Config

User Guide

Issue	01
Date	2023-12-30

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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 Resource List

1.1 Viewing Resources

1.1.1 Querying All Resources

Scenarios

On the **Resource List** page, you can view all resources from the current account.

NOTE

There is a delay in synchronizing resource data to Config, so if there is a resource change, the change may not be updated in the resource list immediately.

If you have enabled the resource recorder, Config updates resource data within 24 hours after a change is made to a resource. If the resource recorder remains disabled, Config periodically corrects the resource data based on your activities. Resource historical information and message content will also be collectively updated.

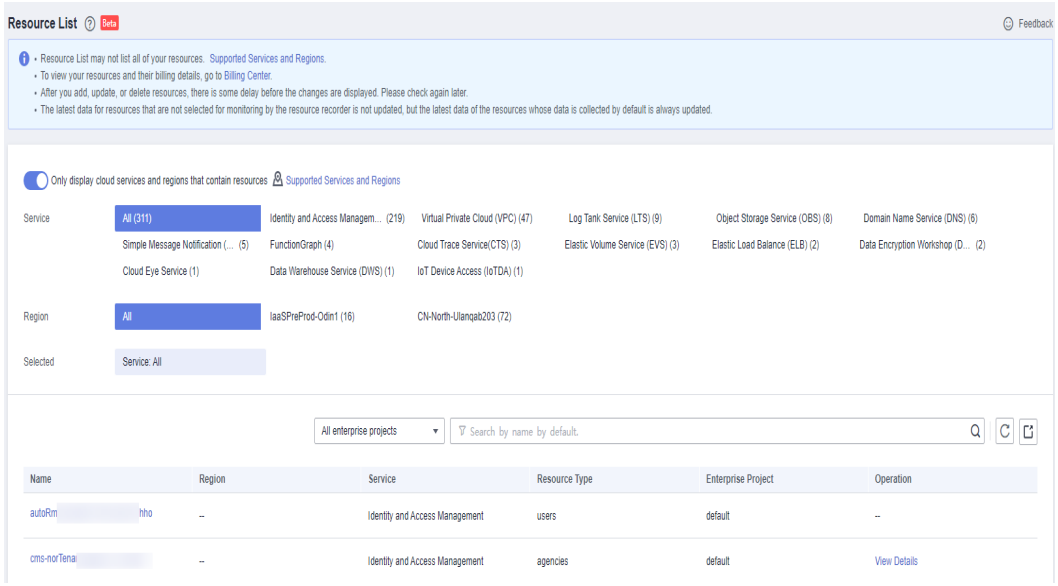
Procedure

Step 1 Log in to the management console.

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

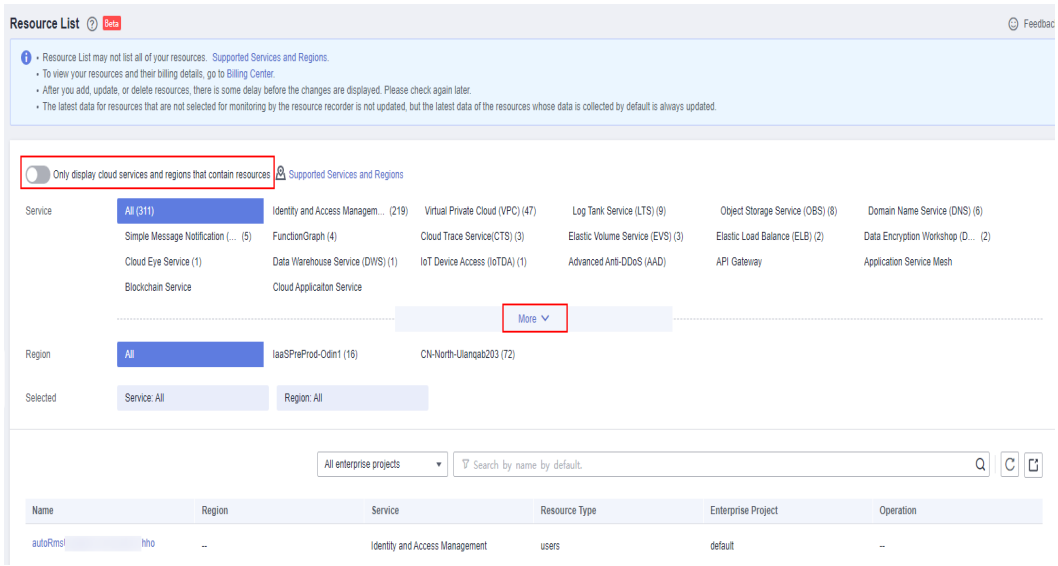
By default, your services that contain resources are displayed in the **Service** area, and all your resources are displayed in the list.

Figure 1-1 Resource List



Step 3 To view all services supported by Config, disable **Only display cloud services and regions that contain resources**.

Figure 1-2 Viewing all supported services



Step 4 To view all supported services and regions, click **Supported Services and Regions**.

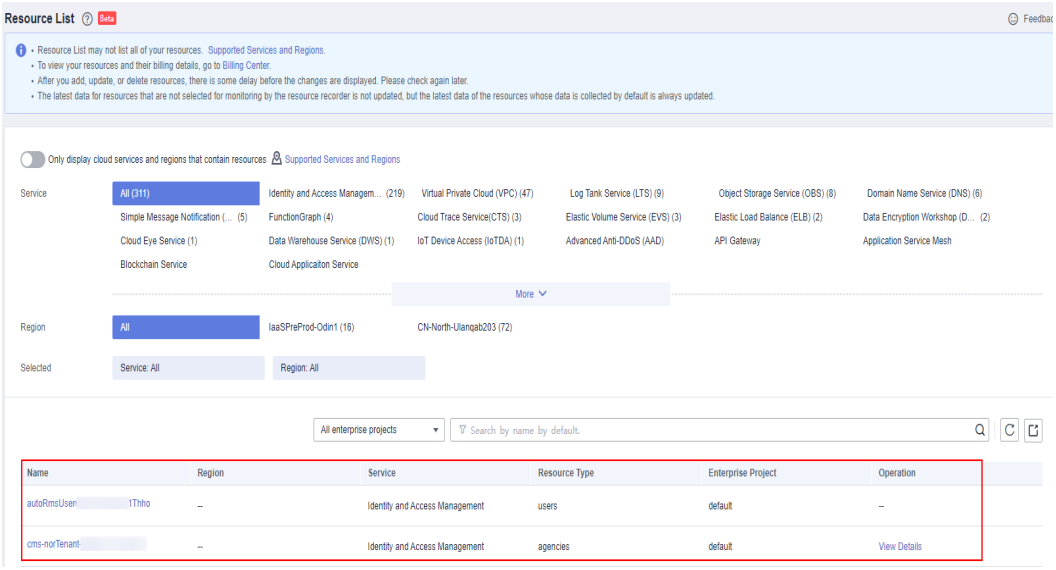
----End

1.1.2 Querying Details About a Resource

Scenarios

By default, the **Resource List** page only displays part of resource attributes. You can perform the following procedure to view more resource details.

Figure 1-3 Resource List



Procedure

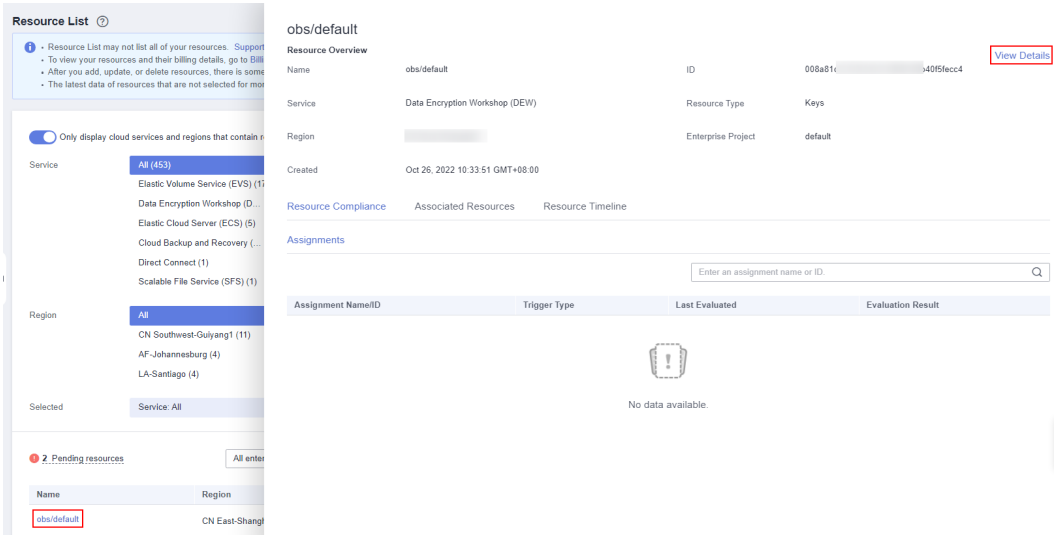
Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

Step 3 Click a resource name to view more details.

Resource overview, resource compliance, associated resources, and the resource timeline are displayed.

Figure 1-4 Resource overview



Step 4 Click **View Details** in the upper right corner of the **Resource Overview** area to go to the console of the corresponding cloud service and view resource details.

Alternatively, in the resource list, click **View Details** in the **Operation** column to view resource details.

----End

1.1.3 Filtering Resources

Scenarios

You can filter resources by service, resource type, or region on the Resource List page. You can also directly enter more specific resource information to quickly search for resources.

This section describes how to quickly search for your resources.

Supported Filter Criteria

Table 1-1 Supported filter criteria

Filter Criteria	Description
Name	Enter a name in the search box for a fuzzy search. The resource name is case-insensitive.
Resource ID	Enter a resource ID in the search box for a fuzzy search. The resource ID is case-sensitive.
Tags	If you select **Tags** as a search criterion, **Tag key** and **Tag value** are displayed in sequence, and you need to select a tag key and value.
Enterprise Project	Select an enterprise project from the drop-down list. Resources in the enterprise project are automatically displayed in the resource list.

NOTE

You need to **enable Enterprise Center** before filtering resources by enterprise project.

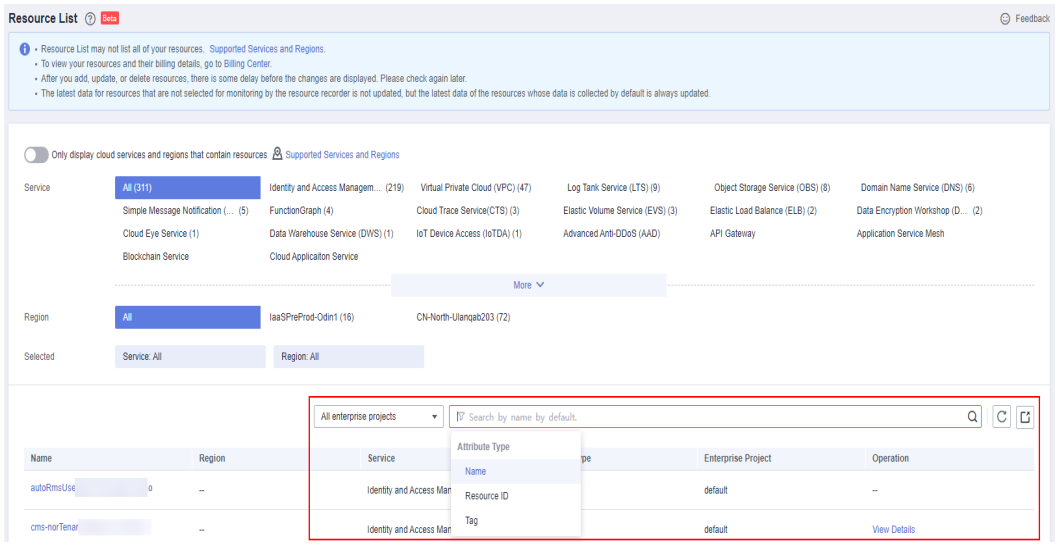
Procedure

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

Step 3 Enter an enterprise project, a resource name, a resource ID, or a tag in the middle search box.

Figure 1-5 Filtering resources



Step 4 Click .

----End

1.1.4 Exporting Resource Information

Scenarios

You can export the resource list on the Resource List page.

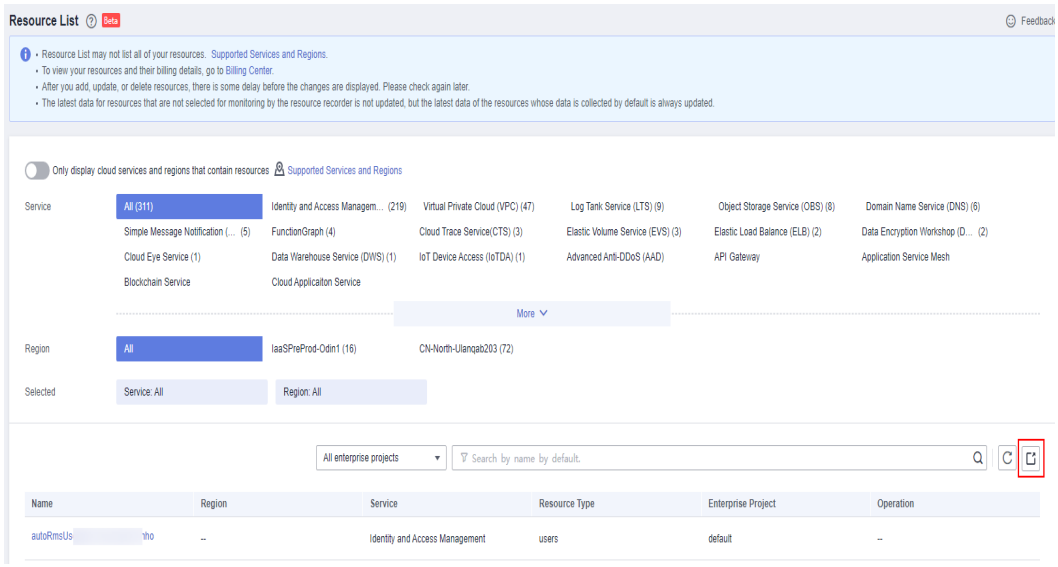
Procedure

Step 1 Log in to the management console.

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

Step 3 Filter resources and click to export the resource list.

Figure 1-6 Exporting resource information



----End

NOTE

The exported list contains all filtered resources.

1.2 Viewing Resource Compliance Data

Scenarios

Config provides you with rules to evaluate resources. You can view compliance data of the resources evaluated in the resource overview page.

Procedure

Step 1 Log in to the management console.

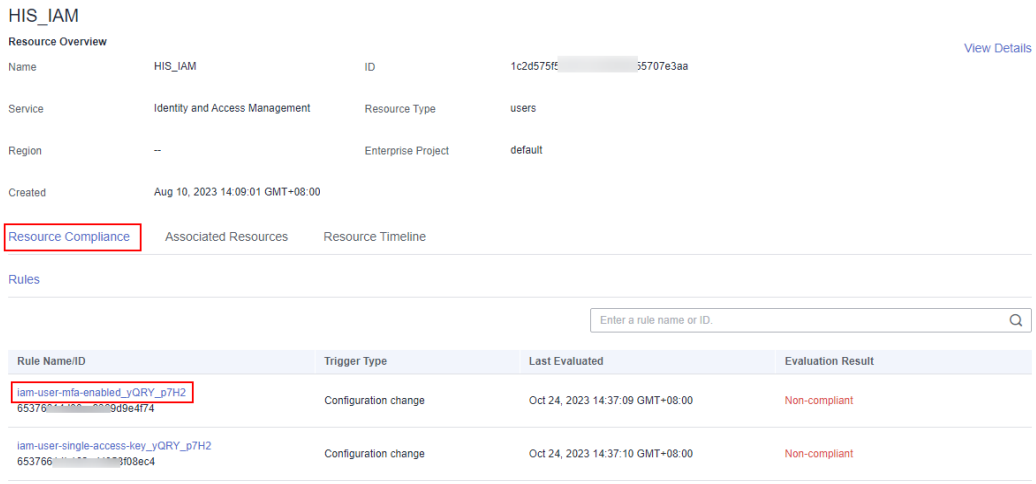
Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

Step 3 On the **Resource List** page, click the name of a target resource.

Step 4 The **Resource Compliance** tab is displayed by default. The rules applied and the evaluation results are displayed in a list in the **Resource Compliance** tab.

Step 5 Click a rule name in the rule list to see rule details.

Figure 1-7 Viewing resource compliance data



----End

1.3 Viewing Resource Relationships

Scenarios

You can gain insights into various relationships between your resources. For example, a resource relation ship may be described as that an EVS disk is attached to an ECS or an ECS is deployed in a VPC. In this way, you have a clear view of resource dependencies.

For details, see **Relationships with Supported Resources**.

Procedure

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

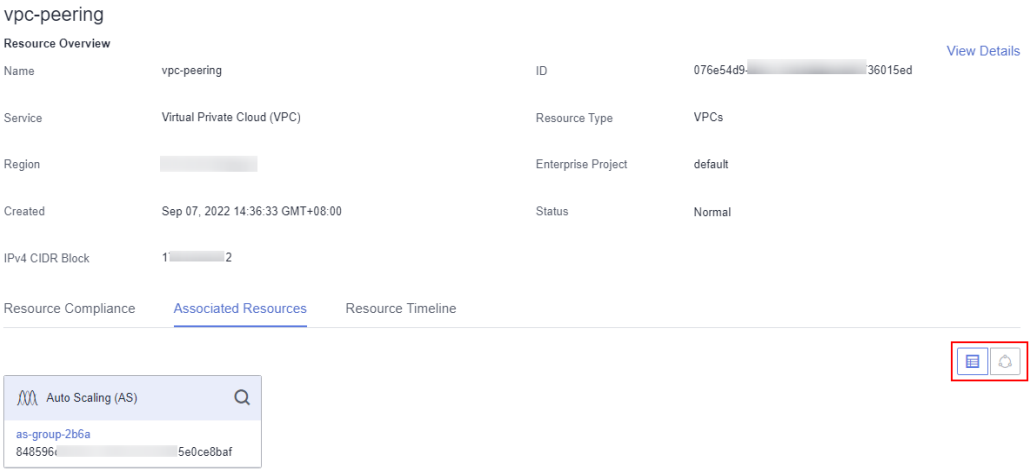
Step 3 On the **Resource List** page, click the name of a target resource.

Step 4 Click the **Associated Resources**tab.

Hover over a resource name to view related resource information and resource relationships.

Step 5 In the upper right corner of the **Associated Resources** tab, you can switch to display resource relationships in a list or topology view.

Figure 1-8 Viewing associated resources



----End

NOTE

If you click a resource name on the **Associated Resources** tab, **Resource Overview** is displayed by default.

1.4 Viewing Resource Changes

Prerequisites

Resource changes are recorded only after the resource recorder is enabled. For details about the resource recorder, see **Resource Recorder**.

Scenarios

You can view resource changes over a time period. Any attribute or relationship changes made to a resource are recorded in a resource timeline and the records are retained for seven years by default.

Procedure

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

Step 3 On the **Resource List** page, click the name of a target resource.

