# Config

# Getting Started

**Issue** 01

**Date** 2025-07-01

HUAWEI

**HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.**

## Trademarks and Permissions


and other Huawei trademarks are the property 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 Cloud 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.

# Contents



# 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, .

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

## Procedure

The following steps describe only the mandatory parameters for the resource recorder. Retain the default values for other parameters. For more information about how to configure the resource recorder, see "Configuring the Resource Recorder" in the *Config User Guide*.

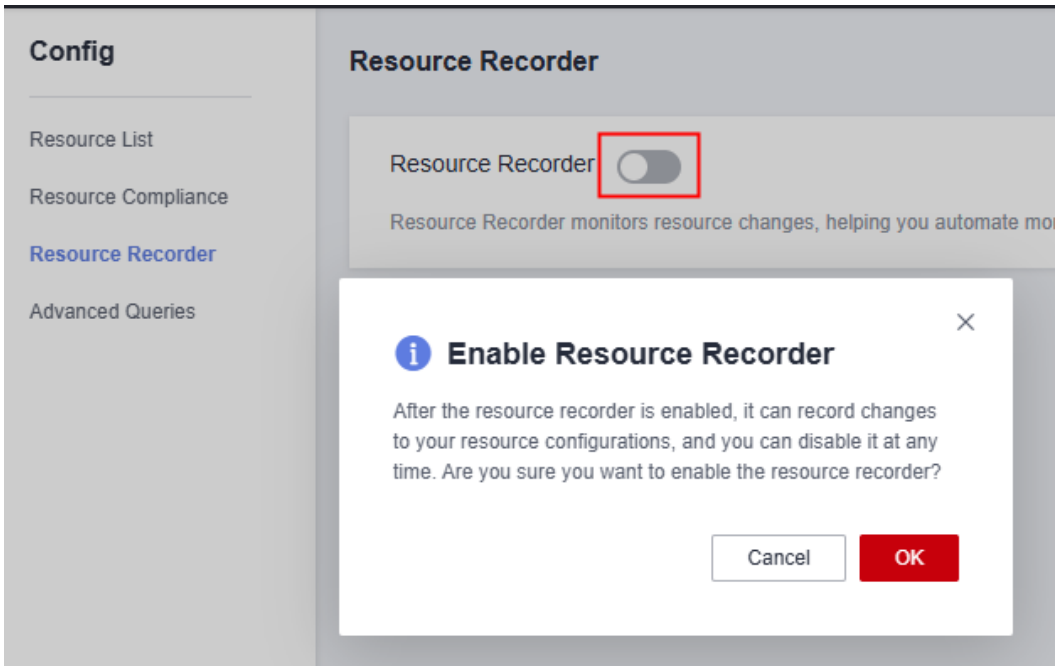
**Step 1** Log in to the management console.

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

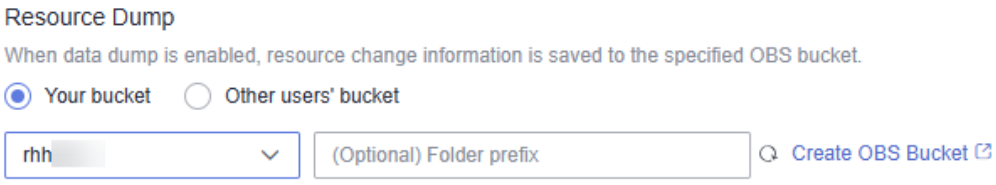
**Step 3** In the navigation pane on the left, choose **Resource Recorder**.

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



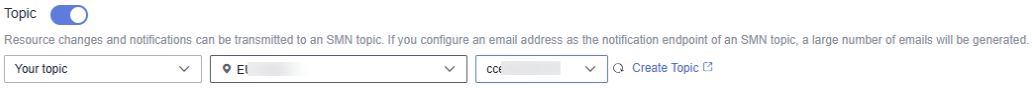

**Step 5** Specify an OBS bucket.




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 the *Object Storage Service User Guide*.

**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 the *Simple Message Notification User Guide*.

**NOTE**

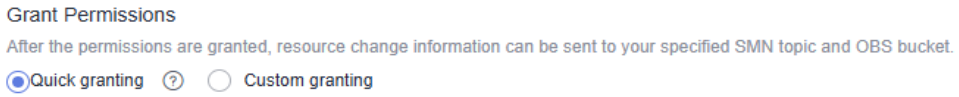
To send notifications with an SMN topic, you not only need to create the topic, but also add subscriptions and request subscription confirmations. For details, see the *Simple Message Notification User Guide*.

