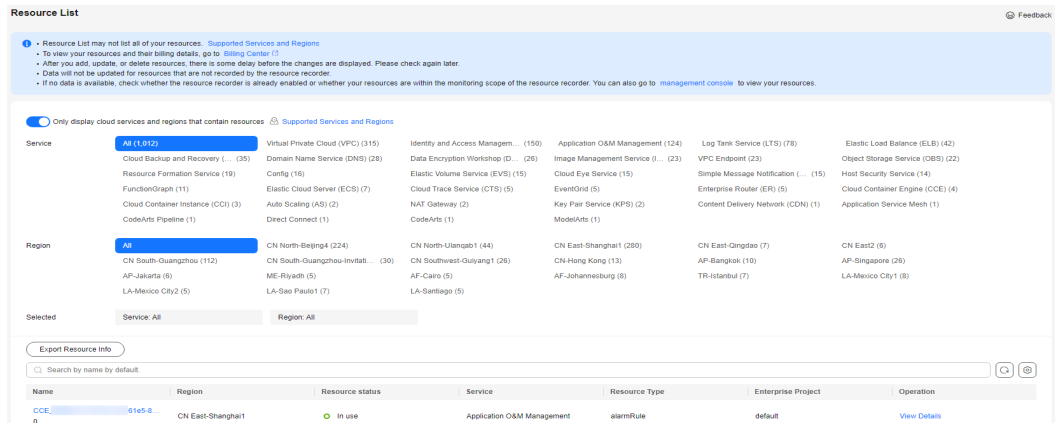
To use the resource list, the resource recorder must be enabled.

Procedure

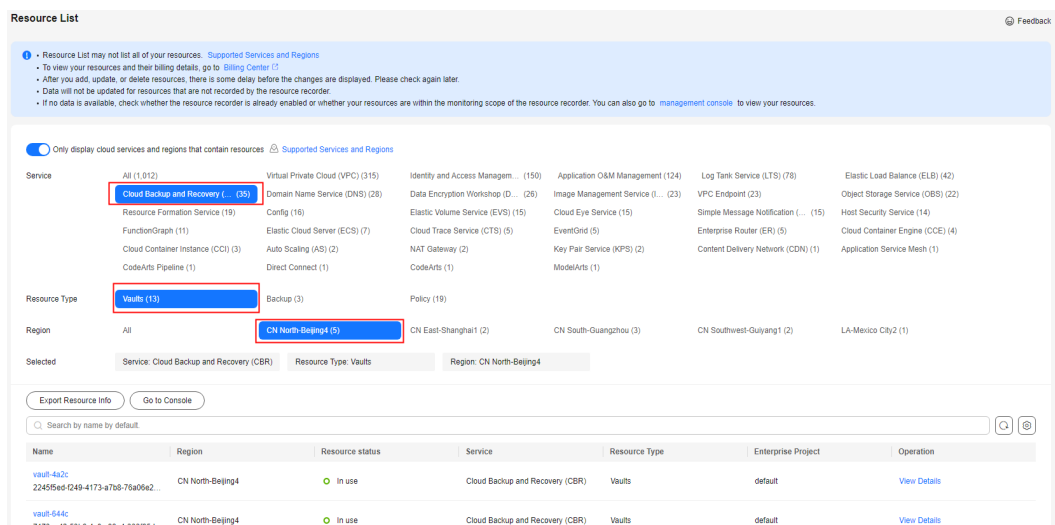
Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the page. Under **Management & Governance**, select **Config**.