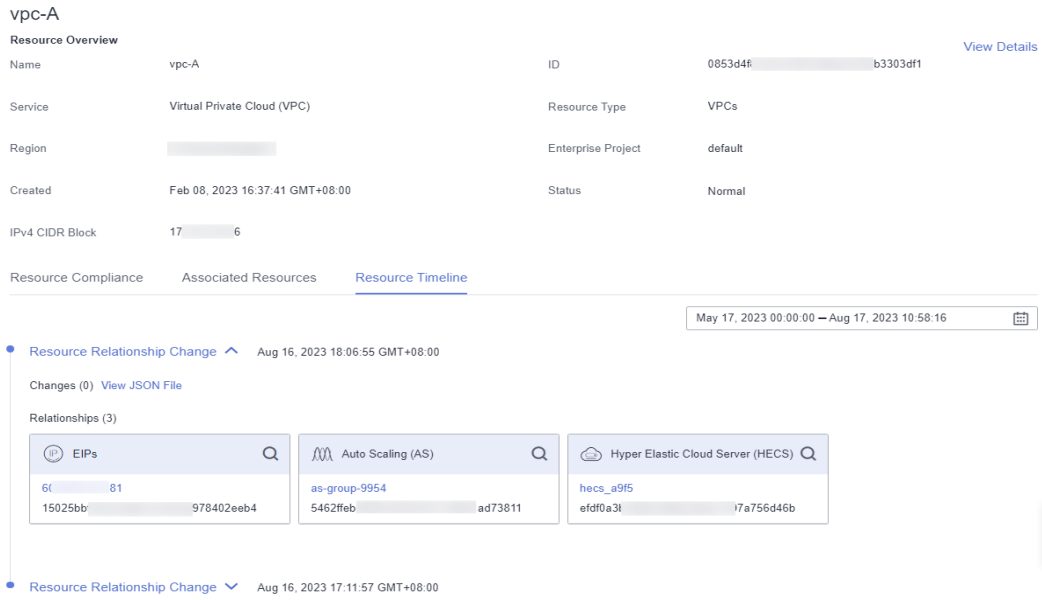
Step 4 Choose the **Resource Timeline** tab to view the resource changes.

Step 5 In the upper right corner of the **Resource Timeline** tab, set a time range to filter records.

By default, resource changes of the latest three months are displayed.

You can click **View JSON File** to view all resource attributes.

Figure 1-9 Resource timeline



----End

2 Resource Recorder

2.1 Overview

Introduction

The resource recorder automatically detect and records changes made to your resources. It helps you easily monitor resource changes.

To be specific, the resource recorder

- Notifies you when resources are created, modified, or deleted.
- Notifies you when resource relationships are changed.
- Stores resource change notifications every 6 hours.
- Stores resource snapshots every 24 hours.

For details about resources that can be tracked by the resource recorder, see **Services and Regions Supported by Config**.

For details about resource relationships that can be tracked by the resource recorder, see **Relationships with Supported Resources**.

Notes and Constraints

- When enabling and configuring the resource recorder, you must configure **Topic** or**Resource Dump**.
- When you configure **Topic**, if you select a topic in a region but do not add a subscription, you cannot receive a message when resources change.
- The resource recorder only updates data for specified resources.

2.2 Configuring the Resource Recorder

Scenarios

You must enable the resource recorder before Config can track your resource configurations.

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

NOTE

To enable, configure, or modify the resource recorder, you need required permissions. For details about Config permissions, see **Permissions Management**.

This section includes the following content:

- **Enabling the Resource Recorder**
- **Modifying the Resource Recorder**
- **Disabling the resource recorder**
- **Cross-Account Authorization**
- **Storing Resource Change Messages and Resource Snapshots to an Encrypted OBS Bucket**

Enabling the Resource Recorder

After the resource recorder is enabled, you will be notified of any resource changes (creations, modifications, deletions, or relationship changes) and have your notifications and resource snapshots stored periodically.

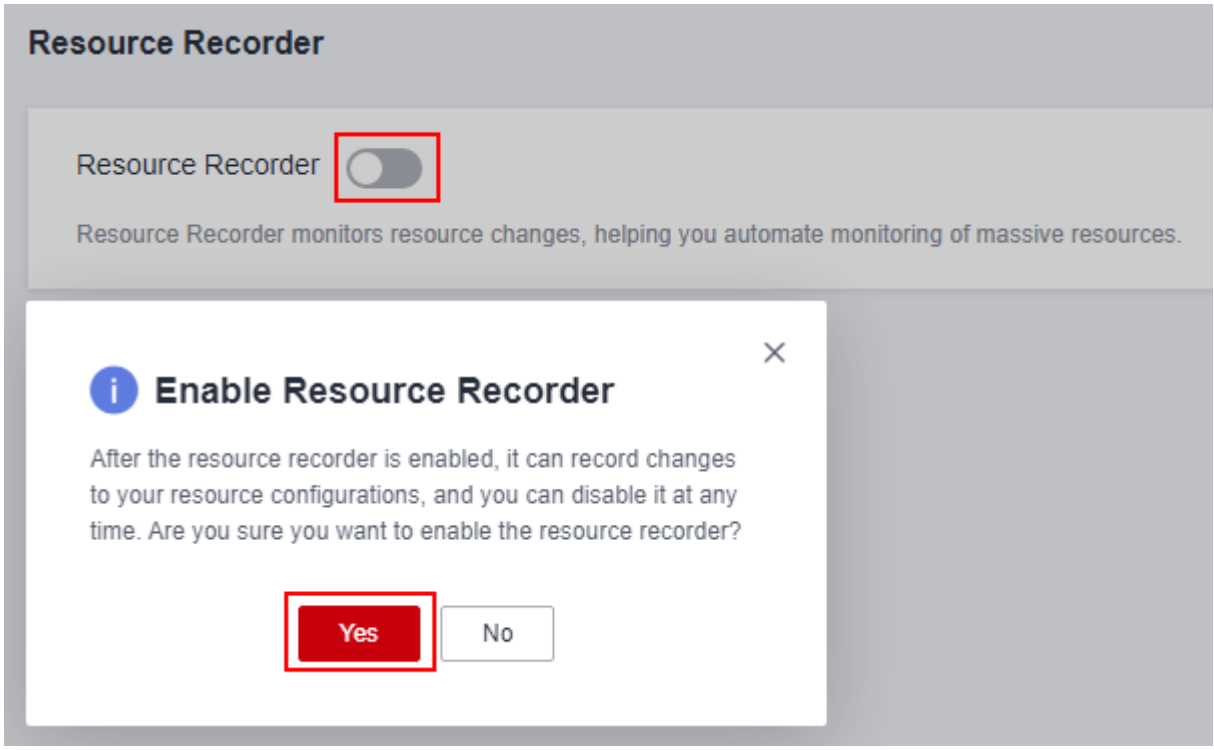
Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

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

Step 4 Toggle on the resource recorder. In the dialog box, click Yes.

Figure 2-1 Enabling the resource recorder



Step 5 Select the monitoring scope.

By default, the resource recorder records all supported resources. You can specify a resource scope for the resource recorder.

Step 6 Specify an OBS bucket.

Specify an OBS bucket to store notifications of resource changes and resource snapshots. If no OBS bucket is available, create one. For details about how to create an OBS bucket, see ***Object Storage Service User Guide***.

- **Select an OBS bucket from the current account**:

  Click **Your bucket**. If the OBS bucket name has a prefix, you need to enter the prefix. If no OBS buckets are available of the current account, create one. For details about how to create an OBS bucket, see ***Object Storage Service User Guide***.

- **Select an OBS bucket from another account**:

  Select **Other users' bucket**, then configure **Region ID** and **Bucket Name**. If the OBS bucket name has a prefix, you need to enter the prefix. If you select a bucket from another account, you need required permissions granted by the account. For details, see **Cross-Account Authorization**.

NOTE

After you have specified an OBS bucket, Config writes an empty file named **ConfigWritabilityCheckFile** to the OBS bucket to verify whether resources can be written to the OBS bucket.

Step 7 Select an SMN topic.

Toggle on **Topic**, then select a region and an SMN topic for receiving notifications of resource changes. If no SMN topics are available, create one. For details about how to create an SMN topic, see ***Simple Message Notification User Guide***.

- **Select a topic from the current account**:

  Select **Your topic**, then select a region and an SMN topic. If no SMN topics are available, create one. For details about how to create an SMN topic, see ***Simple Message Notification User Guide***.

- **Select a topic from another account.**

  Select **Topic under other account**, then enter a topic URN. If you select a topic from another account, you need required permissions granted by the account. For details, see **Cross-Account Authorization**.

NOTE

After you create a topic, you must add subscriptions to the topic and confirm the subscriptions. For details, see ***Simple Message Notification User Guide***.

Step 8 Grant permissions.

- **Quick granting**: This option will automatically create an agency named **rms_tracker_agency** to grant the required permissions for the resource recorder to work properly. The agency contain permissions, such as the **SMN Administrator** and the **OBS OperateAccess** permissions, for sending notifications using an SMN topic and for writing data into an OBS bucket. The agency created by **quick granting** doesn't contain KMS permissions. So, the resource recorder is unable to store resource change messages and resource

snapshots to an OBS bucket encrypted using KMS. If you need to do so, you can add the **KMS Administrator** permission to the agency or use custom authorization. For details, see **Storing Resource Change Messages and Resource Snapshots to an Encrypted OBS Bucket**.

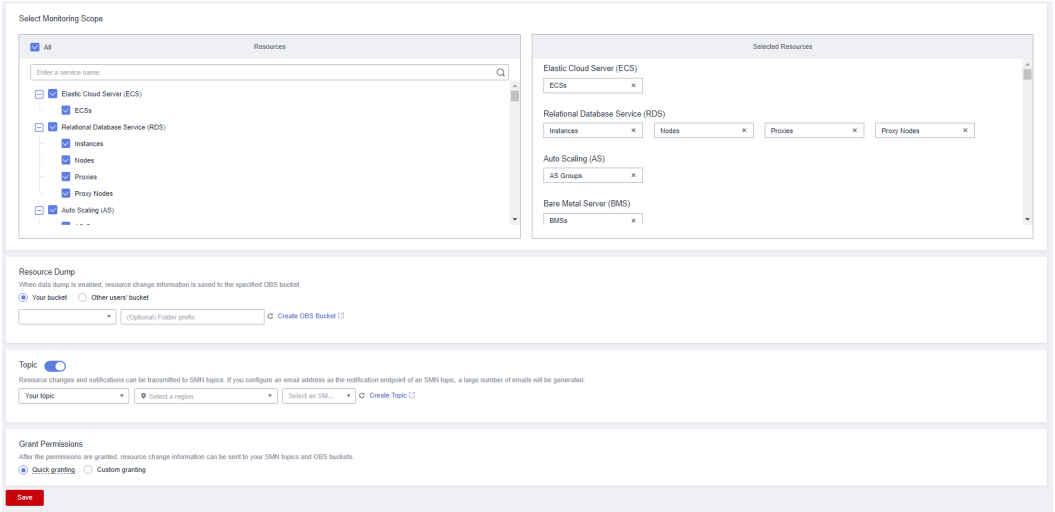
- **Custom granting**: You can create an agency using IAM to customize authorization for RMS. The agency must include permissions for sending notifications using an SMN topic and for writing data into an OBS bucket. To store resource change messages and resource snapshots to an OBS bucket encrypted using KMS, you need the **KMS Administrator** permission. For details, see **Storing Resource Change Messages and Resource Snapshots to an Encrypted OBS Bucket**. For details about how to create an agency, see **Identity and Access Management User Guide**.

  NOTE

  This agency grants Config related SMN and OBS permissions that are required for sending resource change notifications using an SMN topic and storing resource snapshots into an OBS bucket.

Step 9 Click **Save**.

Figure 2-2 Configuring the resource recorder



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

----End

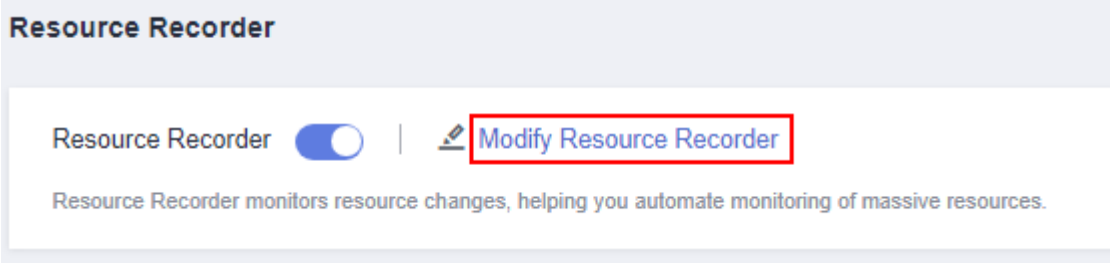
Modifying the Resource Recorder

You can modify the resource recorder at any time.

Step 1 In the left navigation, choose **Resource Recorder**.

Step 2 Click **Modify Resource Recorder**.

Figure 2-3 Modifying the resource recorder



Step 3 Modify configurations.

Step 4 Click **Save**.

Step 5 In the displayed dialog box, click **Yes**.

----End

Disabling the resource recorder

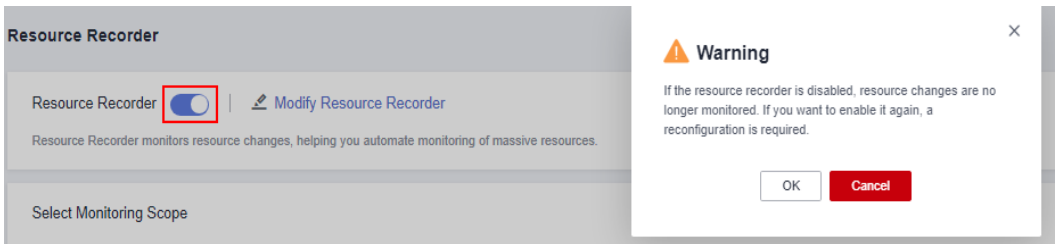
You can disable the resource recorder at any time.

Step 1 In the left navigation, choose **Resource Recorder**.

Step 2 Toggle off the resource recorder.

Step 3 In the displayed dialog box, click **OK**.

Figure 2-4 Disabling the resource recorder



----End

Cross-Account Authorization

- **Granting SMN topic permissions to another account**
  a. Sign in to the management console using the account which owns the topic and go to the SMN console.
  b. To grant accounts related SMN permissions, see **Configuring Topic Policies**.
- **Granting OBS bucket permissions to another account**
  a. Sign in to the Huawei Cloud console and go to the OBS console.
  b. To grant accounts related OBS permissions, see **Creating a Custom Bucket Policy (JSON View)**.
  Add the following bucket policy:

```
{
  "Statement": [
```



```
    {
        "Sid": "org-bucket-policy",
        "Effect": "Allow",
        "Principal": {
            "ID": [
                "domain/account ID:agency/rms_tracker_agency"  //account ID indicates the
domain ID of the account to be authorized. rms_tracker_agency indicates the name of the
agency to be authorized.
            ]
        },
        "Action": [
            "PutObject"
        ],
        "Resource": [
            "targetBucketName/RMSLogs/*/Snapshot/*",
            "targetBucketName/RMSLogs/*/Notification/*"
        ]
    }
  ]
}
```

NOTE

You need to set **Principal** to the agency required for enabling the resource recorder. Set **Resource** to the path where the resource recorder dumped files. If the OBS bucket name has a prefix, include the prefix. Set **Action** to **PutObject**.

Storing Resource Change Messages and Resource Snapshots to an Encrypted OBS Bucket

- **Encrypting an OBS bucket using SSE-OBS**

  If you need to store resource change messages and snapshots to an OBS bucket encrypted using SSE-OBS, you only need to select the corresponding OBS bucket and no other operations are required.

- **Encrypting an OBS bucket using a default key of SSE-KMS**

  If you need to store resource change messages and snapshots to an OBS bucket encrypted using a default key of SSE-KMS, you need to add the **KMS Administrator** permission to the agency assigned to the resource recorder.

- **Encrypting an OBS bucket using a custom key of SSE-KMS**

  If you need to store resource change messages and snapshots to an OBS bucket that is from the current account and that is encrypted using a custom key of SSE-KMS, you need to add the **KMS Administrator** permission to the agency assigned to the resource recorder.

  If you need to store resource change messages and snapshots to an OBS bucket that is from another account, and that is encrypted using a custom key of SSE-KMS, you need to add the **KMS Administrator** permission to the agency assigned to the resource recorder, and set the cross-account permission for the key at the same time. The procedure is as follows:

  a. Sign in to the Data Encryption Workshop (DEW) console and go to the Key Management Service page.

  b. In the Custom Keys tab, click the alias of a target key to go to its details page and create a grant on it.

  c. Grant the account the permission for using the key based on **Creating a Grant**.

     - Select **Account** for **User or Account** and enter an account ID.

- Select **Create Data Key** for **Granted Operations**.

2.3 Notifications

Notifications of any changes to your resources will be sent to the SMN topic subscriber after you enable the resource recorder and configure the SMN topic. If no topics are available, you need to create a topic, add subscriptions to the topic, and request confirmation for the subscriptions.

For details about how to use SMN, see ***Simple Message Notification User Guide***.

Config uses SMN to send notifications of:

- Resource changes (creation, modification, and deletion)
- Resource relationship changes
- Resource change notification storage completed
- Resource snapshot storage completed

For details about example codes for resource change notifications, see **Message Notification Models**.

2.4 Storing Resources

Your resource snapshots will be stored into the OBS bucket every 24 hours after you enable the resource recorder.

For details about example code for storing resources, see **Resource Storage Models**.

2.5 Storing Resource Change Messages

After you enable the resource recorder and specify an SMN topic (create a topic, add a subscription, and request confirmation) and an OBS bucket, Config stores your resource change messages to the OBS bucket every 6 hours.

For details about example code for storing resource change messages, see **Models of Resource Change Notification Storage**.

3 Resource Compliance

3.1 Rule

3.1.1 Adding Predefined Rules

Scenarios

You can create a rule to evaluate the compliance of your resources. When you creat a rule, you need to select a built-in policy or custom policy, specify the resources to be evaluated, and specify the trigger type.

This section describes how to add predefined rules.

Constraints and Limitations

You can add up to 500 rules for one account.

Procedure

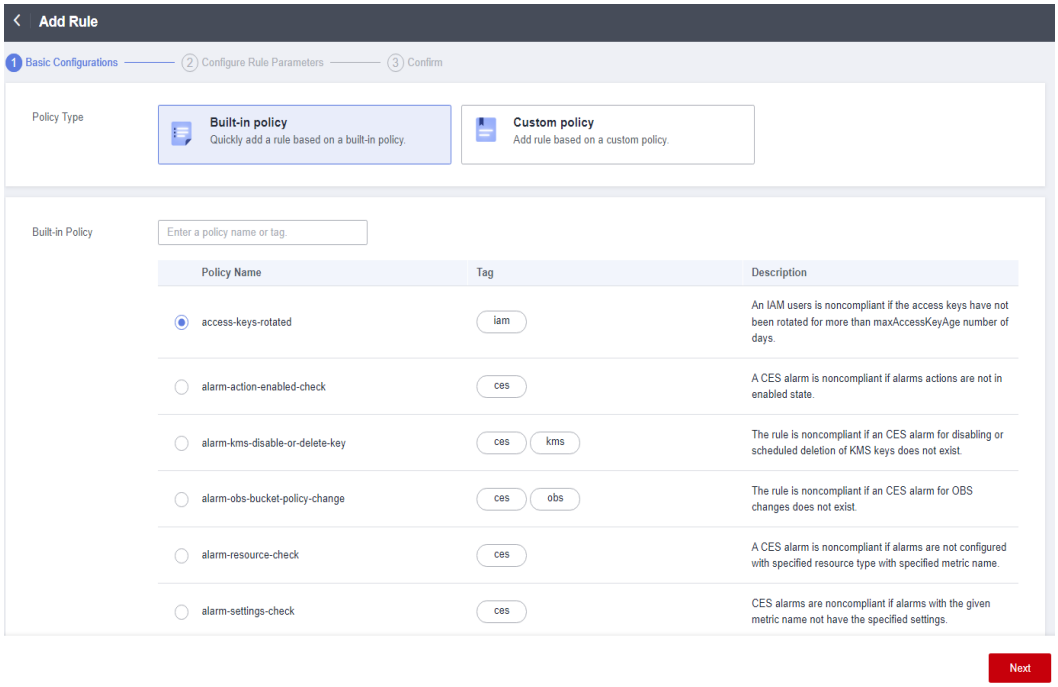
Step 1 Log in to the management console.

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

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

Step 4 In the middle of the page, click **Add Rule**. On the displayed **Configure Basic Details** page, select a policy, specify **Rule Name** and **Description**, and click **Next**.