**Step 7** Specify a data retention period.


You can select **Seven years (2,557 days)** or customize a period.

**Step 8** Grant permissions.




**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 for writing data into an OBS bucket.

**Step 9** Click **Save**.

**Step 10** In the displayed dialog box, click **OK**.

**----End**

## Related Information

You can modify or disable the resource recorder at any time.

- When configuring the resource recorder, you can select OBS buckets or SMN topics of other accounts. However, you must first use the other accounts to authorize the current account. For details, see "Configuring the Resource Recorder" > "Cross-Account Authorization" in the *Config User Guide*.
- 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. If you want to store resource change messages and resource snapshots in an OBS bucket encrypted using KMS, you will also need the KMS Administrator permission. For details, see "Configuring the Resource Recorder" > "Storing Resource Change Notifications and Resource Snapshots to an Encrypted OBS Bucket" in the *Config User Guide*. For details about how to create an agency, see **Cloud Service Agency**.

# 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.

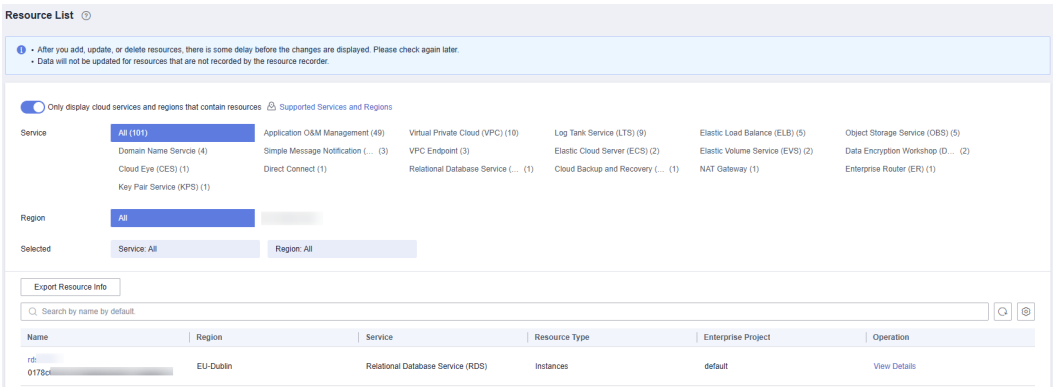
There is a delay in synchronizing data to Config, so if there is a resource change, the change may not be updated in the resource list immediately. If the resource recorder is enabled, Config will update resource changes within 24 hours.

## Procedure

**Step 1** Log in to the management console.

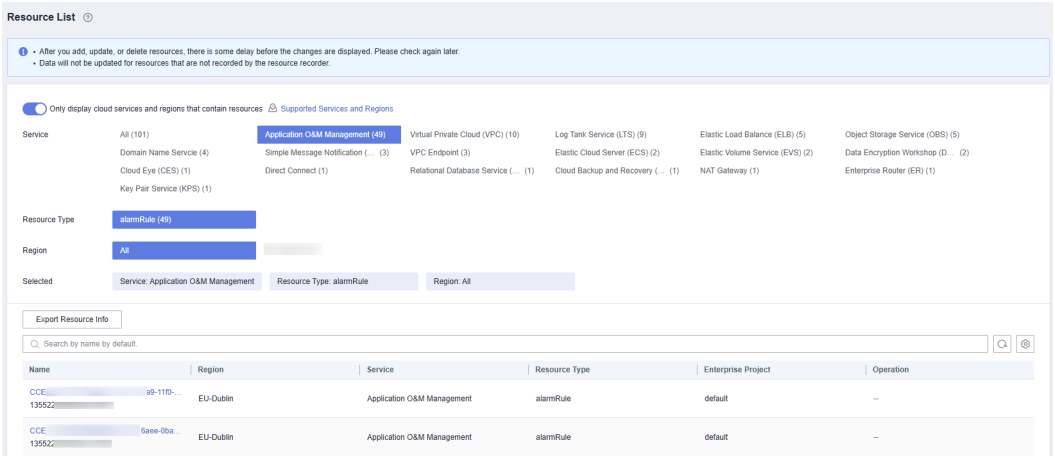
**Step 2** Click ☰ in the upper left corner of the page. Under **Management & Deployment**, select **Config**.