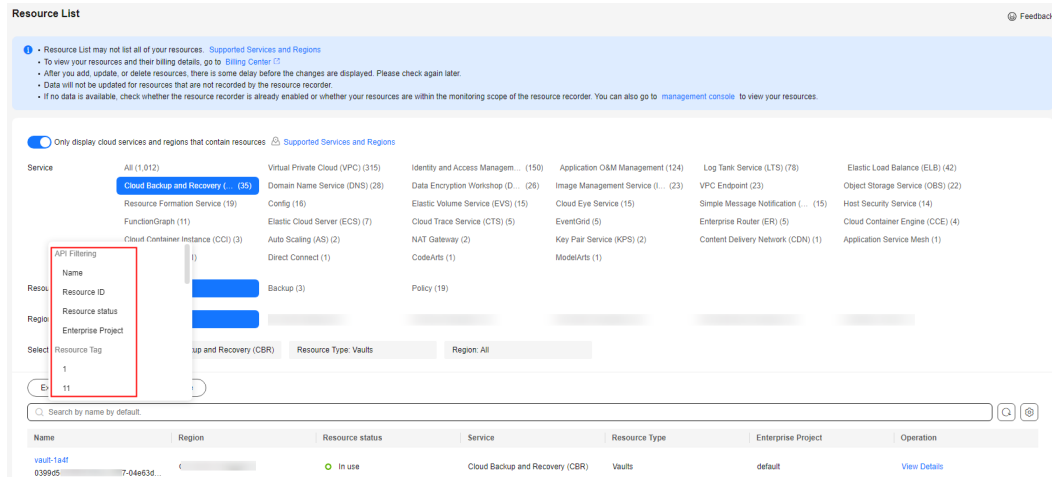
By default, the **Resource List** displays the resources that you have and are within the monitoring scope of the resource recorder.



Step 3 Set filters (service, resource type, and region) to search for resources. For global services, you do not need to set the region.



Step 4 In the search box in the middle of the page, set more refined filters to narrow down the search scope.



Filter	Description
Name	Resource name. Fuzzy search is supported. The resource name is case-insensitive.
Resource ID	Resource ID. Fuzzy search is supported. The resource ID is case-sensitive.
Resource status	Resource status. Possible resource states include: <ul style="list-style-type: none"> ● In use: A resource is being used. ● Deleted: A resource has been deleted.
Tag	Resource tag. You can select a tag key and one or all values of this key to filter resources.
Enterprise project	The enterprise project which resources belong to. If you select an enterprise project, resources in this enterprise project will be displayed. NOTE To filter resources by enterprise project, you need to enable Enterprise Center first.

----End

Related Information

The resource list allows you to perform the following operations on your resources:

- [Querying details about a resource](#)
- [Exporting resources](#)
- [Checking resource compliance](#)
- [Learning about resource relationships](#)
- [Viewing resource changes](#)

Config also provides the following advanced features for you to query resources in a more refined manner and aggregate resource data from other accounts.

- [Advanced Queries](#)
- [Resource Aggregation](#)

3 Evaluating Resource Compliance

Scenario

You can create a rule to evaluate your resource compliance. When creating a rule, you need to select [a built-in policy](#) or a custom policy, specify a monitoring scope, and specify the [trigger](#). After the evaluation, you can check the evaluation results.

This section uses the built-in policy, [Last Login Check](#) as an example to describe how to detect inactive IAM users. This policy can help reduce idle users and password leakage risks for enhanced account security.


Preparations

1. If you already have a Huawei account, skip this step. If you do not have one, follow the following steps to create one:
 - a. Go to [Huawei Cloud](#) and click **Sign Up**.
 - b. [Sign up for a Huawei account and enable Huawei Cloud services](#).
After your account is created, you will be directed to your personal information page.
 - c. Complete real-name authentication by following the instructions in [Individual Real-Name Authentication](#) or [Enterprise Real-Name Authentication](#).
2. Topping Up Your Account
Config is free of charge, but the SMN topic and the OBS bucket that you configured for the resource recorder will be charged. For details, see [SMN billing](#) and [OBS billing](#).
Ensure your account has sufficient balance to avoid unavailability of the resource recorder and other functions of Config. For more details, see [Topping up an Account](#).
3. [Enabling the Resource Recorder](#)
The resource recorder must be enabled for adding, modifying, enabling, or triggering a rule. If the resource recorder is disabled, you can only view, disable, and delete rules. In addition, only resources within the monitoring scope of the resource recorder can be evaluated by Config rules, so you are advised to select all your resources when you configure the resource recorder.