Figure 3-1 Configuring basic details



For details about parameter settings, see **Table 3-1**.

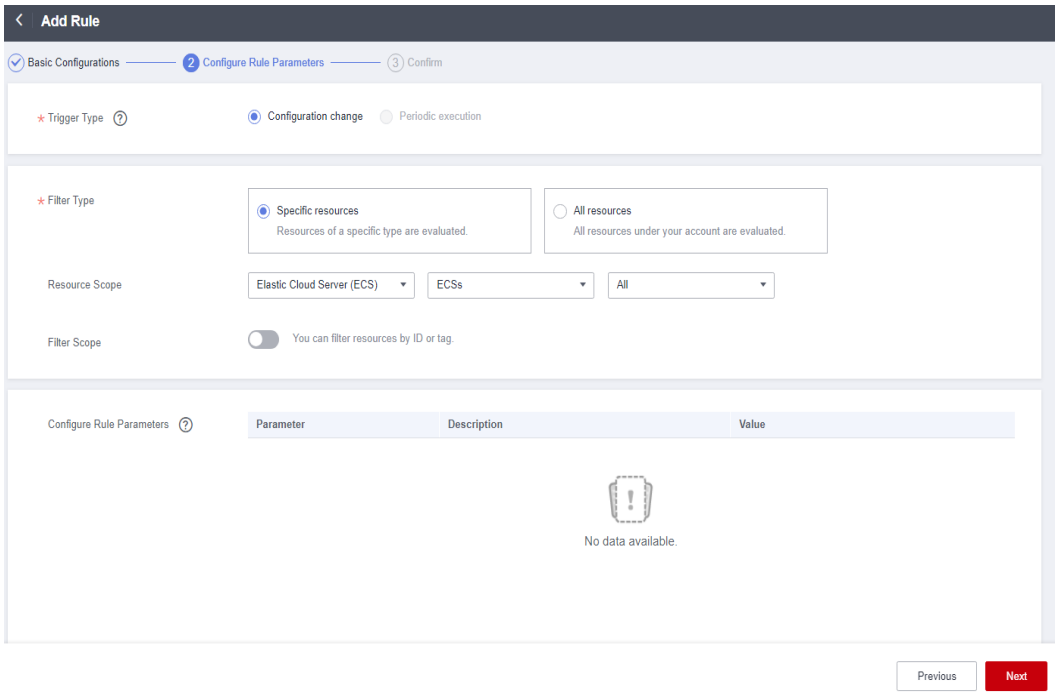
Table 3-1 Basic configuration parameters

Parameter	Description
Policy Type	Possible values are: • **Built-in policy** • **Custom policy**
Built-in Policy	Specifies the policy that has been developed for a service. You can use built-in policies to quickly add rules. For details, see **Predefined Policies**.
Custom Policy	Config allows you to create custom policies to add rules. For details, see **Example Custom Policies**.
Rule Name	By default, the predefined policy name is reused as the rule name. A rule name must be unique. The rule name can contain only digits, letters, underscores (_), and hyphens (-).
Description	By default, the rule description is the same as the selected predefined policy description. You can also customize the rule description. There are no restrictions on the rule description.

Parameter	Description
FunctionGraph Function	Specifies the URN of the FunctionGraph function in the custom policy. For details about how to create a FunctionGraph function, see **Creating a FunctionGraph Function for a Config Custom Policy**. This parameter is mandatory only when **Policy Type** is set to **Custom policy**.
Grant Permissions	This agency grants Config the read-only and call permissions of FunctionGraph. These permissions allow you to customize rules to query FunctionGraph or send events to FunctionGraph. This parameter is mandatory only when **Policy Type** is set to **Custom policy**. **NOTE** • **Quick granting**: This option will automatically create an agency named **rms_custom_policy_agency** to grant the permissions required for the customized rule to work properly. The permissions include the read-only and call permissions for FunctionGraph. • **Custom granting**: This option allows you to create an agency and assign permissions in IAM. The permissions assigned must include the read-only and call permissions of FunctionGraph. For details about how to create an agency, see ***Identity and Access Management User Guide***.

Step 5 On the displayed **Configure Rule Parameters** page, configure required parameters and click **Next**.

Figure 3-2 Configure Rule Parameters



For details about parameter settings, see **Table 3-2**.

Table 3-2 Parameter descriptions

Parameter	Description
Trigger Type	Specifies the conditions under which rules are triggered. Possible values are: • **Configuration change**: The rule is triggered when a specific cloud resource is changed. • **Periodic execution**: The rule is triggered at a specific frequency.
Filter Type	Specifies the resources to be evaluated. Possible types are: • **Specific resources**: Resources of a specific type will be evaluated. • **All resources**: All resources from your account will be evaluated. This parameter is mandatory only when **Trigger Type** is set to **Configuration change**.
Resource Scope	If you set **Filter Type** to **Specific resources**, you need to specify a resource scope. • Service: Select the service the resource belongs to. • Resource type: Select the resource type of the corresponding service. • Region: Select the region where the resource is located. This parameter is mandatory only when **Trigger Type** is set to **Configuration change**.
Filter Scope	After you enable **Filter Scope**, you can filter resources by resource ID or tag. You can specify a specific resource for compliance evaluation. This parameter is mandatory only when **Trigger Type** is set to **Configuration change**.
Execute Every	Indicates how often a rule is triggered. This parameter is mandatory only when **Trigger Type** is set to **Periodic execution**.

Parameter	Description
Configure Rule Parameters	Specifies the parameter configuration for the built-in policy or custom policy you selected in step **Configure Basic Details**. For example, if you select policy **required-tag-check** and **Keywords** is **tag**, you need to specify a tag key and a tag value here. Then, resources that do not have this tag are non-compliant. Not all built-in policies have parameters to be configured. For example, if you select policy **volumes-encrypted-check**, you do not need to configure any rule parameters. You can set up to 10 rule parameters for a custom policy.

Step 6 On the **Confirm** page displayed, confirm the rule information and click **Submit**.

Figure 3-3 Confirm

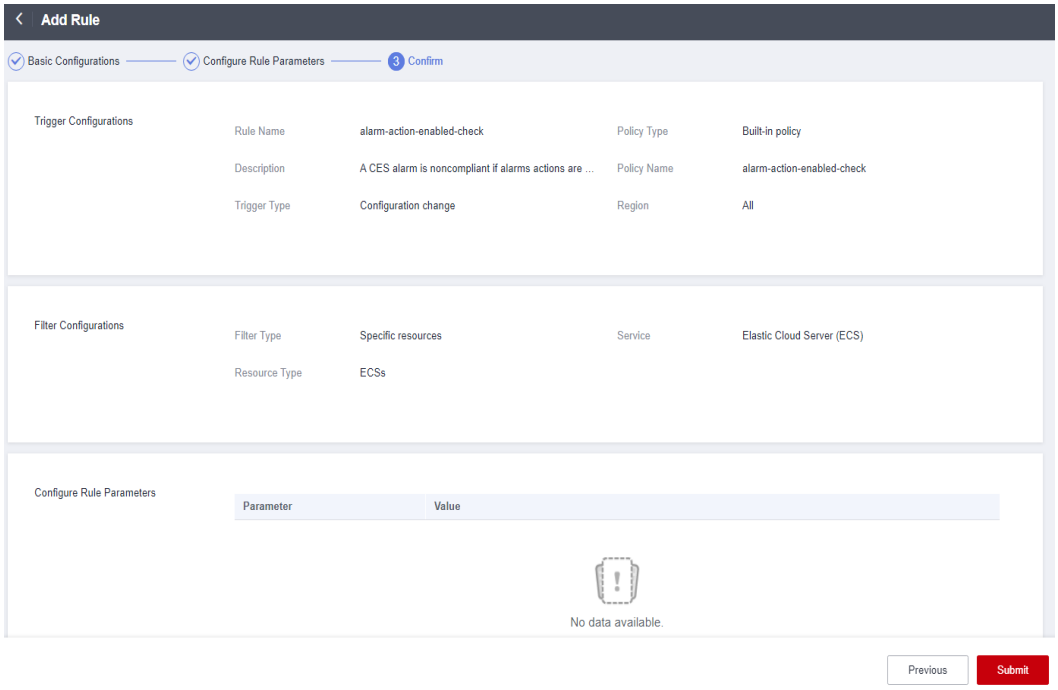
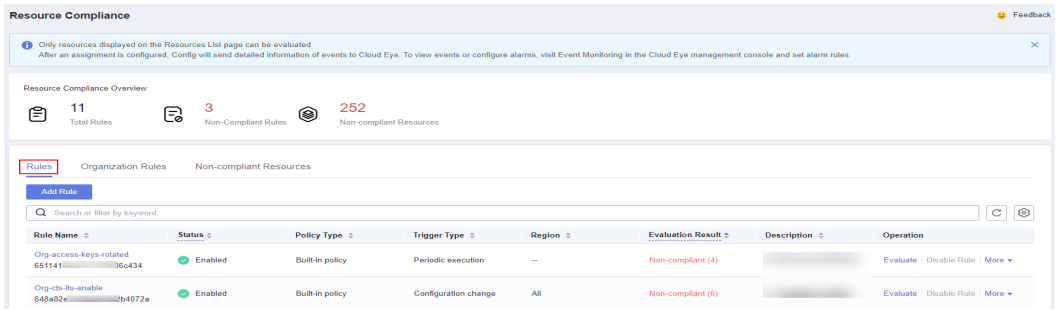


Figure 3-4 Querying a rule



NOTE

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

----End

3.1.2 Adding a Custom Rule

Scenario

You can create custom rules to supplement predefined rules.

To create a custom rule, you need to use **FunctionGraph**. You associate each custom rule with a Function Graph function, then the function collects rule parameters and resource attributes and evaluates whether your resources comply with the rule. The function is invoked either in response to configuration changes or periodically. For details about how to use FunctionGraph, see **FunctionGraph User Guide**.

This section describes how to create a custom rule by following steps:

1. **Creating a function using FunctionGraph**
2. **Adding a Custom Rule**

Creating a function using FunctionGraph

Step 1 Sign in to the **FunctionGraph** console. In the left navigation, choose **Functions** > **Function List**.

Step 2 In the upper right corner, click **Create Function**. The **Create from scratch** tab is displayed by default.

Step 3 Set **Function Type** to **Event Function** and configure the required IAM agency. They agency grants the function required permissions, including **rms:policyStates:update**.

Step 4 Click **Create Function** and then on the **Code** tab, configure the code.

Step 5 Click **Deploy**.

For details about example code, see **Example Functions (Python)**.

Step 6 Click **Configurations**, modify **Execution Timeout (s)** and **Memory (MB)** in the **Basic Settings** area as required. Configure **Concurrency**.

Step 7 Click **Save**.

For details, see **Creating an Event Function**.

----End

Adding a Custom Rule

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

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

Step 4 Click **Add Rule** in the middle of the page.

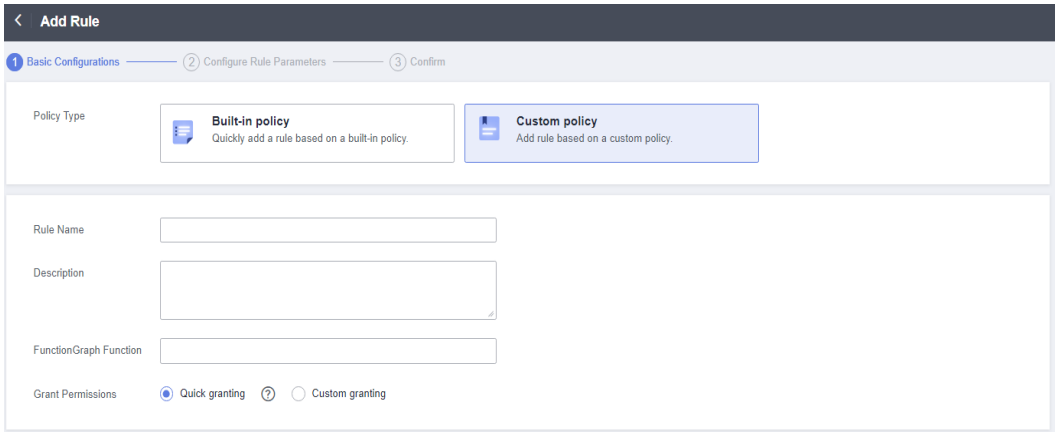
Step 5 Set **Policy Type** to **Custom Policy**. Set related parameters, select **Quick granting** or **Custom granting** to grant permissions, and click **Next**.

- **Quick granting**: Quick granting quickly grants you permissions of the rms_custom_policy_agency agency. The permissions ensure proper functioning of a custom policy, including the permissions for obtaining and asynchronously execute a function through FunctionGraph.
- **Custom granting**: You can create an agency using IAM and and grants necessary permissions to Config by yourself. The permission content is as follows:

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "functiongraph:function:invokeAsync",
                "functiongraph:function:getConfig"
            ]
        }
    ]
}
```

For details about how to create an angency, see **Creating an Agency**.

Figure 3-5 Adding a rule using a custom policy



Step 6 On the displayed **Configure Rule Parameters** page, configure required parameters and click **Next**.

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

----End

3.1.3 Viewing Rules

Scenario

You can view all created rules and details of each rule on the Config console.

On the rule details page, you can also initiate resource evaluation, modify the rule, enable or disable the rule, or delete the rule.

Procedure

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

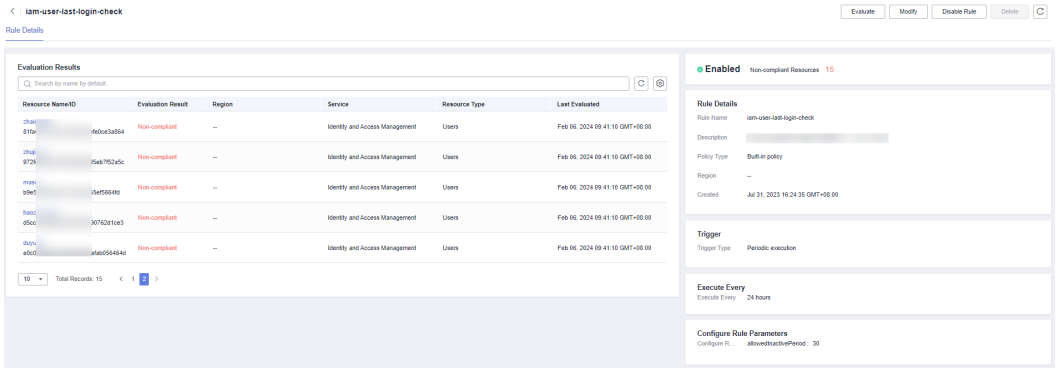
Step 3 In the navigation pane on the left, choose **Resource Compliance**.

Step 4 On the **Rules** tab, view rules, rule status, and evaluation results.

Step 5 Click a rule name to go to the **Rule Details** page.

The evaluation results are displayed on the left of the page, and the rule details on the right of the page.

Figure 3-6 Rule details



NOTE

A rule may be in one of the following statuses:

- **Enabled**: The rule is available.
- **Disabled**: The rule is disabled.
- **Evaluating**: The rule is evaluating resources.
- **Submitting**: The rule is submitting an evaluation task to the associated FunctionGraph function.

During the evaluation, the rule is in the **Evaluating** state. After the evaluation is complete, the rule status changes to **Enabled**, and then, you can view the evaluation results.

----End

3.1.4 Triggering Resource Compliance Evaluation

Scenarios

Rules can be triggered automatically or manually.

- **Automatic**

  Rules are automatically triggered in the following scenarios:

  - Adding a new rule
  - Modifying a rule

  - Enabling a rule
  - There are any resource changes if the **Trigger Type** is set to **Configuration change**

  If the **Trigger Type** is set to **Periodic execution**, the rule is triggered at a specific frequency.
- **Manual**

  You can manually initiate rule evaluation through the console or call the **run-evaluation** API.

Limitations and Constraints

The following lists the limitations and constraints for the resource recorder to collect resource data:

- The resource recorder must be enabled.
- The resource recorder only collects data of specified resources if you have configured a monitoring scope when enabling the resource recorder.
- If you enable the resource recorder and then disable it after a period of time, the recorder only collect resource data during the period when it is enabled.

Procedure

Step 1 Log in to the management console.

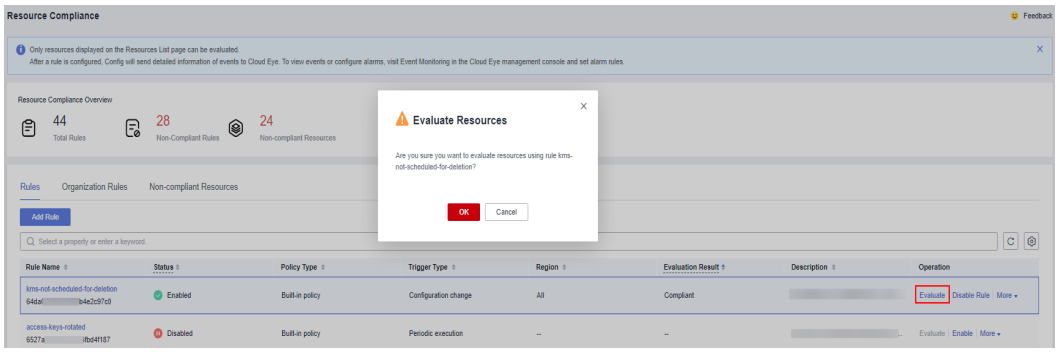
Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

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

Step 4 Locate a target rule and click **Evaluate** in the **Operation** column.

Step 5 In the displayed dialog box, click **OK**.

Figure 3-7 Manually triggering a rule



----End

3.1.5 Managing a Rule

Scenario

You can modify, enable, disable, or delete a rule at any time.

You can perform these operations in the rule list or on the **Rules Details** page. This section describes how to modify, enable, disable, or delete a rule in the rule list.

- **Disabling a Rule**
- **Enabling a Rule**
- **Modifying a Rule**
- **Deleting a Rule**

NOTE

Organization members cannot modify or delete organization rules. A rule in a conformance package cannot be independently modified or deleted. If you need to delete a rule in a conformance package, delete the package.. For details, see **Organization Rules** and **Conformance Packages**.

Disabling a Rule

Step 1 Log in to the management console.

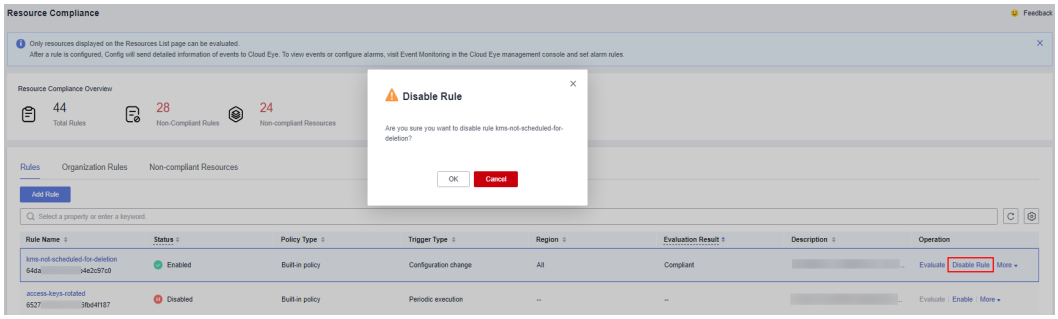
Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

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

Step 4 On the **Rules** tab, locate a target rule and click **Disable** in the **Operation** column.

Step 5 In the displayed dialog box, click **OK**.

Figure 3-8 Disabling a rule



----End

Enabling a Rule

Step 1 Log in to the management console.

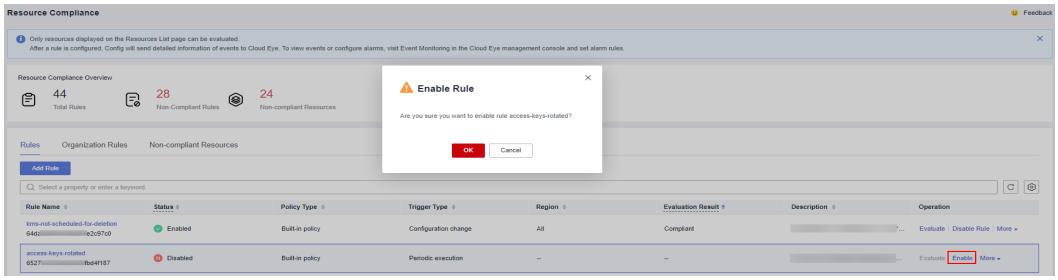
Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

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

Step 4 On the **Rules** tab, locate a target rule and click **Enable** in the **Operation** column.

Step 5 In the displayed dialog box, click **OK**.

Figure 3-9 Enabling a rule



----End

Modifying a Rule

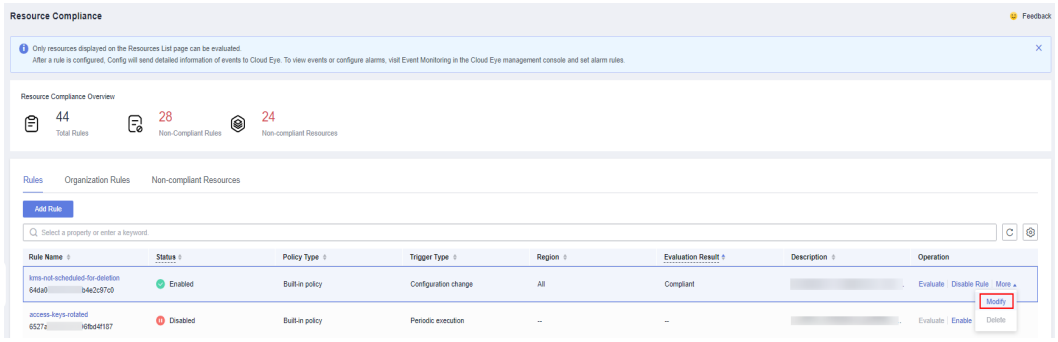
Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

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

Step 4 On the **Rules** tab, locate a target rule and click **More** > **Modify** in the **Operation** column.

Figure 3-10 Modifying a rule



Step 5 On the **Modify Rule** page, modify the rule description and click **Next**.

Step 6 Configure rule parameters and click **Next**.

Step 7 Confirm rule information and click **Submit.**

----End

Deleting a Rule

Before deleting a rule, you need to disable the rule.

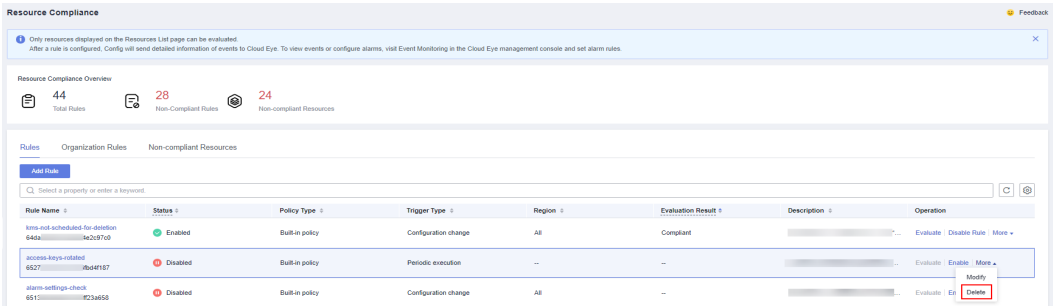
Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

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

Step 4 On the **Rules** tab, locate a target rule and click **More** > **Delete** in the **Operation** column.

Figure 3-11 Deleting a rule



Step 5 Click **OK**.

----End

3.1.6 Example Custom Rules

3.1.6.1 Example Functions (Python)

Example Function for Evaluations Triggered by Configuration Changes

Config will invoke a function like the following example when it detects a configuration change for a target resource.