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

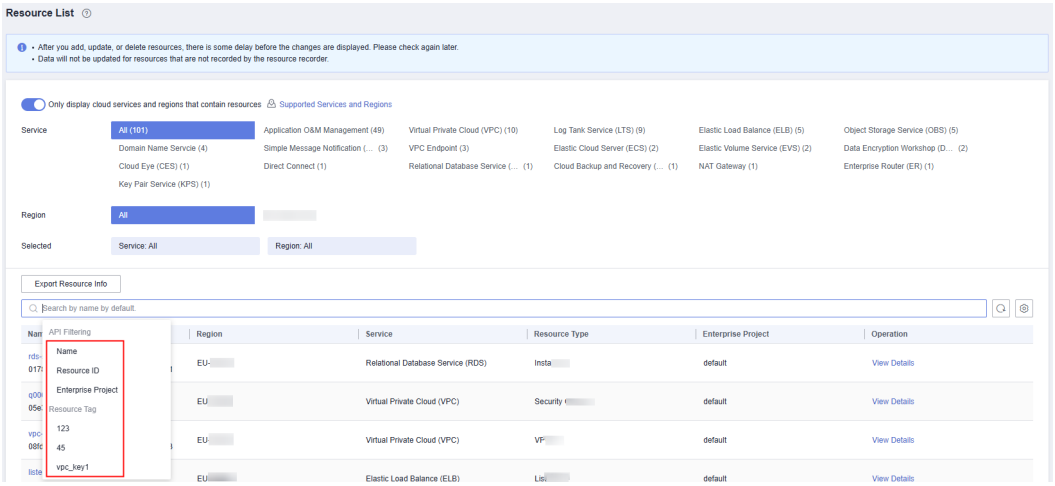



**Step 3** Set filters (service, resource type, and region) to search for resources. For global services, you do not need to set the region.




**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. |
| 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.<br>**NOTE**<br>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 Resource Information**
- "Viewing Resource Compliance Data" in the *Config User Guide*
- **Viewing Resource Relationships**
- "Viewing Resource Changes" in the *Config User Guide*

Config provides the following advanced functions to query resources more accurately. For details, see "Advanced Queries" in the *Config User Guide*.

# 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 for IAM user 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.

## Step 1: Add a Rule

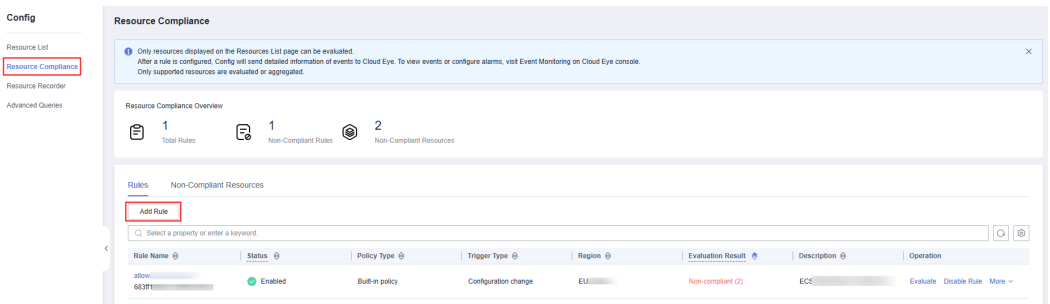
The following steps are only for reference. For details about all the parameters, see section "Adding a Rule Based on a Built-in Policy" in the *Config User Guide*.

**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 & Deployment**, select **Config**.

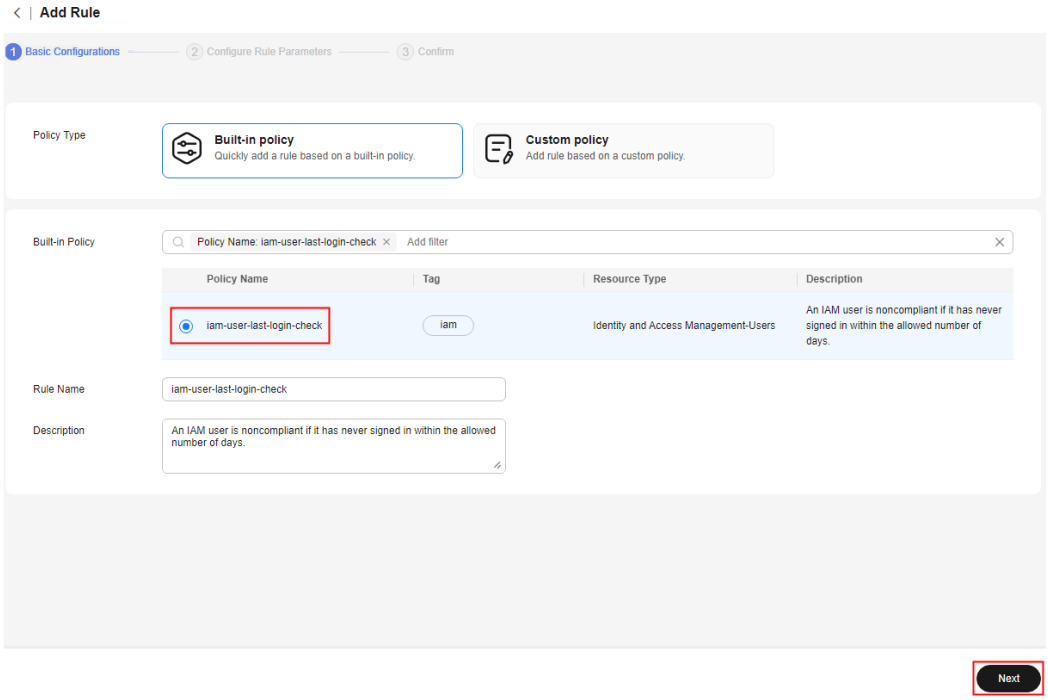
**Step 3** In the navigation pane on the left, choose **Resource Compliance**.