Step 1: Add a Rule

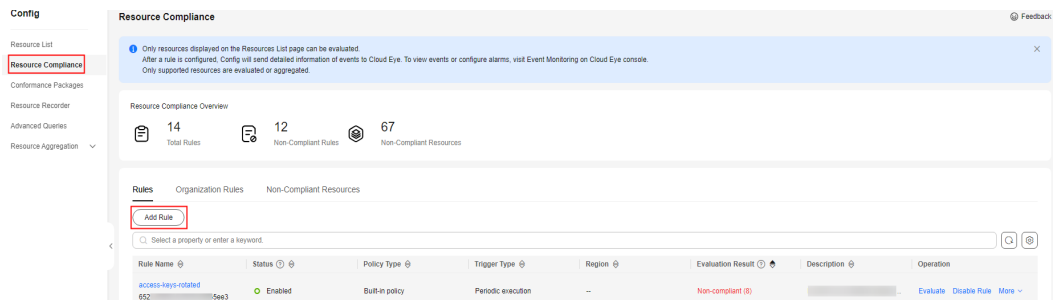
The following procedure involves specific parameters for the example rule. Other rules may contain different parameters. For more details, see [Adding a Rule with a Predefined Policy](#).

Step 1 Log in to the management console.

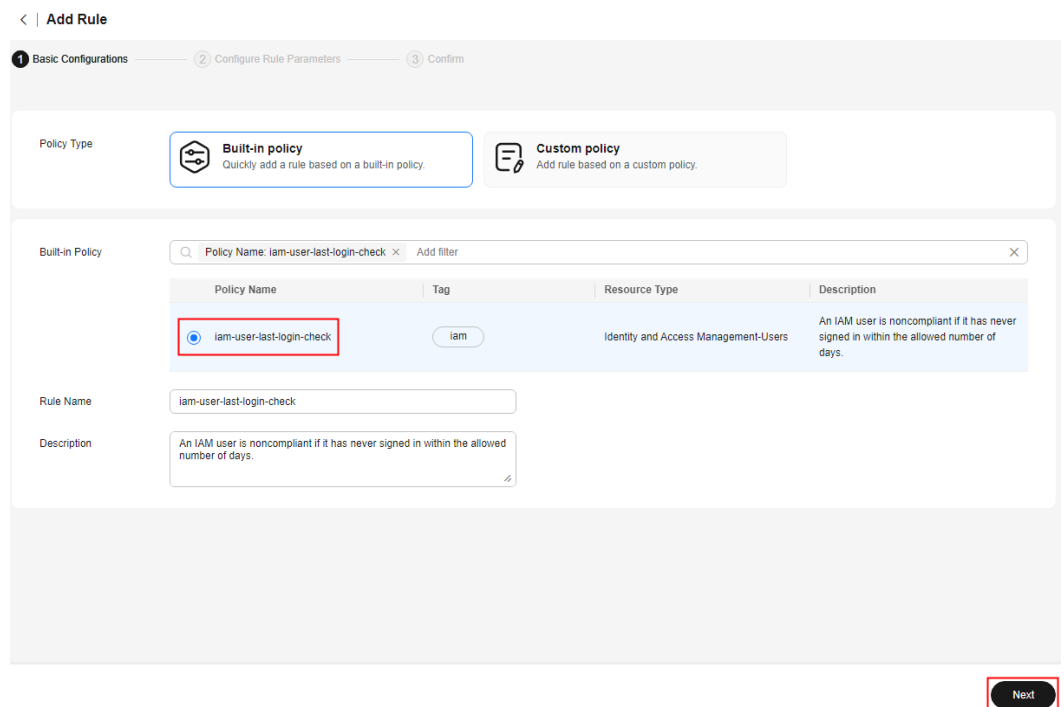
Step 2 Click  in the upper left corner of the page. In the service list that is displayed, under **Management & Governance**, select **Config**.

Step 3 In the navigation pane on the left, choose **Resource Compliance**.

Step 4 On the **Rules** tab, click **Add Rule**.



Step 5 On the **Basic Configurations** page, select **iam-user-last-login-check** and click **Next**.



Step 6 On the **Configure Rule Parameters** page, configure required parameters based on the following picture and click **Next**.

The screenshot shows the 'Add Rule' configuration interface. At the top, there are three steps: 1. Basic Configurations, 2. Configure Rule Parameters (current step), and 3. Confirm. Under 'Trigger Type', 'Periodic execution' is selected. The 'Execute Every' dropdown is set to '24 hours' and the 'Resource Scope' dropdown is set to 'All'. A table titled 'Configure Rule Parameters' has the following content:

Parameter	Description	Value
allowedInactivePeriod	Maximum number of days without login.	90

At the bottom right, there are 'Previous' and 'Next' buttons, with 'Next' being highlighted.