```
import requests
import http.client
import time

requests.packages.urllib3.disable_warnings()


def get_policy_resource(domain_id, resource):
    return {
        "domain_id": domain_id,
        "region_id": resource.get("region_id"),
        "resource_id": resource.get("id"),
        "resource_name": resource.get("name"),
        "resource_provider": resource.get("provider"),
        "resource_type": resource.get("type")
    }


'''
Possible evaluation results are compliant or noncompliant.
In this example, if the resource type is ecs.cloudservers and the vpcId field of the ECS is not the VPC ID specified by rule parameters, Compliant is returned. Otherwise, NonCompliant is returned.
'''
def evaluate_compliance(resource, parameter):
```

```
    if resource.get("provider") != "ecs" or resource.get("type") != "cloudservers":
        return "Compliant"
    vpc_id = resource.get("properties", {}).get("metadata", {}).get("vpcId")
    return "Compliant" if vpc_id == parameter.get("vpcId") else "NonCompliant"


def update_policy_state(token, domain_id, evaluation):
    endpoint = "https://rms.myhuaweicloud.com"
    url = "{}/v1/resource-manager/domains/{}/policy-states".format(endpoint, domain_id)
    return requests.put(
        url=url,
        headers={
            "X-Auth-Token": token
        },
        json=evaluation,
        verify=False,
    )


def handler(event, context):
    resource = event.get("invoking_event", {})
    parameters = event.get("rule_parameter")
    compliance_state = evaluate_compliance(resource, parameters)

    requests = {
        "policy_resource": get_policy_resource(event.get("domain_id"), resource),
        "trigger_type": event.get("trigger_type"),
        "compliance_state": compliance_state,
        "policy_assignment_id": event.get("policy_assignment_id"),
        "policy_assignment_name": event.get("policy_assignment_name"),
        "function_urn": event.get("function_urn"),
        "evaluation_time": event.get("evaluation_time"),
        "evaluation_hash": event.get("evaluation_hash")
    }

    for retry in range(3):
        response = update_policy_state(context.getToken(), event.get("domain_id"), requests)
        if response.status_code == http.client.TOO_MANY_REQUESTS:
            print("TOO_MANY_REQUESTS: retry again")
            time.sleep(1)
        else:
            if response.status_code == http.client.OK:
                print("Update policyState successfully.")
            else:
                print("Failed to update policyState.")
                print(response.json())
            break
```

Example Function for Evaluations Triggered by Periodic Execution

Config will invoke a function like the following example for a custom rule that is executed periodically.

```
import requests
import http.client
import time

requests.packages.urllib3.disable_warnings()


def get_policy_resource(domain_id, resource):
    return {
        "domain_id": domain_id,
        "region_id": resource.get("region_id"),
        "resource_id": resource.get("id"),
        "resource_name": resource.get("name"),
        "resource_provider": resource.get("provider"),
        "resource_type": resource.get("type")
    }
```



```
"""
Possible evaluation results are compliant or noncompliant.
In this example, if the session timeout configured for the account is greater than 30 minutes, Compliant is returned. Otherwise, NonCompliant is returned.
The IAM API ShowDomainLoginPolicy is invoked.
"""
def evaluate_compliance(token, domain_id):
    endpoint = "https://iam.cn-north-4.myhuaweicloud.com"
    url = "{}/v3.0/OS-SECURITYPOLICY/domains/{}/login-policy".format(endpoint, domain_id)
    r = requests.get(
        url=url,
        headers={
            "X-Auth-Token": token,
            "User-Agent": "API Explorer",
            "Content-Type": "application/json;charset=UTF-8"
        },
        verify=False,
    )
    session_timeout = r.json().get("login_policy", {}).get("session_timeout", 60)
    return "NonCompliant" if session_timeout > 30 else "Compliant"


def update_policy_state(token, domain_id, evaluation):
    endpoint = "https://rms.myhuaweicloud.com"
    url = "{}/v1/resource-manager/domains/{}/policy-states".format(endpoint, domain_id)
    return requests.put(
        url=url,
        headers={
            "X-Auth-Token": token
        },
        json=evaluation,
        verify=False,
    )


def handler(event, context):
    resource = event.get("invoking_event", {})
    if resource.get("name") != "Account":
        return
    compliance_state = evaluate_compliance(context.getToken(), event.get("domain_id"))

    requests = {
        "policy_resource": get_policy_resource(event.get("domain_id"), resource),
        "trigger_type": event.get("trigger_type"),
        "compliance_state": compliance_state,
        "policy_assignment_id": event.get("policy_assignment_id"),
        "policy_assignment_name": event.get("policy_assignment_name"),
        "function_urn": event.get("function_urn"),
        "evaluation_time": event.get("evaluation_time"),
        "evaluation_hash": event.get("evaluation_hash")
    }

    for retry in range(3):
        response = update_policy_state(context.getToken(), event.get("domain_id"), requests)
        if response.status_code == http.client.TOO_MANY_REQUESTS:
            print("TOO_MANY_REQUESTS: retry again")
            time.sleep(1)
        else:
            if response.status_code == http.client.OK:
                print("Update policyState successfully.")
            else:
                print("Failed to update policyState.")
                print(response.json())
            break
```


3.1.6.2 Events

Sample Event for Evaluations Triggered by Configuration Changes

When a custom rule is triggered, Config publish an event to invoke the FunctionGraph function associated with the rule. The following example shows that a custom rule was triggered by a configuration change for **ecs.cloudservers**.


```
{
  "domain_id": "domain_id",
  "policy_assignment_id": "637c6b2e6b647c4d313d9719",
  "policy_assignment_name": "period-policy-period",
  "function_urn": "urn:fss:region_1:123456789:function:default:test-custom-policyassignment:latest",
  "trigger_type": "resource",
  "evaluation_time": 1669098286719,
  "evaluation_hash": "3bf8ecaeb0864feb98639080aea5c7d9",
  "rule_parameter": {
    "vpcId": {
      "value": "fake_id"
    }
  },
  "invoking_event": {
    "id": "5e0d49c8-7ce0-4c31-9d92-28b05200b838",
    "name": "default",
    "provider": "vpc",
    "type": "securityGroups",
    "tags": {},
    "created": "2022-11-07T12:58:46.000+00:00",
    "updated": "2022-11-07T12:58:46.000+00:00",
    "properties": {
      "description": "Default security group",
      "security_group_rules": [
        {
          "remote_group_id": "5e0d49c8-7ce0-4c31-9d92-28b05200b838",
          "ethertype": "IPv6",
          "security_group_id": "5e0d49c8-7ce0-4c31-9d92-28b05200b838",
          "port_range_max": 0,
          "id": "19f581bc-08a7-4037-ae59-9a6838c43709",
          "direction": "ingress",
          "port_range_min": 0
        },
        {
          "ethertype": "IPv6",
          "security_group_id": "5e0d49c8-7ce0-4c31-9d92-28b05200b838",
          "port_range_max": 0,
          "id": "75dae7b6-0b71-496f-8f11-87fb30300e18",
          "direction": "egress",
          "port_range_min": 0
        }
      ]
    },
    "ep_id": "0",
    "project_id": "vpc",
    "region_id": "region_1",
    "provisioning_state": "Succeeded"
  }
}
```


Example Event for Evaluations Triggered by a Periodic Execution

Config publishes an event when it evaluates your resources at a frequency that you specify, such as every 24 hours. The following example shows that a custom rule was triggered at a specific frequency.