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




**Step 5** On the **Basic Configurations** page, select the built-in policy **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**.

| Parameter | Example | Description |
| --- | --- | --- |
| Execute Every | **24 hours** | How often a rule will be triggered.<br>The rule will be periodically triggered at the configured frequency.<br>Available options: **1 hour**, **3 hours**, **6 hours**, **12 hours**, **24 hours**. |
| Resource Scope | **All** | The region where your resources are deployed.<br>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**.<br>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**.

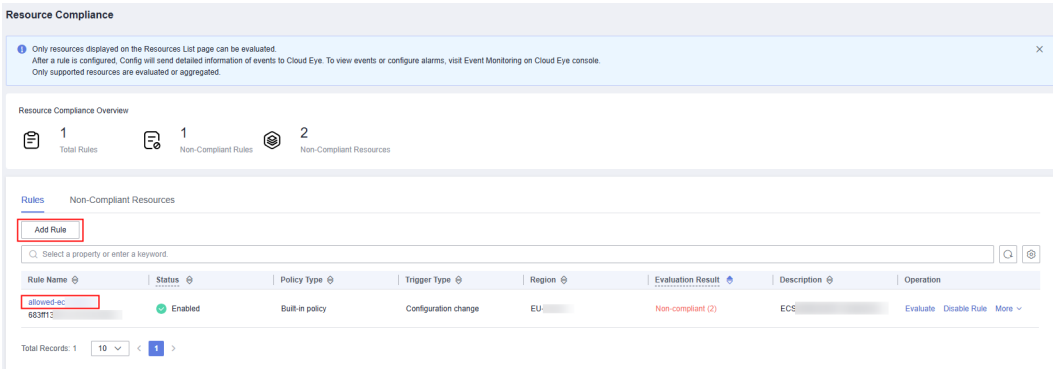
After you add a rule, the first evaluation is automatically triggered immediately.

**----End**

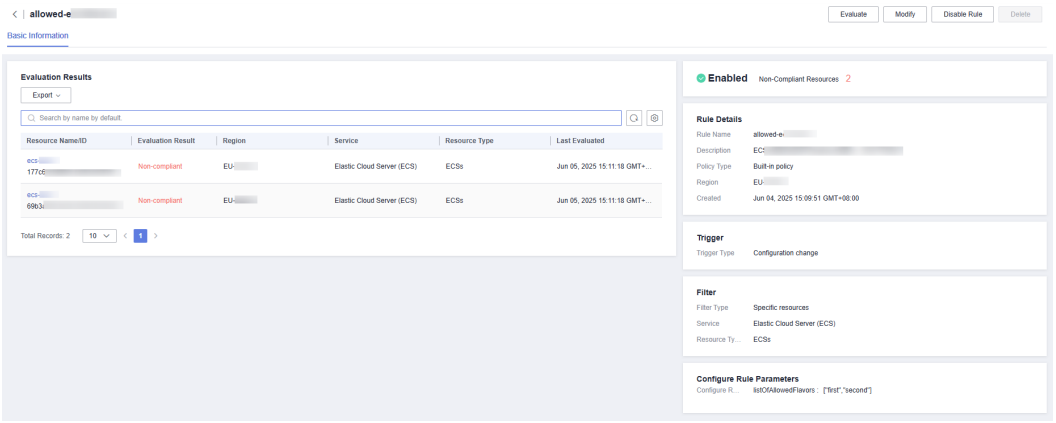
  

## Step 2: View evaluation results.

**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 who 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**