Parameter	Example	Description
Execute Every	24 hours	How often a rule will be triggered. The rule will be periodically triggered at the configured frequency. Available options: 1 hour, 3 hours, 6 hours, 12 hours, 24 hours.
Resource Scope	All	The region where your resources are deployed. Only resources in the specified region will be evaluated.
Configure Rule Parameters	90	Number of days during which an IAM user has not logged in the system. The default value is 90 . If an IAM user does not log in to the system within the specified period of time, this user is noncompliant.

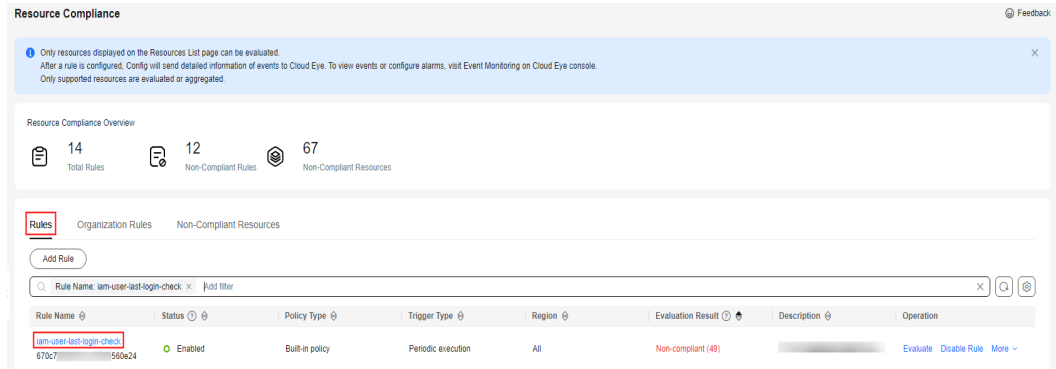
Step 7 On the **Confirm** page, confirm the rule information and click **Submit**.

After you add a rule, the first evaluation is automatically triggered immediately.

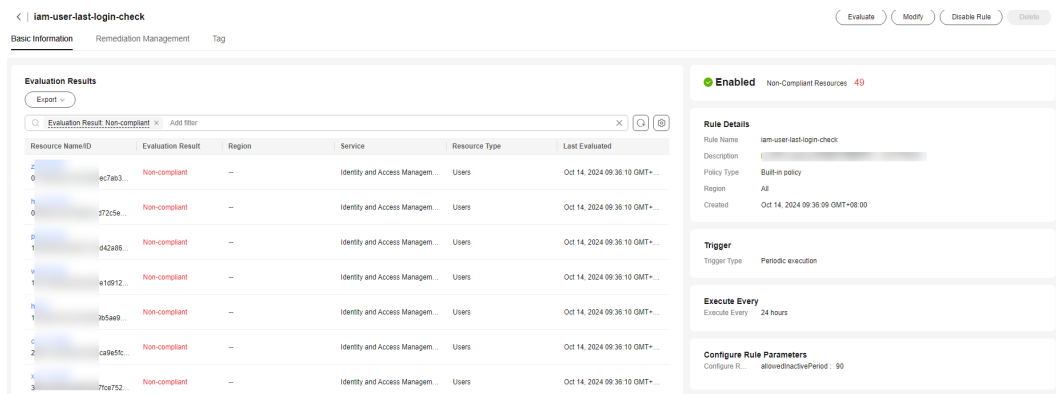
----End

Step 2: View evaluation results.

Step 1 On the **Rules** tab of the **Resource Compliance** page, click the name of the rule that was added in **Step 1**.



Step 2 View evaluation results and rule details on the **Basic Information** tab.



By default, noncompliant resources are displayed. Above the list, you can filter the resources by evaluation result, resource name, and resource ID. You can also export all evaluation results.

IAM users that do not log in to the management console within 90 days are listed as noncompliant users. You can make adjustments on these users as needed.

----End

Related Information

Config also provides the following features to meet your requirements of resource compliance audit:

- **Custom rules:** You can create custom rules with FunctionGraph if built-in policies cannot meet your resource audit requirements.
- **Organization rules:** If you are an organization administrator or a delegated administrator of Config, you can add organization rules, and then the organization rules can apply to all member accounts in your organization.
- **Conformance packages:** A conformance package is a collection of rules. With conformance packages, you can evaluate resource compliance using multiple rules at the same time and centrally query conformance data.