```
{
  "domain_id": "domain_id",
```



```
 "policy_assignment_id": "637c6b2e6b647c4d313d9719",
 "policy_assignment_name": "period-policy-assignment",
 "function_urn": "urn:fss:region_1:123456789:function:default:test-custom-policyassignment:latest",
 "trigger_type": "period",
 "evaluation_time": 1669098286719,
 "evaluation_hash": "3bf8ecaeb0864feb98639080aea5c7d9",
 "rule_parameter": {},
 "invoking_event": {
  "id": "domain_id",
  "name": "Account",
  "provider": null,
  "type": null,
  "tags": null,
  "created": null,
  "updated": null,
  "properties": null,
  "ep_id": null,
  "project_id": null,
  "region_id": "global",
  "provisioning_state": null
 }
}
```


3.2 Organization Rules

3.2.1 Adding a Predefined Organization Rule

Scenarios

If you are an organization administrator or delegated administrator of Config, you can add organization rules, and then the organization rules can apply to all member accounts in your organization.

A deployed organization rule will be displayed in the rule list of each members in the organization. If you create an organization rule using an account, you can only use the same account to delete or modify the organization rule. Members can only trigger an organization rule and view evaluation results.

You can use a built-in policy or a custom policy to create an organization rule. This section describes how to create an organization rule with a built-in policy.

Constraints and Limitations

- Up to 500 rules can be added to an account.
- The **Organization Rules** tab is inaccessible for a non-organization member.
- The Organizations service is in open beta test (OBT). To use organization rules, apply for OBT.

Procedure

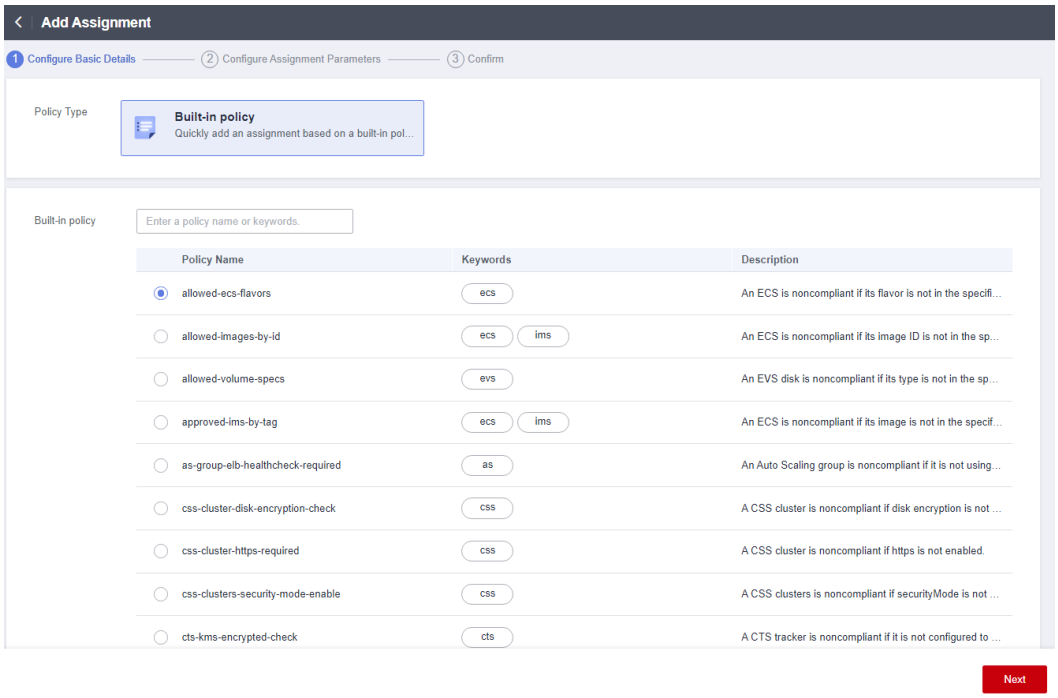
Step 1 Sign in to the Config console as an organization administrator or an agency administrator of Config.

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 Select the **Organization Rules** tab and click **Add Rule**. Complete the basic configurations and click **Next**.

Figure 3-12 Basic configuration



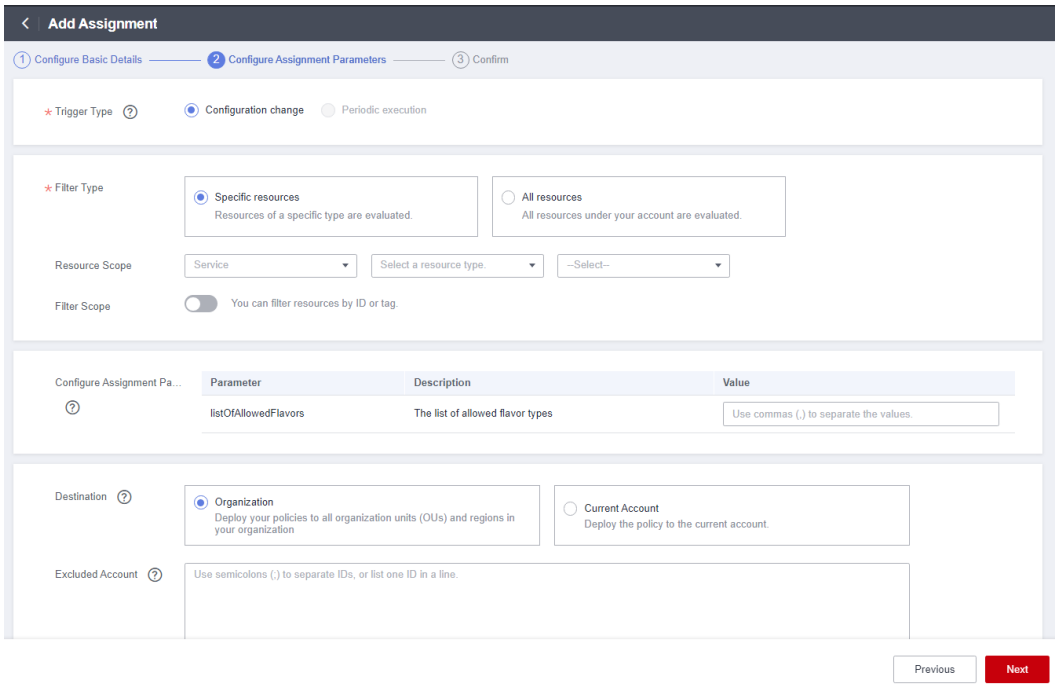
For details about parameter settings, see **Table 3-3**.

Table 3-3 Basic parameters

Parameter	Description
Policy Type	There are two types of policies: • Built-in policy • Custom policy
Built-in Policy	Built-in policies are provided by Config. You can use built-in policies to quickly add rules. For more information about built-in policies, see **Predefined Policies**.
Rule Name	By default, the predefined policy name is reused as the rule name. A rule name must be unique. A rule name can contain only digits, letters, underscores (_), and hyphens (-).
Description	By default, the rule description is the same as the description of the predefined policy. You can also customize the rule description. There are no restrictions on the rule description.

Step 5 On the displayed **Configure Rule Parameters** page, configure required parameters and click **Next**.

Figure 3-13 Rule parameters



For details about parameter settings, see **Table 3-4**.

Table 3-4 Rule parameter description

Parameter	Description
Trigger Type	Specifies the conditions under which rules are triggered . Trigger types are as follows: • **Configuration change**: A rule is triggered when there is a change in configuration of the resource. • **Periodic execution**: A rule is triggered at a specific frequency.
Filter Type	Specifies the resource scope. Filter types are as follows: • **Specific resources**: Resources of a specific type will be evaluated. • **All resources**: All resources from your account will be evaluated. This parameter is mandatory only when **Trigger Type** is set to **Configuration change**.

Parameter	Description
Resource Scope	If you set **Filter Type** to **Specific resources**, you need to specify a resource scope. • **Service**: The service to which a resource belongs. • **Resource type**: The resource type of the corresponding service. • **Region**: The region where the resource is located. This parameter is mandatory only when **Trigger Type** is set to **Configuration change**.
Filter scope	After you enable **Filter Scope**, you can filter resources by resource ID or tag. You can specify a specific resource for compliance evaluation. This parameter is mandatory only when **Trigger Type** is set to **Configuration change**.
Execute every	Indicates how often a rule is triggered. This parameter is mandatory only when **Trigger Type** is set to **Periodic execution**.
Rule parameter	Parameters of a built-in policy. For example, if you select a built-in policy **required-tag-check** and the policy stipulates that resources without a specific tag added are noncompliant, the rule parameters you need to specify are a tag key and a tag value. This parameter is not mandatory for all built-in policies, for example, a built-in policy **volumes-encrypted-check** stipulates that if a mounted EVS disk is not encrypted, this disk is noncompliant.
Destination	Specifies where the organization rule will be deployed. • **Organization**: A policy is deployed to all member accounts in an organization. • **Current Account**: A policy is deployed to the current account. When creating an organization rule, select **Organization**.
Excluded Account	Specifies member accounts in an organization for which organization rules will not be deployed. This parameter is only required when **Destination** is set to **Organization**.

Step 6 Confirm the rule information and click **Submit**.

Figure 3-14 Confirming a rule

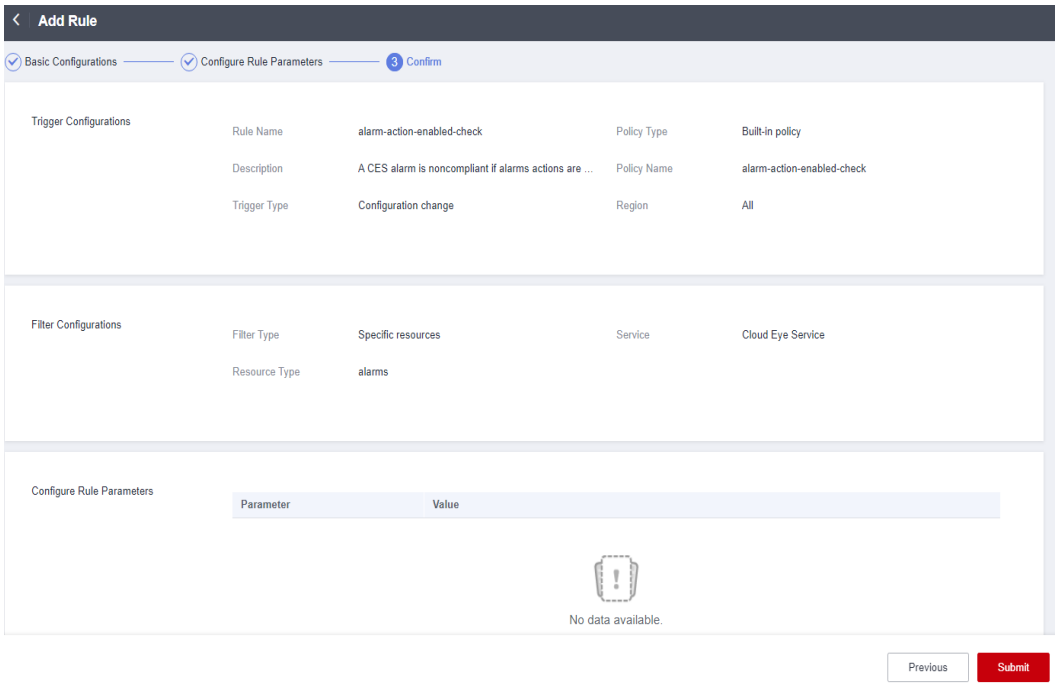
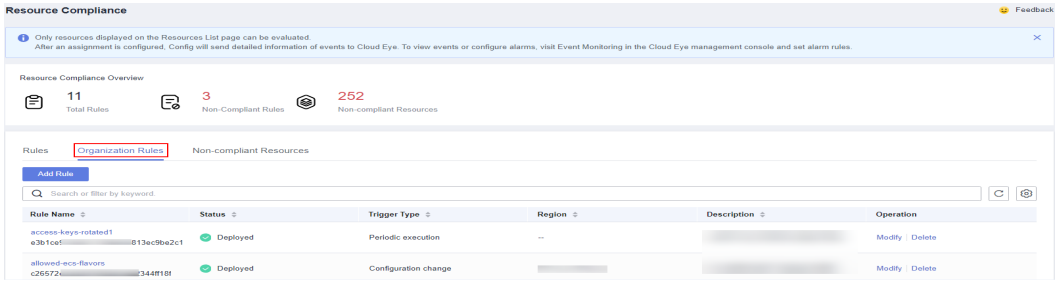


Figure 3-15 Querying an organization rule



NOTE

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

----End

Triggering a Rule Evaluation

For details about how a membe can trigger an organization rule, see **Triggering Resource Compliance Evaluation**.

3.2.2 Querying an Organization Rule

Scenario

You can view organization rules and their details.

This section consists of **Viewing an Organization Rule** and **Viewing Organization Rules Deployed to Member Accounts**.

Viewing an Organization Rule

You can view details about a created organization rule.

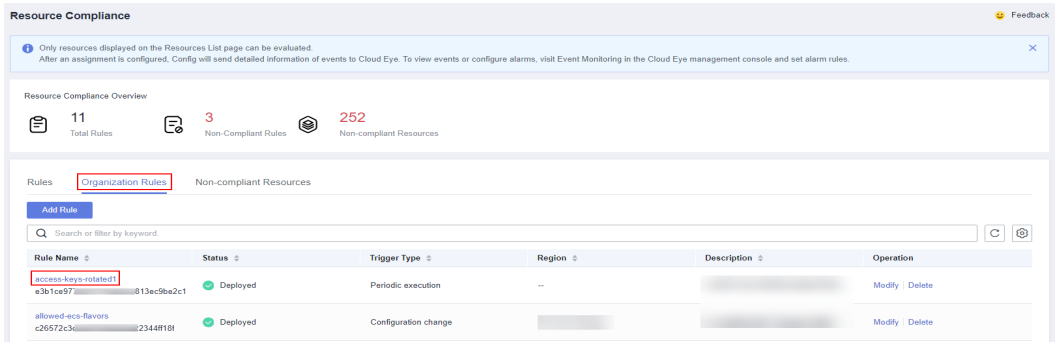
Step 1 Sign in to the Config console using the account with which the organization rules are created.

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 Click the **Organization Rules** tab and then click the name of the rule you want to view.

Figure 3-16 Viewing organization rules



Step 5 On the left of the **Rule Details** page, view member accounts to which the rule deploys, the deployment status, and excluded accounts. On the right of the page, view rule details.

NOTE

Members in an organization can only view organization rules created by themselves.

----End

Viewing Organization Rules Deployed to Member Accounts

A deployed organization rule will be displayed in the rule list of each member account in the organization. If you create an organization rule using an account, you can only use the same account to delete or modify the organization rule. Members can only trigger an organization rule and view evaluation results.

Step 1 Sign in to the management console as an organization member.

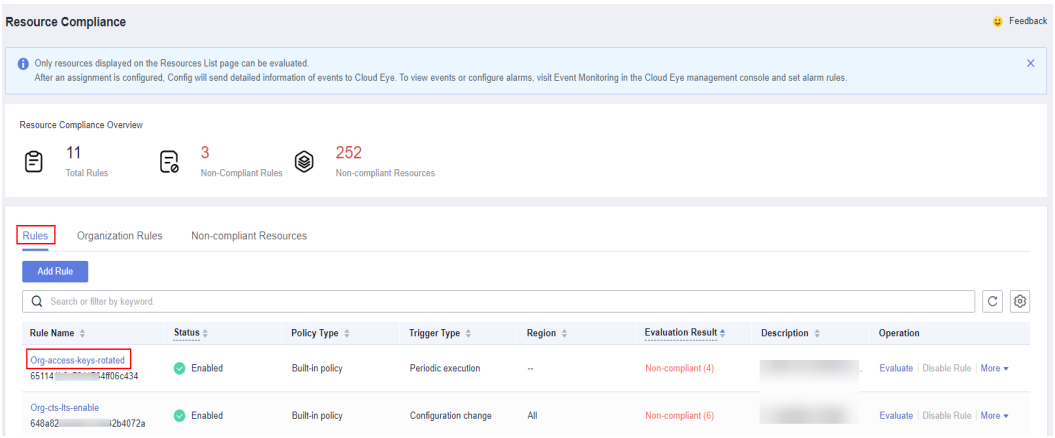
Step 2 Click ☰ in the upper left corner of the page. In the service list that is displayed, under **Management & Governance**, select **Config**.

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

Step 4 On the **Rules** tab, click an organization rule name in the rule list to view details.

The evaluation results are displayed on the left of the page, and the rule details on the right of the page.

Figure 3-17 Viewing organization rules deployed to member accounts



NOTE

A deployed organization rule will be displayed in the rule list of every member account in the organization. The system automatically adds the **Org** field before the rule name.

Members in an organization can only trigger evaluations against the organization rules and view evaluation results and details. They cannot modify, disable, or delete an organization rule.

----End

3.2.3 Modifying an Organization Rule

Scenarios

After an organization rule is added, you can modify its description and parameters at any time.

Procedure

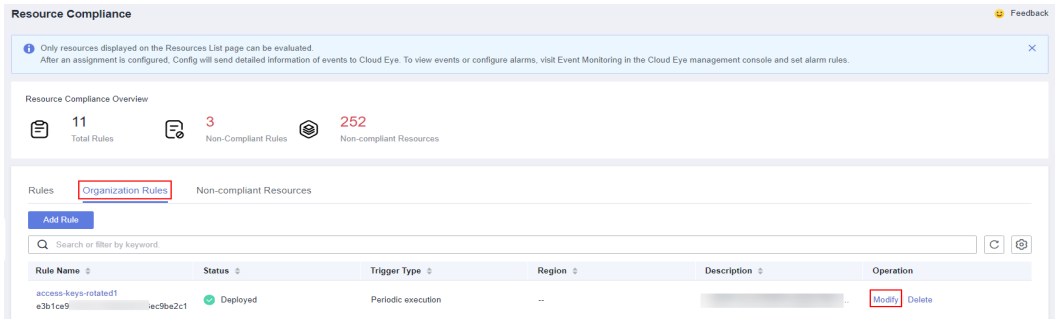
Step 1 Sign in to the Config console using the account with which the organization rules are created.

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 Click the **Organization Rules** tab. In the list, locate the rule and click **Edit** in the **Operation** column.

Figure 3-18 Editing an organization rule



Step 5 On the **Modify Rule** page, modify the rule description and click **Next**.

Step 6 Modify the rule parameters and click **Next**.

Step 7 Confirm the rule modifications and click **Submit.**

----End

3.2.4 Deleting an Organization Rule

Scenarios

If you no longer need an organization rule, you can delete it.

Procedure

Step 1 Sign in to the Config console using the account with which the organization rules are created.

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

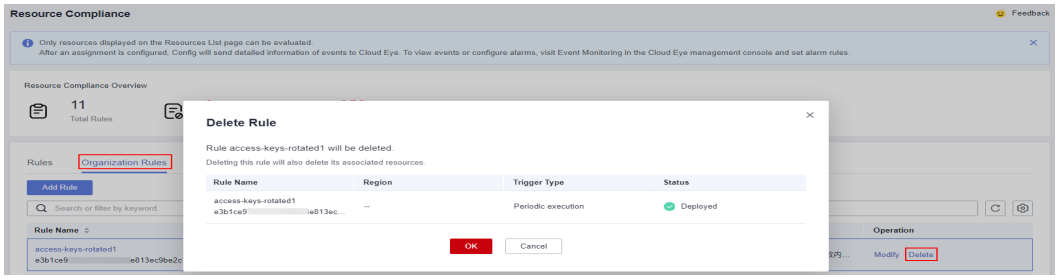
Step 3 In the navigation pane on the left, choose **Resource Compliance**.

Step 4 Click the **Organization Rules** tab. In the list, locate the rule and click **Delete** in the **Operation** column.

Step 5 In the displayed **Delete Rule** dialog box, confirm the information and click **OK**.

After an organization rule is deleted, the rule is also automatically deleted from the rule lists of member accounts to which the rule was deployed.

Figure 3-19 Deleting organization rules



----End

NOTE

You can also click a rule name in the **Rules** list to go to the **Rule Details** page. In the upper right corner of the page, click **Modify** or **Delete** to manage the rule.

3.2.5 Example Custom Organization Rules

3.2.5.1 Example Functions (Python)

Example Function Triggered by Configuration Changes

Config will invoke a function like the following example when it detects any configuration changes to the resources that are within the resource scope recorded by the rule.

```
import requests
import http.client
import time

requests.packages.urllib3.disable_warnings()


def get_policy_resource(domain_id, resource):
    return {
        "domain_id": domain_id,
        "region_id": resource.get("region_id"),
        "resource_id": resource.get("id"),
        "resource_name": resource.get("name"),
        "resource_provider": resource.get("provider"),
        "resource_type": resource.get("type")
    }


'''
Possible evaluation results are compliant or noncompliant.
In this example, if the resource type is ecs.cloudservers and the vpcId value does not match the specified VPC ID, NonCompliant is returned. Otherwise, Compliant is returned.
'''
def evaluate_compliance(resource, parameter):
    if resource.get("provider") != "ecs" or resource.get("type") != "cloudservers":
        return "Compliant"
    vpc_id = resource.get("properties", {}).get("metadata", {}).get("vpcId")
    return "Compliant" if vpc_id == parameter.get("vpcId") else "NonCompliant"


def update_policy_state(token, domain_id, evaluation):
    endpoint = "https://rms.myhuaweicloud.com"
# For custom organization rules, domain_id in the url must match the domain_id of the function creator (organization administrator or Config agency administrator). Otherwise, Config cannot be accessed.
    url = "{}/v1/resource-manager/domains/{}/policy-states".format(endpoint, domain_id)
    return requests.put(
        url=url,
        headers={
            "X-Auth-Token": token
        },
        json=evaluation,
        verify=False,
    )


def handler(event, context):
    resource = event.get("invoking_event", {})
    parameters = event.get("rule_parameter")
    compliance_state = evaluate_compliance(resource, parameters)
```



```
    requests = {
        "policy_resource": get_policy_resource(event.get("domain_id"), resource),
        "trigger_type": event.get("trigger_type"),
        "compliance_state": compliance_state,
        "policy_assignment_id": event.get("policy_assignment_id"),
        "policy_assignment_name": event.get("policy_assignment_name"),
        "function_urn": event.get("function_urn"),
        "evaluation_time": event.get("evaluation_time"),
        "evaluation_hash": event.get("evaluation_hash")
    }

    for retry in range(3):
        response = update_policy_state(context.getToken(), event.get("domain_id"), requests)
        if response.status_code == http.client.TOO_MANY_REQUESTS:
            print("TOO_MANY_REQUESTS: retry again")
            time.sleep(1)
        else:
            if response.status_code == http.client.OK:
                print("Update policyState successfully.")
            else:
                print("Failed to update policyState.")
                print(response.json())
            break
```

Example Function Triggered Periodically

Config will invoke a function like the following example for a custom organization rule that is executed periodically.

```
import requests
import http.client
import time

requests.packages.urllib3.disable_warnings()


def get_policy_resource(domain_id, resource):
    return {
        "domain_id": domain_id,
        "region_id": resource.get("region_id"),
        "resource_id": resource.get("id"),
        "resource_name": resource.get("name"),
        "resource_provider": resource.get("provider"),
        "resource_type": resource.get("type")
    }


"""
Possible evaluation results are compliant or noncompliant.
In this example, if the session timeout configured for the account is greater than 30 minutes, Compliant is returned. Otherwise, NonCompliant is returned.
The IAM API ShowDomainLoginPolicy is invoked.
"""
def evaluate_compliance(token, domain_id):
    endpoint = "https://iam.cn-north-4.myhuaweicloud.com"
# For custom organization rules, domain_id in the url must match the domain_id of the function creator (organization administrator or Config agency administrator). Otherwise, Config cannot be accessed.
    url = "{}/v3.0/OS-SECURITYPOLICY/domains/{}/login-policy".format(endpoint, domain_id)
    r = requests.get(
        url=url,
        headers={
            "X-Auth-Token": token,
            "User-Agent": "API Explorer",
            "Content-Type": "application/json;charset=UTF-8"
        },
        verify=False,
    )
    session_timeout = r.json().get("login_policy", {}).get("session_timeout", 60)
```



```
    return "NonCompliant" if session_timeout > 30 else "Compliant"


def update_policy_state(token, domain_id, evaluation):
    endpoint = "https://rms.myhuaweicloud.com"
    url = "{}/v1/resource-manager/domains/{}/policy-states".format(endpoint, domain_id)
    return requests.put(
        url=url,
        headers={
            "X-Auth-Token": token
        },
        json=evaluation,
        verify=False,
    )


def handler(event, context):
    resource = event.get("invoking_event", {})
    if resource.get("name") != "Account":
        return
    compliance_state = evaluate_compliance(context.getToken(), event.get("domain_id"))

    requests = {
        "policy_resource": get_policy_resource(event.get("domain_id"), resource),
        "trigger_type": event.get("trigger_type"),
        "compliance_state": compliance_state,
        "policy_assignment_id": event.get("policy_assignment_id"),
        "policy_assignment_name": event.get("policy_assignment_name"),
        "function_urn": event.get("function_urn"),
        "evaluation_time": event.get("evaluation_time"),
        "evaluation_hash": event.get("evaluation_hash")
    }

    for retry in range(3):
        response = update_policy_state(context.getToken(), event.get("domain_id"), requests)
        if response.status_code == http.client.TOO_MANY_REQUESTS:
            print("TOO_MANY_REQUESTS: retry again")
            time.sleep(1)
        else:
            if response.status_code == http.client.OK:
                print("Update policyState successfully.")
            else:
                print("Failed to update policyState.")
                print(response.json())
            break
```

3.2.5.2 Events

Sample Event for Evaluations Triggered by Configuration Changes

When a custom organization rule is triggered, Config publish an event to invoke the FunctionGraph function associated with the rule. The following is an example of events pushed by Config when a custom organization rule is triggered by a configuration change of **ecs.cloudservers**.

```
{
  "domain_id": "domain_id",
  "policy_assignment_id": "637c6b2e6b647c4d313d9719",
  "policy_assignment_name": "period-policy-period",
  "function_urn": "urn:fss:region_1:123456789:function:default:test-custom-policyassignment:latest",
  "trigger_type": "resource",
  "evaluation_time": 1669098286719,
  "evaluation_hash": "3bf8ecaeb0864feb98639080aea5c7d9",
  "rule_parameter": {
    "vpcId": {
      "value": "fake_id"
    }
```



```
 },
 "invoking_event": {
  "id": "5e0d49c8-7ce0-4c31-9d92-28b05200b838",
  "name": "default",
  "provider": "vpc",
  "type": "securityGroups",
  "tags": {},
  "created": "2022-11-07T12:58:46.000+00:00",
  "updated": "2022-11-07T12:58:46.000+00:00",
  "properties": {
   "description": "Default security group",
   "security_group_rules": [
    {
     "remote_group_id": "5e0d49c8-7ce0-4c31-9d92-28b05200b838",
     "ethertype": "IPv6",
     "security_group_id": "5e0d49c8-7ce0-4c31-9d92-28b05200b838",
     "port_range_max": 0,
     "id": "19f581bc-08a7-4037-ae59-9a6838c43709",
     "direction": "ingress",
     "port_range_min": 0
    },
    {
     "ethertype": "IPv6",
     "security_group_id": "5e0d49c8-7ce0-4c31-9d92-28b05200b838",
     "port_range_max": 0,
     "id": "75dae7b6-0b71-496f-8f11-87fb30300e18",
     "direction": "egress",
     "port_range_min": 0
    }
   ]
  },
  "ep_id": "0",
  "project_id": "vpc",
  "region_id": "region_1",
  "provisioning_state": "Succeeded"
 }
}
```


Example Event for Evaluations Triggered Periodically

Config publishes an event when it evaluates your resources at a frequency that you specify, such as every 24 hours. The following is an example of events pushed by Config when a custom organization rule is triggered at a specified frequency.


```
{
 "domain_id": "domain_id",
 "policy_assignment_id": "637c6b2e6b647c4d313d9719",
 "policy_assignment_name": "period-policy-assignment",
 "function_urn": "urn:fss:region_1:123456789:function:default:test-custom-policyassignment:latest",
 "trigger_type": "period",
 "evaluation_time": 1669098286719,
 "evaluation_hash": "3bf8ecaeb0864feb98639080aea5c7d9",
 "rule_parameter": {},
 "invoking_event": {
  "id": "domain_id",
  "name": "Account",
  "provider": null,
  "type": null,
  "tags": null,
  "created": null,
  "updated": null,
  "properties": null,
  "ep_id": null,
  "project_id": null,
  "region_id": "global",
  "provisioning_state": null
 }
}
```


3.3 Viewing Noncompliant Resources

Scenarios

You can view all noncompliant resources detected by your rules.

Procedure

Step 1 Log in to the management console.

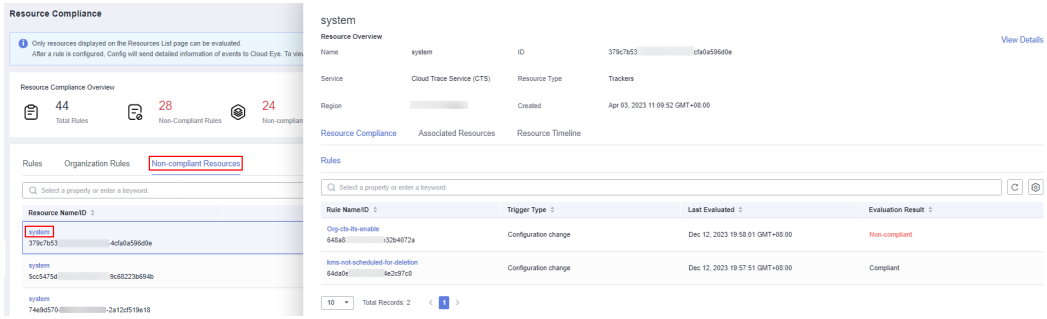
Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

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

Step 4 Click **Non-compliant Resources**. All non-compliant resources from the current account are displayed in a list.

Step 5 Click a resource name to view resource overview.

Figure 3-20 Viewing non-compliant resources



----End

3.4 Compliance Rule Concepts

3.4.1 Policies

A policy is a logical expression used to evaluate resource compliance. It is part of a compliance rule.

Policies are static. To make a policy work, you need to specify specific resource scope.

A policy can be a JSON expression. **Table 3-5** lists policy (JSON expression) parameters.

Table 3-5 Policy parameters

Parameter	Description	Remarks
id	Policy ID	N/A
name	Policy name	A policy name can contain up to 64 characters.
display_name	Display name of a policy	A policy display name can contain up to 64 characters.
description	Policy description	Policy description can contain up to 512 characters.
parameters	Policy parameters The following attributes are used to describe each policy parameter: • **name** • **description** • **type** • **default_value** • **allowed_values** • minimum • maximum • min_items • max_items • min_length • max_length • pattern	The parameter names, such as **name** and **description** contained in the compliance policy remain unchanged. • **name** indicates the name of a rule. • **description**: supplementary information of **parameters** • **type**: the type of **parameters**, which can be **String**, **Array**, **Boolean**, **Integer**, or **Float**. • **default_value**: Specifies the default value of **parameters**. If the parameter is specified, you can use it when you add a rule. • **allowed_values**: Specifies the list of values allowed by **parameters**. If the parameter is specified, you can only select values from the list. • Minimum value, which is valid when **type** is set to **Integer** or **Float**. • Maximum value, which is valid when **type** is set to **Integer** or **Float**. • Minimum items, which is valid when **type** is set to **Array**. • Maximum items, which is valid when **type** is set to **Array**. • Minimum string length, which is valid when **type** is set to **String** or **Array**. • Maximum string length, which is valid when **type** is set to **String** or **Array**. • Regular expression requirements, which is valid when **type** is set to **String** or **Array**.
keywords	Policy keywords	Generally, the name abbreviation of the related product is used as a keyword.

Parameter	Description	Remarks
policy_type	Policy type The options are as follows: • **builtin** • **custom**	• **builtin**: specifies the type of policies that are provided and maintained by Config. For details, see **Predefined Policies**. • **custom**: specifies the type of policies that are customized by users.
policy_rule_type	Policy syntax	**Domain Specific Language (DSL)**: provided by Config to write policy expressions.
policy_rule	Policy logical expression	For details about how to use DSL to write policy expressions, see **DSL Syntax**.
trigger_type	Trigger type. The options are as follows: • **resource** • **period**	• **resource**: runs when a specified resource is changed. • **period**: specifies the frequency at which a rule is triggered.
default_resource_types	Resource type	Most policies only apply to a limited scope of resources. You are advised to use a rule to only evaluate resource types in **default_resource_types**.

The following is an example policy used to check whether specified images are used for ECSs.

```
{
  "id": "5fa265c0aa1e6afc05a0ff07",
  "name": "allowed-images-by-id",
"description": "An ECS image is non-compliant if its ID is not within the specific image ID range.",
  "parameters": {
    "listOfAllowedImages": {
      "name": "null",
      "description": "The list of allowed image IDs",
      "type": "Array"
      "allowed_values": null,
      "default_value": null,
    }
  },
  "keywords": [
    "ecs",
    "ims"
  ],
  "policy_type": "builtin",
  "policy_rule_type": "dsl",
  "trigger_type": "resource",
  "policy_rule": {
    "allOf": [
      {
        "value": "${resource().provider}",
        "comparator": "equals",
        "pattern": "ecs"
      },
      {
       "value": "${resource().type}",
```



```
      "comparator": "equals",
      "pattern": "cloudservers"
     },
     {
      "value": "${resource().properties.metadata.meteringImageId}",
       "comparator": "notIn",
       "pattern": "${parameters('listOfAllowedImages')}"
     }
    ]
   },
}
```

For more examples, see **Example Custom Rules**.

3.4.2 Rule

A rule is created by specifying a policy and the application scope, for example, some resources in a region.

You can use a JSON expression to represent a rule, as shown in **Table 3-6**.

Table 3-6 Rule in JSON

Parameter	Description	Limitations	Remarks
id	Specifies the unique ID of a rule.	N/A	N/A
policy_assignment_type	Specifies the rule type.	N/A	The options are as follows: • **builtin**: built-in policy. In this case, **policy_definition_id** for the rule is mandatory. • **custom**: custom policy. In this case, **custom_policy** for the rule is mandatory. If this parameter is not configured, **builtin** is used by default.
name	Specifies the rule name.	Its value must be a string with up to 64 characters.	By default, the rule name is the same as the selected policy name. You can customize the rule name. You can set a name of up to 64 characters.

Parameter	Description	Limitations	Remarks
description	Specifies supplementary information about the rule.	Its value must be a string with up to 512 characters.	By default, the rule description is the same as the description of the selected policy. You can customize the rule description. You can set the description of up to 512 characters.
period	Specifies how often the rule is executed.	N/A	Possible values are: • **One_Hour** • **Three_Hours** • **Six_Hours** • **Twelve_Hours** • **TwentyFour_Hours**

Parameter	Description	Limitations	Remarks
policy_filter	Specifies the rule filter, which is used to filter the resources that will be evaluated by this rule. A filter has the following properties: • **region_id**: Specifies the region ID. • **resource_provider**: Specifies the service. • **resource_type**: Specifies the resource type of the service. • **resource_id**: Specifies the resource ID. • **tag_key**: Specifies the resource tag key. • **tag_value**: Specifies the resource tag value.	**policy_filter**: Its value must be an object. • **region_id**: Its value must be a string with up to 128 characters. Only letters, digits, and hyphens (-) are allowed. • **resource_provider**: Its value must be a string with up to 128 characters. Only letters and digits are allowed. • **resource_type**: Its value must be a string with up to 128 characters. Only letters and digits are allowed. • **resource_id**: Its value must be a string with up to 256 characters. • **tag_key**: Its value must be a string with up to 128 characters. • **tag_value**: Its value must be a string with up to 256 characters.	**NOTE** **resource_provider** is used to determine the filter type (**Specific resources** or **All resources**). • If **resource_provider** exists in **policy_filter**, the filter type is **Specific resources**. • If **resource_provider** does not exist in **policy_filter**, the filter type is **All resources**. Therefore, no separate filter type property is set in **policy_filter**.
state	Specifies the rule status.	N/A	Possible values are: • **Enabled**: The rule is available. • **Disabled**: The rule is disabled. • **Evaluating**: The rule is being used for resource compliance evaluation.

Parameter	Description	Limitations	Remarks
created	Specifies the time when the rule was created.	N/A	**NOTE** The time is a UTC time in a fixed format complying with ISO-8601 (for example, **2018-11-14T08:59:14Z**).
updated	Specifies the time when the rule was updated.	N/A	
policy_definition_id	Specifies the ID of the compliance policy bound to the rule.	Its value must be a string with up to 64 characters. Only letters, digits, and hyphens (-) are allowed.	Policy ID
custom_policy	Custom policy, which contains the following attributes: • **function_urn**: Specifies the URN of the function. • **auth_type**: Specifies the authentication type for the function to be invoked. • **auth_value**: Specifies the authentication value of the function to be invoked.	**custom_policy**: Its value is an object type. • **function_urn**: Its value must be a string with up to 1,024 characters. • **auth_type**: Its value must be a string. Only **agency** is supported. • **auth_value**: Its value must be an object which is related to **auth_type**. Only the **{"agency_name": value_name}** structure is supported, where **value_name** indicates the IAM agency name configured for Config.	**custom_policy** specifies the URN of the function in the custom policy and the authentication type for invoking the function.

Parameter	Description	Limitations	Remarks
parameters	Specifies the values of rule parameters.	**parameters**: Its value must be an object. • **key**: Its value must be a string including only letters and numbers. If the policy type of the rule is **Custom policy**, the value can have up to 1,024 characters. • **value**: Its value must be an object, and the value restrictions vary depending on the parameter type.	The compliance policy bound to the rule has corresponding parameters. The number, type, and value range of those parameters depend on the selected compliance policy.

NOTE

You cannot create a rule to evaluate another rule or a conformance package.

The following is an example policy used to check whether ECSs in region 1 have the tag (**env**: **production**).

```
{
  "id": "5fcd8696dfb78231e6f2f899",
  "name": "required-tag-check",
  "description": "A resource is non-compliant if it does not contain the specific tag.",
  "policy_filter": {
        "region_id": "regionid_1",
        "resource_provider": "ecs",
        "resource_type": "cloudservers",
        "tag_key": "env",
        "tag_value": "production"
  },
  "period": null,
  "state": "Enabled",
  "created": "2020-12-07T01:34:14.266Z",
  "updated": "2020-12-07T01:34:14.266Z",
  "policy_definition_id": "5fa9f89b6eed194ccb2c04db",
  "parameters": {
        "specifiedTagKey": {
        "value": "a"     },
        "specifiedTagValue": {
        "value": []
    }
  }
}
```

The following JSON file contains a custom rule for checking ECSs in **regionid_1**:

```
{
  "id": "719d8696dfb78231e6f2f719",
  "name": "test_consume_policy",
"description": "A resource is non-compliant if it does not contain the specific tag.",
```



```
"policy_filter": {
      "region_id": "regionid_1",
      "resource_provider": "ecs",
      "resource_type": "cloudservers",
      "tag_key": null,
      "tag_value": null
 },
 "period": null,
 "state": "Enabled",
 "created": "2022-07-19T01:34:14.266Z",
 "updated": "2022-07-19T01:34:14.266Z",
 "policy_definition_id": null,
 "custom_policy": {
   "function_urn": "urn:fss:regionid_1:projectidforpolicy:function:default:test_consume_policy:latest",
   "auth_type": "agency",
   "auth_value": {"agency_name": "rms_fg_agency"}
 },
 "parameters": {
      "vpcId": {"value": "allowed-vpc-id"}
   }
 }
}
```

3.4.3 Evaluation Results

After an evaluation is triggered, the corresponding evaluation result (**PolicyState**) will be generated.

You can use a JSON expression to represent an evaluation result, as shown in **Table 3-7**.

Table 3-7 Evaluation result in JSON

Parameter	Description	Remarks
domain_id	Account ID	This parameter is used to distinguish users. **domain_id** in the evaluation result will not be left blank.
resource_id	Specifies the ID of the evaluated resource.	N/A
resource_name	Specifies the name of the evaluated resource.	N/A
resource_provider	Specifies the service the resource belongs to.	N/A
resource_type	Specifies the resource type.	N/A
trigger_type	Trigger type	Possible values are: • resource • period

Parameter	Description	Remarks
compliance_state	Specifies the compliance result.	Possible values are: • **Compliant** • **NonCompliant**
policy_assignment_id	Rule ID	N/A
policy_definition_id	Specifies the ID of the policy used for evaluation.	N/A
evaluation_time	Specifies the evaluation timestamp.	N/A

The following JSON indicates a non-compliant evaluation result:

```
{
  "domain_id": "domainidforpolicy",
  "resource_id": "special-ecs1-with-public-ip-with-tag",
  "resource_name": "ecs1-with-public-ip-with-tag",
  "resource_provider": "ecs",
  "resource_type": "cloudservers",
  "trigger_type": "resource",
  "compliance_state": "NonCompliant",
  "policy_assignment_id": "5fa9f8a2501013093a192b07",
  "policy_definition_id": "5fa9f8a2501013093a192b06",
  "evaluation_time": 1604974757084
}
```

3.5 Predefined Policies

3.5.1 Predefined Policy List

You can use predefined policies to create rules on the Config console.

The following table lists predefined policies provided by Config.

Table 3-8 Predefined policies

Service	Policy	Triggered By	Object
General services	**regular-matching-of-names**	Configuration change	All resources
	required-tag-check	Configuration change	All resources

Service	Policy	Triggered By	Object
	resource-in-enterprise-project	Configuration change	All resources
	resources-in-supported-region	Configuration change	All resources
API Gateway (APIG)	apig-instances-authorization-type-configured	Configuration change	apig.instances
	apig-instances-execution-logging-enabled	Configuration change	apig.instances
	apig-instances-ssl-enabled	Configuration change	apig.instances
CodeArts Deploy	codeartsdeploy-host-cluster-resource-status	Configuration change	codeartsdeploy.host-cluster
MapReduce Service (MRS)	mrs-cluster-in-allowed-security-groups	Configuration change	mrs.mrs
	mrs-cluster-in-vpc	Configuration change	mrs.mrs
	mrs-cluster-kerberos-enabled	Configuration change	mrs.mrs
	mrs-cluster-multiAZ-deployment	Configuration change	mrs.mrs
	mrs-cluster-no-public-ip	Configuration change	mrs.mrs
NAT Gateway	private-nat-gateway-authorized-vpc-only	Configuration change	nat.privateNatGateways
VPC Endpoint (VPCEP)	vpcep-endpoint-enabled	Periodic	vpcep.endpoints

Service	Policy	Triggered By	Object
Web Application Firewall (WAF)	**waf-instance-policy-not-empty**	Configuration change	waf.instance
ELB	**elb-loadbalancers-no-public-ip**	Configuration change	elb.loadbalancers
	elb-predefined-security-policy-https-check	Configuration change	elb.loadbalancers
	elb-tls-https-listeners-only	Configuration change	elb.loadbalancers
	elb-members-weight-check	Configuration change	elb.members
Elastic IP (EIP)	**eip-bandwidth-limit**	Configuration change	vpc.publicips
	eip-unbound-check	Configuration change	vpc.publicips
	eip-use-in-specified-days	Periodic	vpc.publicips
Auto Scaling (AS)	**as-capacity-rebalancing**	Configuration change	as.scalingGroups
	as-group-elb-healthcheck-required	Configuration change	as.scalingGroups
	as-multiple-az	Configuration change	as.scalingGroups
Scalable File Service (SFS)	**sfsturbo-encrypted-check**	Configuration change	sfsturbo.shares
Elastic Cloud Server (ECS)	**allowed-ecs-flavors**	Configuration change	ecs.cloudservers

Service	Policy	Triggered By	Object
	allowed-images-by-id	Configuration change	ecs.cloudservers
	approved-ims-by-tag	Configuration change	ecs.cloudservers
	ecs-in-allowed-security-groups	Configuration change	ecs.cloudservers
	ecs-instance-in-vpc	Configuration change	ecs.cloudservers
	ecs-instance-key-pair-login	Configuration change	ecs.cloudservers
	ecs-instance-no-public-ip	Configuration change	ecs.cloudservers
	ecs-multiple-public-ip-check	Configuration change	ecs.cloudservers
	stopped-ecs-date-diff	Periodic	ecs.cloudservers
Distributed Cache Service (DCS)	dcs-memcached-enable-ssl	Configuration change	dcs.memcached
	dcs-memcached-in-vpc	Configuration change	dcs.memcached
	dcs-memcached-no-public-ip	Configuration change	dcs.memcached
	dcs-memcached-password-access	Configuration change	dcs.memcached
	dcs-redis-enable-ssl	Configuration change	dcs.redis

Service	Policy	Triggered By	Object
	dcs-redis-high-tolerance	Configuration change	dcs.redis
	dcs-redis-in-vpc	Configuration change	dcs.redis
	dcs-redis-no-public-ip	Configuration change	dcs.redis
	dcs-redis-password-access	Configuration change	dcs.redis
FunctionGraph	function-graph-concurrency-check	Configuration change	fgs.functions
	function-graph-inside-vpc	Configuration change	fgs.functions
	function-graph-public-access-prohibited	Configuration change	fgs.functions
	function-graph-settings-check	Configuration change	fgs.functions
Content Delivery Network (CDN)	cdn-enable-https-certificate	Configuration change	cdn.domains
	cdn-origin-protocol-no-http	Configuration change	cdn.domains
	cdn-security-policy-check	Configuration change	cdn.domains
	cdn-use-my-certificate	Configuration change	cdn.domains
Config	tracker-config-enabled-check	Periodic	config.trackers

Service	Policy	Triggered By	Object
Data Warehouse Service (DWS)	**dws-enable-kms**	Configuration change	dws.clusters
	dws-enable-log-dump	Configuration change	dws.clusters
	dws-enable-snapshot	Configuration change	dws.clusters
	dws-enable-ssl	Configuration change	dws.clusters
Data Replication Service (DRS)	**drs-data-guard-job-not-public**	Configuration change	drs.dataGuardJob
	drs-migration-job-not-public	Configuration change	drs.migrationJob
	drs-synchronization-job-not-public	Configuration change	drs.synchronizationJob
Data Encryption Workshop (DEW)	**kms-not-scheduled-for-deletion**	Configuration change	kms.keys
	kms-rotation-enabled	Configuration change	kms.keys
Identity and Access Management (IAM)	**access-keys-rotated**	Periodic	iam.users
	iam-customer-policy-blocked-kms-actions	Configuration changes	iam.roles&iam.policies
	iam-group-has-users-check	Configuration change	iam.groups
	iam-password-policy	Configuration change	iam.users

Service	Policy	Triggered By	Object
	iam-policy-blacklisted-check	Configuration change	iam.users, iam.groups, iam.agencies
	iam-policy-no-statements-with-admin-access	Configuration change	iam.roles, iam.policies
	iam-role-has-all-permissions	Configuration change	iam.roles, iam.policies
	iam-root-access-key-check	Periodic	iam.users
	iam-user-access-mode	Configuration change	iam.users
	iam-user-console-and-api-access-at-creation	Configuration change	iam.users
	iam-user-group-membership-check	Configuration change	iam.users
	iam-user-last-login-check	Periodic	iam.users
	iam-user-mfa-enabled	Configuration change	iam.users
	iam-user-single-access-key	Configuration change	iam.users
	mfa-enabled-for-iam-console-access	Configuration change	iam.users
	root-account-mfa-enabled	Periodic	iam.users
Document Database Service (DDS)	dds-instance-enable-ssl	Configuration change	dds.instances
	dds-instance-hamode	Configuration change	dds.instances

Service	Policy	Triggered By	Object
	dds-instance-has-eip	Configuration change	dds.instances
	dds-instance-in-vpc	Configuration change	dds.instances
Simple Message Notification (SMN)	smn-lts-enable	Configuration change	smn.topic
Virtual Private Cloud (VPC)	vpc-acl-unused-check	Configuration change	vpc.firewallGroups
	vpc-default-sg-closed	Configuration change	vpc.securityGroups
	vpc-flow-logs-enabled	Configuration change	vpc.vpcs
	vpc-sg-ports-check	Configuration change	vpc.securityGroups
	vpc-sg-restricted-common-ports	Configuration change	vpc.securityGroups
	vpc-sg-restricted-ssh	Configuration change	vpc.securityGroups
Virtual Private Network (VPN)	vpn-connections-active	Configuration change	vpnaas.vpnConnections, vpnaas.ipsec-site-connections
Cloud Eye	alarm-action-enabled-check	Configuration change	ces.alarms
	alarm-kms-disable-or-delete-key	Periodic	ces.alarms

Service	Policy	Triggered By	Object
	alarm-obs-bucket-policy-change	Periodic	ces.alarms
	alarm-resource-check	Periodic	ces.alarms
	alarm-settings-check	Configuration change	ces.alarms
	alarm-vpc-change	Periodic	ces.alarms
Cloud Container Engine (CCE)	cce-cluster-end-of-maintenance-version	Configuration change	cce.clusters
	cce-cluster-oldest-supported-version	Configuration change	cce.clusters
	cce-endpoint-public-access	Configuration change	cce.clusters
Cloud Trace Service (CTS)	cts-kms-encrypted-check	Configuration change	cts.trackers
	cts-lts-enable	Configuration change	cts.trackers
	cts-obs-bucket-track	Periodic	cts.trackers
	cts-support-validate-check	Configuration change	cts.trackers
	cts-tracker-exists	Periodic	cts.trackers
	multi-region-cts-tracker-exists	Periodic	cts.trackers
Relational Database Service (RDS)	gaussdb-instance-in-vpc	Configuration change	gaussdb.instance
	gaussdb-nosql-deploy-in-single-az	Configuration change	nosql.instances

Service	Policy	Triggered By	Object
	gaussdb-nosql-enable-backup	Configuration change	nosql.instances
	gaussdb-nosql-enable-disk-encryption	Configuration change	nosql.instances
	gaussdb-nosql-enable-error-log	Configuration change	nosql.instances
	gaussdb-nosql-support-slow-log	Configuration change	nosql.instances
	rds-instance-enable-backup	Configuration change	rds.instances
	rds-instance-enable-errorLog	Configuration change	rds.instances
	rds-instance-enable-slowLog	Configuration change	rds.instances
	rds-instance-multi-az-support	Configuration change	rds.instances
	rds-instance-no-public-ip	Configuration change	rds.instances
	rds-instances-enable-kms	Configuration change	rds.instances
	rds-instances-in-vpc	Configuration change	rds.instances
	rds-instance-logging-enabled	Configuration change	rds.instances
Cloud Search Service (CSS)	css-cluster-authority-enable	Configuration change	css.clusters

Service	Policy	Triggered By	Object
	css-cluster-backup-available	Configuration change	css.clusters
	css-cluster-disk-encryption-check	Configuration change	css.clusters
	css-cluster-https-required	Configuration change	css.clusters
	css-cluster-in-vpc	Configuration change	css.clusters
	css-cluster-multiple-az-check	Configuration change	css.clusters
	css-cluster-multiple-instances-check	Configuration change	css.clusters
	css-cluster-no-public-zone	Configuration change	css.clusters
	css-cluster-security-mode-enable	Configuration change	css.clusters
	css-cluster-not-enable-white-list	Configuration change	css.clusters
	css-cluster-kibana-not-enable-white-list	Configuration change	css.clusters
Elastic Volume Service (EVS)	**allowed-volume-specs**	Configuration changes	evs.volumes
	evs-use-in-specified-days	Periodic	evs.volumes
	volume-unused-check	Configuration changes	evs.volumes

Service	Policy	Triggered By	Object
	volumes-encrypted-check	Configuration change	evs.volumes
Cloud Certificate Manager (CCM)	pca-certificate-authority-expiration-check	Periodic	pca.ca
	pca-certificate-expiration-check	Periodic	pca.cert
Distributed Message Service (for Kafka)	dms-kafka-not-enable-private-ssl	Configuration change	dms.kafkas
	dms-kafka-not-enable-public-ssl	Configuration change	dms.kafkas
	dms-kafka-public-access-enabled-check	Configuration change	dms.kafkas
Distributed Message Service for RabbitMQ (for RabbitMQ)	dms-rabbitmq-not-enable-ssl	Configuration change	dms.rabbitmqs
Distributed Message Service for RocketMQ (for RocketMQ)	dms-rocketmq-not-enable-ssl	Configuration change	dms.reliabilitys

3.5.2 General Service Policies

3.5.2.1 regular-matching-of-names

Rule Details

Table 3-9 Rule details

Parameter	Description
Rule Name	regular-matching-of-names

Parameter	Description
Description	If a resource name does not comply with regular expression requirements, this name is considered noncompliant.
Tag	name
Trigger Type	Configuration change
Filter Type	All resources
Configure Rule Parameters	**regularExpression**: indicates the regular expression to be matched. **%** indicates any characters, and _ indicates a character.

3.5.2.2 required-tag-check

Rule Details

Table 3-10 Rule details

Parameter	Description
Rule Name	required-tag-check
Description	If a resource is not attached with the specified tag, this resource is considered noncompliant.
Tag	tag
Trigger Type	Configuration change
Filter Type	All resources
Configure Rule Parameters	• **specifiedTagKey**: indicates the tag key. A tag key must be a string. • **specifiedTagValue**: indicates tag values. If the value list is left empty, all values are allowed. A tag value must be an array. You can include up to 10 values.

NOTE

Currently, OBS and NAT do not support tag-related rules.

3.5.2.3 resource-in-enterprise-project

Rule Details

Table 3-11 Rule details

Parameter	Description
Rule Name	resource-in-enterprise-project
Description	If a resource is not included in a specified enterprise project ID, this resource is considered noncompliant.
Tag	enterprise project
Trigger Type	Configuration change
Filter Type	All resources
Configure Rule Parameters	**epId**: indicates the enterprise project ID. The value must be a string.

3.5.2.4 resources-in-supported-region

Rule Details

Table 3-12 Rule details

Parameter	Description
Rule Name	resources-in-supported-region
Description	If a resource is not in a specified region, this resource is noncompliant.
Tag	region
Trigger Type	Configuration change
Filter Type	All resources
Configure Rule Parameters	**regions**: indicates regions. The value must be an array. For global resources, the value of this parameter is **global**.

3.5.3 API Gateway (APIG)

3.5.3.1 apig-instances-authorization-type-configured

Rule Details

Table 3-13 Rule details

Parameter	Description
Rule Name	apig-instances-authorization-type-configured
Description	If security authentication is not provided for a dedicated API gateway, this gateway is non-compliant.
Tag	apig
Trigger Type	Configuration change
Filter Type	apig.instances
Configure Rule Parameters	None

3.5.3.2 apig-instances-execution-logging-enabled

Rule Details

Table 3-14 Rule details

Parameter	Description
Rule Name	apig-instances-execution-logging-enabled
Description	If access logs are not configured for a dedicated API gateway, this gateway is considered non-compliant.
Tag	apig
Trigger Type	Configuration change
Filter Type	apig.instances
Configure Rule Parameters	None

3.5.3.3 apig-instances-ssl-enabled

Rule Details

Table 3-15 Rule details

Parameter	Description
Rule Name	apig-instances-ssl-enabled
Description	If no SSL certificates are attached to a dedicated API gateway, this gateway is considered noncompliant.
Tag	apig
Trigger Type	Configuration changes
Filter Type	apig.instances
Configure rule parameters	None

3.5.4 CodeArts Deploy

3.5.4.1 codeartsdeploy-host-cluster-resource-status

Rule Details

Table 3-16 Rule details

Parameter	Description
Rule Name	codeartsdeploy-host-cluster-resource-status
Description	If the status of a cluster in the codearts project is unavailable, the cluster is noncompliant.
Tag	codeartsdeploy
Trigger Type	Configuration change
Filter Type	codeartsdeploy.host-cluster
Configure Rule Parameters	None

3.5.5 MapReduce Service (MRS)

3.5.5.1 mrs-cluster-in-allowed-security-groups

Rule Details

Table 3-17 Rule details

Parameter	Description
Rule Name	mrs-cluster-in-allowed-security-groups
Description	If an MRS cluster is not configured with a specified security group, the cluster is noncompliant.
Tag	mrs
Trigger Type	Configuration change
Filter Type	mrs.mrs
Configure Rule Parameters	**mrsSecurityGroupsId**: indicates security group IDs. This is an array type parameter.

3.5.5.2 mrs-cluster-in-vpc

Rule Details

Table 3-18 Rule Details

Parameter	Description
Rule Name	mrs-cluster-in-vpc
Description	If an MRS cluster is not in the specified VPC, this cluster is noncompliant.
Tag	mrs
Trigger Type	Configuration change
Filter Type	mrs.mrs
Configure rule parameters	**vpcId**: indicatew the VPC ID. This is a string type parameter.

3.5.5.3 mrs-cluster-kerberos-enabled

Rule Details

Table 3-19 Rule details

Parameter	Description
Rule Name	mrs-cluster-kerberos-enabled
Description	If kerberos authentication is not enabled for an MRS cluster, this cluster is noncompliant.
Tag	mrs
Trigger Type	Configuration change
Filter Type	mrs.mrs
Configure Rule Parameters	None

3.5.5.4 mrs-cluster-multiAZ-deployment

Rule Details

Table 3-20 Rule details

Parameter	Description
Rule Name	mrs-cluster-multiAZ-deployment
Description	If the nodes in a MapReduce cluster are not deployed across AZs, this cluster is noncompliant.
Tag	mrs
Trigger Type	Configuration change
Filter Type	mrs.mrs
Configure Rule Parameters	None

3.5.5.5 mrs-cluster-no-public-ip

Rule Details

Table 3-21 Rule details

Parameter	Description
Rule Name	mrs-cluster-no-public-ip
Description	If an MRS cluster is not attached with an EPI, this cluster is noncompliant.
Tag	mrs
Trigger Type	Configuration change
Filter Type	mrs.mrs
Configure Rule Parameters	None

3.5.6 NAT Gateway

3.5.6.1 private-nat-gateway-authorized-vpc-only

Rule Details

Table 3-22 Rule details

Parameter	Description
Rule Name	private-nat-gateway-authorized-vpc-only
Description	If a private NAT gateway is not in a specified VPC, this gateway is noncompliant.
Tag	nat
Trigger Type	Configuration change
Filter Type	nat.privateNatGateways
Configure Rule Parameters	**authorizedVpcIds**: indicates the IDs of the specified VPCs. If there are no VPCs specified, all values are allowed. This is an array type parameter. You can include up to 10 VPCs.

3.5.7 VPC Endpoint (VPCEP)

3.5.7.1 vpcep-endpoint-enabled

Rule Details

Table 3-23 Rule details

Parameter	Description
Rule Name	vpcep-endpoint-enabled
Description	If there are no VPC endpoints created with a specified service name, the result is noncompliant.
Tag	vpcep
Trigger Type	Periodic
Filter Type	vpcep.endpoints
Configure rule parameters	serviceName: indicates the specified service name

3.5.8 Web Application Firewall (WAF)

3.5.8.1 waf-instance-policy-not-empty

Rule Details

Table 3-24 Rule details

Parameter	Description
Rule name	waf-instance-policy-not-empty
Description	If no protection policy is configured for a WAF domain name, this domain name is noncompliant.
Tag	waf
Trigger Type	Configuration change
Filter Type	waf.instance
Configure Rule Parameters	None

3.5.9 Elastic Load Balance (ELB)

3.5.9.1 elb-loadbalancers-no-public-ip

Rule Details

Table 3-25 Rule details

Parameter	Description
Rule Name	elb-loadbalancers-no-public-ip
Description	If a load balancer has an EIP attached, this load balancer is noncompliant.
Tag	elb
Trigger Type	Configuration change
Filter Type	elb.loadbalancers
Configure Rule Parameters	None

3.5.9.2 elb-predefined-security-policy-https-check

Rule Details

Table 3-26 Rule details

Parameter	Description
Rule Name	elb-predefined-security-policy-https-check
Description	If a specified security policy is not configured for the HTTPS listener of a dedicated load balancer, this dedicated load balancer is noncompliant.
Tag	elb
Trigger Type	Configuration change
Filter Type	elb.loadbalancers
Configure Rule Parameters	**predefinedPolicyName**: indicates the the specified security policy. The default value is **tls-1-0**. Example values: tls-1-0, tls-1-1, tls-1-2, tls-1-0-inherit, tls-1-2-strict, tls-1-0-with-1-3, tls-1-2-fs-with-1-3, tls-1-2-fs, and hybrid-policy-1-0. For more information, see **TLS Security Policy**.

3.5.9.3 elb-tls-https-listeners-only

Rule Details

Table 3-27 Rule details

Parameter	Description
Rule Name	elb-tls-https-listeners-only
Description	If any listener of a load balancer is not configured with HTTPS, this load balancer is noncompliant.
Tag	elb
Trigger Type	Configuration change
Filter Type	elb.loadbalancers
Configure Rule Parameters	None

3.5.9.4 elb-members-weight-check

Rule Details

Table 3-28 Rule details

Parameter	Description
Rule Name	elb-members-weight-check
Description	If the weight of a backend server is 0 and the load balancing algorithm of the backend server group to which the backend server belongs is not SOUCE_IP, the result is noncompliant.
Tag	elb
Trigger Type	Configuration change
Filter Type	elb.members
Configure Rule Parameters	**weight**: the weight of the backend server. Requests are routed to backend servers in the same backend server group based on their weights. The larger the weight is, the more requests the backend server receives. Value range: 0–100

3.5.10 Elastic IP (EIP)

3.5.10.1 eip-bandwidth-limit

Rule Details

Table 3-29 Rule details

Parameter	Description
Rule Name	eip-bandwidth-limit
Description	If the bandwidth of an EIP is smaller than a specified size, the EIP is noncompliant.
Tag	eip
Trigger Type	Configuration change
Filter Type	vpc.publicips
Configure Rule Parameters	**bandwidthSize**: indicates the bandwidth size of an EIP. The unit is Mbit/s. This is a string type parameter.

3.5.10.2 eip-unbound-check

Rule Details

Table 3-30 Rule details

Parameter	Description
Rule Name	eip-unbound-check
Description	If an EIP has not been attached to any resource, this EIP is noncompliant.
Tag	vpc
Trigger Type	Configuration change
Filter Type	vpc.publicips
Configure Rule Parameters	None

3.5.10.3 eip-use-in-specified-days

Rule Details

Table 3-31 Rule details

Parameter	Description
Rule Name	eip-use-in-specified-days
Description	If an EIP is not used within a specified number of days after being created, the EIP is noncompliant.
Tag	eip
Trigger Type	Periodic
Filter Type	vpc.publicips
Configure Rule Parameters	**allowDays**: indicates the maximum number of days that an EIP is allowed to remain unused. This is a numeric type parameter.

3.5.11 Auto Scaling (AS)

3.5.11.1 as-capacity-rebalancing

Rule Details

Table 3-32 Rule details

Parameter	Description
Rule Name	as-capacity-rebalancing
Description	If the priority policy EQUILIBRIUM_DISTRIBUTE is not used when an AS group scales in or out, the AS group is noncompliant.
Tag	as
Trigger Type	Configuration change
Filter Type	as.scalingGroups
Configure Rule Parameters	None

3.5.11.2 as-group-elb-healthcheck-required

Rule Details

Table 3-33 Rule details

Parameter	Description
Rule Name	as-group-elb-healthcheck-required
Description	If health check is not enabled for an Auto Scaling group, this Auto Scaling group is noncompliant.
Tag	as
Trigger Type	Configuration change
Filter Type	as.scalingGroups
Configure Rule Parameters	None

3.5.11.3 as-multiple-az

Rule Details

Table 3-34 Rule details

Parameter	Description
Rule Name	as-multiple-az
Description	If an AS group is not deployed across AZs, this AS group is noncompliant.
Tag	as
Trigger Type	Configuration change
Filter Type	as.scalingGroups
Configure Rule Parameters	None

3.5.12 Scalable File Service (SFS)

3.5.12.1 sfsturbo-encrypted-check

Rule Details

Table 3-35 Rule details

Parameter	Description
Rule Name	sfsturbo-encrypted-check
Description	If an SFS Turbo file system is not encrypted using KMS, this file system is noncompliant.
Tag	sfsturbo
Trigger Type	Configuration change
Filter Type	sfsturbo.shares
Configure Rule Parameters	None

3.5.13 Elastic Cloud Server (ECS)

3.5.13.1 allowed-ecs-flavors

Rule Details

Table 3-36 Rule details

Parameter	Description
Rule Name	allowed-ecs-flavors
Description	If the flavor of an ECS is not in the specified flavor range, this ECS is noncompliant.
Tag	ecs
Trigger Type	Configuration change
Filter Type	ecs.cloudservers
Configure Rule Parameters	**listOfAllowedFlavors**: indicates the list of allowed ECS flavors. The value must be an array with up to 10 elements. Example ECS flavors are as follows: s6.small.1, s6.xlarge.2, m7.large.8, and t6.small.1. To get more details, see ECS documentation.

3.5.13.2 allowed-images-by-id

Rule Details

Table 3-37 Rule details

Parameter	Description
Rule Name	allowed-images-by-id
Description	If the image of an ECS is not within the specified image IDs, this ECS is noncompliant.
Tag	ecs, ims
Trigger Type	Configuration change
Filter Type	ecs.cloudservers
Configure Rule Parameters	**listOfAllowedImages**: indicates the list of allowed image IDs. The value must be an array with up to 10 elements.

3.5.13.3 approved-ims-by-tag

Rule Details

Table 3-38 Rule details

Parameter	Description
Rule Name	approved-ims-by-tag
Description	If the image of an ECS is not within the specified images with a specific tag, this ECS is noncompliant.
Tag	ecs, ims
Trigger Type	Configuration change
Filter Type	ecs.cloudservers
Configure Rule Parameters	• **specifiedIMSTagKey**: indicates the tag key of the specified images. The value must be a string. • **specifiedIMSTagValue**: indicates the tag value list of the specified images. If the list is left blank, all values are allowed. The value must be an array with up to 10 elements.

3.5.13.4 ecs-in-allowed-security-groups

Rule Details

Table 3-39 Rule details

Parameter	Description
Rule Name	ecs-in-allowed-security-groups
Description	If an ECS does not have the specified tag and is not in the specified security groups, this ECS is noncompliant.
Tag	ecs
Trigger Type	Configuration change
Filter Type	ecs.cloudservers
Configure Rule Parameters	• **specifiedECSTagKey**: indicates the tag key of the specified ECS. The value must be a string. • **specifiedECSTagValue**: indicates the tag value list of the specified ECS. If the list is left blank, all values are allowed. The value must be an array with up to 10 elements. • **specifiedSecurityGroupIds**: indicates the ID list of specified high-risk security groups. The value must be an array with up to 10 IDs.

3.5.13.5 ecs-instance-in-vpc

Rule Details

Table 3-40 Rule details

Parameter	Description
Rule Name	ecs-instance-in-vpc
Description	If an ECS is not in a specified VPC, this ECS is noncompliant.
Tag	ecs, vpc
Trigger Type	Configuration change
Filter Type	ecs.cloudservers
Configure Rule Parameters	**vpcId**: indicates the VPC ID. The value must be a string.

3.5.13.6 ecs-instance-key-pair-login

Rule Details

Table 3-41 Rule details

Parameter	Description
Rule Name	ecs-instance-key-pair-login
Description	If no key pairs are configured for an ECS, this ECS is noncompliant.
Tag	ecs
Trigger Type	Configuration change
Filter Type	ecs.cloudservers
Configure Rule Parameters	None

3.5.13.7 ecs-instance-no-public-ip

Rule Details

Table 3-42 Rule details

Parameter	Description
Rule Name	ecs-instance-no-public-ip
Description	If an ECS has an EIP, this ECS is noncompliant.
Tag	ecs
Trigger Type	Configuration change
Filter Type	ecs.cloudservers
Configure Rule Parameters	None

3.5.13.8 ecs-multiple-public-ip-check

Rule Details

Table 3-43 Rule details

Parameter	Description
Rule Name	ecs-multiple-public-ip-check
Description	If an ECS has multiple EIPs, this ECS is noncompliant.
Tag	ecs
Trigger Type	Configuration change
Filter Type	ecs.cloudservers
Configure Rule Parameters	None

3.5.13.9 stopped-ecs-date-diff

Rule Details

Table 3-44 Rule details

Parameter	Description
Rule Name	stopped-ecs-date-diff
Description	If an ECS has been stopped for longer than the time allowed, this ECS is noncompliant.
Tag	ecs
Trigger Type	Periodic
Filter Type	ecs.cloudservers
Configure Rule Parameters	**allowDays**: indicates the number of days allowed. The value must be a string.

3.5.14 Distributed Cache Service (DCS)

3.5.14.1 dcs-memcached-enable-ssl

Rule Details

Table 3-45 Rule details

Parameter	Description
Name	dcs-memcached-enable-ssl
Description	If a DCS Memcached instance can be accessed through public networks but does not support SSL, this instance is noncompliant.
Tag	dcs
Trigger Type	Configuration change
Filter Type	dcs.memcached
Configure Rule Parameters	None

3.5.14.2 dcs-memcached-in-vpc

Rule Details

Table 3-46 Rule details

Parameter	Description
Rule Name	dcs-memcached-in-vpc
Description	If a DCS Redis instance is not in the specified VPC, this instance is noncompliant.
Tag	dcs
Trigger Type	Configuration change
Filter Type	dcs.memcached
Configure Rule Parameters	**vpcId**: indicates the VPC ID. The value must be a string.

3.5.14.3 dcs-memcached-no-public-ip

Rule Details

Table 3-47 Rule details

Parameter	Description
Rule Name	dcs-memcached-no-public-ip
Description	If a DCS Memcached instance is configured with a public IP address, this instance is noncompliant.
Tag	dcs
Trigger Type	Configuration change
Filter Type	dcs.memcached
Configure Rule Parameters	None

3.5.14.4 dcs-memcached-password-access

Rule Details

Table 3-48 Rule details

Parameter	Description
Rule Name	dcs-memcached-password-access
Description	If a DCS Memcached instance can be accessed without passwords, this instance is noncompliant.
Tag	dcs
Trigger Type	Configuration change
Filter Type	dcs.memcached
Configure Rule Parameters	None

3.5.14.5 dcs-redis-enable-ssl

Rule Details

Table 3-49 Rule details

Parameter	Description
Rule Name	dcs-redis-enable-ssl
Description	If a DCS Redis instance can be accessed over public networks but does not support SSL, this instance is noncompliant.
Tag	dcs
Trigger Type	Configuration change
Filter Type	dcs.redis
Configure Rule Parameters	None

3.5.14.6 dcs-redis-high-tolerance

Rule Details

Table 3-50 Rule details

Parameter	Description
Rule Name	dcs-redis-high-tolerance
Description	If a DCS Redis instance is not highly available, the instance is noncompliant.
Tag	dcs
Trigger Type	Configuration change
Filter Type	dcs.redis
Configure Rule Parameters	None

3.5.14.7 dcs-redis-in-vpc

Rule Details

Table 3-51 Rule details

Parameter	Description
Rule Name	dcs-redis-in-vpc
Description	If a DCS Redis instance is not in the specified VPC, this instance is noncompliant.
Tag	dcs
Trigger Type	Configuration change
Filter Type	dcs.redis
Configure Rule Parameters	**vpcId**: indicates the VPC ID. The value must be a string.

3.5.14.8 dcs-redis-no-public-ip

Rule Details

Table 3-52 Rule details

Parameter	Description
Rule Name	dcs-redis-no-public-ip
Description	If a DCS Redis instance is configured with a public IP address, the instance is noncompliant.
Tag	dcs
Trigger Type	Configuration change
Filter Type	dcs.redis
Configure Rule Parameters	None

3.5.14.9 dcs-redis-password-access

Rule Details

Table 3-53 Rule details

Parameter	Description
Rule Name	dcs-redis-password-access
Description	If a DCS Redis instance can be accessed without passwords, this instance is noncompliant.
Tag	dcs
Trigger Type	Configuration change
Filter Type	dcs.redis
Configure Rule Parameters	None

3.5.15 FunctionGraph

3.5.15.1 function-graph-concurrency-check

Rule Details

Table 3-54 Rule details

Parameter	Description
Rule Name	function-graph-concurrency-check
Description	If the number of concurrent requests of a function is not within the specified range, this function is noncompliant.
Tag	fgs
Trigger Type	Configuration change
Filter Type	fgs.functions
Configure Rule Parameters	• **concurrencyLimitLow**: indicates the minimum number of concurrent requests. The value must be an integer. • **concurrencyLimitHigh**: indicates the maximum number of concurrent requests. The value must be an integer.

3.5.15.2 function-graph-inside-vpc

Rule Details

Table 3-55 Rule details

Parameter	Description
Rule Name	function-graph-inside-vpc
Description	If a function does not use a specified VPC, this function is noncompliant.
Tag	fgs
Trigger Type	Configuration change
Filter Type	fgs.functions
Configure Rule Parameters	**vpcId**: indicates the VPC ID. The value must be a string.

3.5.15.3 function-graph-public-access-prohibited

Rule Details

Table 3-56 Rule details

Parameter	Description
Rule Name	function-graph-public-access-prohibited
Description	If a function allows access to public networks, this function is non-compliant.
Tag	fgs
Trigger Type	Configuration change
Filter Type	fgs.functions
Configure Rule Parameters	None

3.5.15.4 function-graph-settings-check

Rule Details

Table 3-57 Rule details

Parameter	Description
Rule Name	function-graph-settings-check
Description	If the runtime, timeout, or memory limit of a function is not within the specified range, this function is noncompliant.
Tag	fgs
Trigger Type	Configuration change
Filter Type	fgs.functions
Configure Rule Parameters	• **runtimeList**: indicates the runtime list. The value must be an array. • **timeout**: indicates the maximum amount of time that a client waits for a request to complete (in seconds). The value must be an integer. • **memorySize**: indicates maximum memory size (MB). The value must be an integer.

3.5.16 Content Delivery Network (CDN)

3.5.16.1 cdn-enable-https-certificate

Rule Details

Table 3-58 Rule details

Parameter	Description
Rule Name	cdn-enable-https-certificate
Description	If a domain name in CDN does not use HTTPS certificates, this domain name is noncompliant.
Tag	cdn
Trigger Type	Configuration change
Filter Type	cdn.domains
Configure Rule Parameters	None

3.5.16.2 cdn-origin-protocol-no-http

Rule Details

Table 3-59 Rule details

Parameter	Description
Rule Name	cdn-origin-protocol-no-http
Description	If the **Origin Protocol** is not set to **HTTPS** for a domain name added in CDN, this domain name is noncompliant.
Tag	cdn
Trigger Type	Configuration change
Filter Type	cdn.domains
Configure Rule Parameters	None

3.5.16.3 cdn-security-policy-check

Rule Details

Table 3-60 Rule details

Parameter	Description
Rule Name	cdn-security-policy-check
Description	If a domain name in CDN uses a TLS version earlier than v1.2, this domain name is noncompliant.
Tag	cdn
Trigger Type	Configuration change
Filter Type	cdn.domains
Configure Rule Parameters	None

3.5.16.4 cdn-use-my-certificate

Rule Details

Table 3-61 Rule details

Parameter	Description
Rule Name	cdn-use-my-certificate
Description	If **Certificate Source** is set to **My certificate** for a domain name in CDN, this domain name is noncompliant.
Tag	cdn
Trigger Type	Configuration change
Filter Type	cdn.domains
Configure Rule Parameters	None

3.5.17 Config

3.5.17.1 tracker-config-enabled-check

Rule Details

Table 3-62 Rule details

Parameter	Description
Rule Name	tracker-config-enabled-check
Description	An account is noncompliant if its Resource Recorder is not enabled.
Tag	config
Trigger Type	Periodic
Filter Type	config.trackers
Configure Rule Parameters	None

3.5.18 Data Warehouse Service (DWS)

3.5.18.1 dws-enable-kms

Rule Details

Table 3-63 Rule details

Parameter	Description
Rule Name	dws-enable-kms
Description	If KMS encryption is not enabled for a DWS cluster, this cluster is noncompliant.
Tag	dws
Trigger Type	Configuration change
Filter Type	dws.clusters
Configure Rule Parameters	None

3.5.18.2 dws-enable-log-dump

Rule Details

Table 3-64 Rule details

Parameter	Description
Rule Name	dws-enable-log-dump
Description	If the log dump is not enabled for a DWS cluster, this cluster is noncompliant.
Tag	dws
Trigger Type	Configuration change
Filter Type	dws.clusters
Configure Rule Parameters	None

3.5.18.3 dws-enable-snapshot

Rule Details

Table 3-65 Rule details

Parameter	Description
Rule Name	dws-enable-snapshot
Description	If snapshots are not enabled for a DWS cluster, this cluster is noncompliant.
Tag	dws
Trigger Type	Configuration change
Filter Type	dws.clusters
Configure Rule Parameters	None

3.5.18.4 dws-enable-ssl

Rule Details

Table 3-66 Rule details

Parameter	Description
Rule Name	dws-enable-ssl
Description	If SSL is not enabled for a Data Warehouse Service (DWS) cluster, this cluster is noncompliant.
Tag	dws
Trigger Type	Configuration change
Filter Type	dws.clusters
Configure Rule Parameters	None

3.5.19 Data Replication Service (DRS)

3.5.19.1 drs-data-guard-job-not-public

Rule Details

Table 3-67 Rule details

Parameter	Description
Rule Name	drs-data-guard-job-not-public
Description	If real-time DR task with DRS is implemented through a public network, this DR task is non-compliant.
Tag	drs
Trigger Type	Configuration change
Filter Type	drs.dataGuardJob
Configure Rule Parameters	None

3.5.19.2 drs-migration-job-not-public

Rule Details

Table 3-68 Rule details

Parameter	Description
Rule Name	drs-migration-job-not-public
Description	If a real-time migration task with RDS is implemented over a public network, this migration task is non-compliant.
Tag	drs
Trigger Type	Configuration change
Filter Type	drs.migrationJob
Configure Rule Parameters	None

3.5.19.3 drs-synchronization-job-not-public

Rule Details

Table 3-69 Rule details

Parameter	Description
Rule Name	drs-synchronization-job-not-public
Description	If a real-time synchronization with RDS is implemented over a public network, this synchronization task is non-compliant.
Tag	drs
Trigger Type	Configuration change
Filter Type	drs.synchronizationJob
Configure Rule Parameters	None

3.5.20 Data Encryption Workshop (DEW)

3.5.20.1 kms-not-scheduled-for-deletion

Rule Details

Table 3-70 Rule details

Parameter	Description
Rule Name	kms-not-scheduled-for-deletion
Description	This rule identifies KMS keys that are scheduled for deletion.
Tag	kms
Trigger Type	Configuration change
Filter Type	kms.keys
Configure Rule Parameters	None

3.5.20.2 kms-rotation-enabled

Rule Details

Table 3-71 Rule details

Parameter	Description
Rule Name	kms-rotation-enabled
Description	If key rotation is not enabled for a KMS key, this key is noncompliant.
Tag	kms
Trigger Type	Configuration change
Filter Type	kms.keys
Configure Rule Parameters	None

3.5.21 Identity and Access Management (IAM)

3.5.21.1 access-keys-rotated

Rule Details

Table 3-72 Rule details

Parameter	Description
Rule Name	access-keys-rotated
Description	If the AK/SK is not changed within the specified time for an IAM user, this user is noncompliant.
Tag	iam
Trigger Type	Periodic
Filter Type	iam.users
Configure Rule Parameters	**maxAccessKeyAge**: indicates the maximum number of days that the AK/SK is allowed to remain unchanged. The default value is 90 days.

3.5.21.2 iam-customer-policy-blocked-kms-actions

Rule Details

Table 3-73 Rule details

Parameter	Description
Rule Name	iam-customer-policy-blocked-kms-actions
Description	If there is a deny action for KMS in an IAM policy, this policy is noncompliant.
Tag	iam
Trigger Type	Configuration change
Filter Type	iam.roles, iam.policies
Configure Rule Parameters	**blockedActionsPatterns**: indicates deny actions for KMS. The value must be an array.

3.5.21.3 iam-group-has-users-check

Rule Details

Table 3-74 Rule details

Parameter	Description
Rule Name	iam-group-has-users-check
Description	If an IAM user group has no user, this user group is noncompliant.
Tag	iam
Trigger Type	Configuration change
Filter Type	iam.groups
Configure Rule Parameters	None

3.5.21.4 iam-password-policy

Rule Details

Table 3-75 Rule details

Parameter	Description
Rule Name	iam-password-policy
Description	If the password of an IAM user does not meet the password complexity requirements, this user is noncompliant.
Tag	iam
Trigger Type	Configuration change
Filter Type	iam.users
Configure Rule Parameters	**pwdStrength**: indicates the password strength. Values include **Strong**, **Medium**, and **Low**. The default value is **Strong**.

3.5.21.5 iam-policy-blacklisted-check

Rule Details

Table 3-76 Rule details

Parameter	Description
Rule Name	iam-policy-blacklisted-check
Description	If a blacklisted policy is attached to an IAM user or user group, or is included in an IAM agency, the user, user group, or agency is noncompliant.
Tag	iam
Trigger Type	Configuration change
Filter Type	iam.users, iam.groups, iam.agencies
Configure Rule Parameters	**blackListPolicyUrns**: indicates the blacklisted policy list. The value must be an array.

3.5.21.6 iam-policy-no-statements-with-admin-access

Rule Details

Table 3-77 Rule details

Parameter	Description
Rule Name	iam-policy-no-statements-with-admin-access
Description	If an IAM policy grants the admin permission (***:*:***, ***:***, or *****), this policy is noncompliant.
Tag	iam
Trigger Type	Configuration change
Filter Type	iam.roles, iam.policies
Configure Rule Parameters	None

3.5.21.7 iam-role-has-all-permissions

Rule Details

Table 3-78 Rule details

Parameter	Description
Rule Name	iam-role-has-all-permissions
Description	If an IAM custom policy contains ***:*** in the **allow** section, this policy is noncompliant.
Tag	iam
Trigger Type	Configuration change
Filter Type	iam.roles, iam.policies
Configure Rule Parameters	None

3.5.21.8 iam-root-access-key-check

Rule Details

Table 3-79 Rule details

Parameter	Description
Rule Name	iam-root-access-key-check
Description	An account is noncompliant if the account have active access key.
Tag	iam
Trigger Type	Periodic
Filter Type	iam.users
Configure Rule Parameters	None

3.5.21.9 iam-user-access-mode

Rule Details

Table 3-80 Rule details

Parameter	Description
Rule Name	iam-user-access-mode
Description	If both console access and API access are enabled for an IAM user, this user is noncompliant.
Tag	iam
Trigger Type	Configuration change
Filter Type	iam.users
Configure Rule Parameters	None

3.5.21.10 iam-user-console-and-api-access-at-creation

Rule Details

Table 3-81 Rule details

Parameter	Description
Rule Name	iam-user-console-and-api-access-at-creation
Description	If an AK/SK is configured for a user during user creation, this user is noncompliant.
Tag	iam
Trigger Type	Configuration change
Filter Type	iam.users
Configure Rule Parameters	None

3.5.21.11 iam-user-group-membership-check

Rule Details

Table 3-82 Rule details

Parameter	Description
Rule Name	iam-user-group-membership-check
Description	If an IAM user is not added to any IAM user groups, this user is noncompliant.
Tag	iam
Trigger Type	Configuration change
Filter Type	iam.users
Configure Rule Parameters	**groupIds**: indicates the ID list of the specified user groups. If the list is left blank, all values are allowed. The value must be an array with up to 10 elements.

3.5.21.12 iam-user-last-login-check

Rule Details

Table 3-83 Rule details

Parameter	Description
Rule Name	iam-user-last-login-check
Description	If an IAM user does not log in to the system within a specified time range, this user is non-compliant.
Tag	iam
Trigger Type	Periodic
Filter Type	iam.users
Configure Rule Parameters	**allowedInactivePeriod**: indicates the time range. The value must be an integer.

3.5.21.13 iam-user-mfa-enabled

Rule Details

Table 3-84 Rule details

Parameter	Description
Rule Name	iam-user-mfa-enabled
Description	If MFA is not enabled for an IAM user, this user is noncompliant.
Tag	iam
Trigger Type	Configuration change
Filter Type	iam.users
Configure Rule Parameters	None

3.5.21.14 iam-user-single-access-key

Rule Details

Table 3-85 Rule details

Parameter	Description
Rule Name	iam-user-single-access-key
Description	If multiple AKs/SKs are in the active state for an IAM user, this user is noncompliant.
Tag	iam
Trigger Type	Configuration change
Filter Type	iam.users
Configure Rule Parameters	None

3.5.21.15 mfa-enabled-for-iam-console-access

Rule Details

Table 3-86 Rule details

Parameter	Description
Rule Name	mfa-enabled-for-iam-console-access
Description	If MFA is not enabled for an IAM user who signs in to the management console using a password, this IAM user is noncompliant.
Tag	iam
Trigger Type	Configuration change
Filter Type	iam.users
Configure Rule Parameters	None

3.5.21.16 root-account-mfa-enabled

Rule Details

Table 3-87 Rule details

Parameter	Description
Rule Name	root-account-mfa-enabled
Description	An account is noncompliant if the root iam user does not have multi-factor authentication (MFA) enabled.
Tag	iam
Trigger Type	Periodic
Filter Type	iam.users
Configure Rule Parameters	None

3.5.22 Document Database Service (DDS)

3.5.22.1 dds-instance-enable-ssl

Rule Details

Table 3-88 Rule details

Parameter	Description
Rule Name	dds-instance-enable-ssl
Description	If SSL is not enabled for a DDS instance, this instance is noncompliant.
Tag	dds
Trigger Type	Configuration change
Filter Type	dds.instances
Configure Rule Parameters	None

3.5.22.2 dds-instance-hamode

Rule Details

Table 3-89 Rule details

Parameter	Description
Rule Name	dds-instance-hamode
Description	If a DDS instance is inconsistent with the specified type, this instance is noncompliant.
Tag	dds
Trigger Type	Configuration change
Filter Type	dds.instances
Configure Rule Parameters	**haMode**: indicates the specified instance type. The value must be a string.

3.5.22.3 dds-instance-has-eip

Rule Details

Table 3-90 Rule details

Parameter	Description
Rule Name	dds-instance-has-eip
Description	If a DDS instance is attached with a public IP, this instance is noncompliant.
Tag	dds
Trigger Type	Configuration change
Filter Type	dds.instances
Configure Rule Parameters	None

3.5.22.4 dds-instance-in-vpc

Rule Details

Table 3-91 Rule details

Parameter	Description
Rule Name	dds-instance-in-vpc
Description	If a DDS MongoDB instance is not in the specified VPC, this instance is noncompliant.
Tag	dds
Trigger Type	Configuration change
Filter Type	dds.instances
Configure Rule Parameters	**vpcId**: indicates the VPC ID. The value must be a string.

3.5.23 Simple Message Notification (SMN)

3.5.23.1 smn-lts-enable

Rule Details

Table 3-92 Rule details

Parameter	Description
Name	smn-lts-enable
Description	If logging is not enabled for an SMN topic, the SMN topic is noncompliant.
Tag	smn
Trigger Type	Configuration change
Filter Type	smn.topic
Configure Rule Parameters	None

3.5.24 Virtual Private Cloud (VPC)

3.5.24.1 vpc-acl-unused-check

Rule Details

Table 3-93 Rule details

Parameter	Description
Rule Name	vpc-acl-unused-check
Description	If no subnets are included in an ACL, this ACL is noncompliant.
Tag	vpc
Trigger Type	Configuration change
Filter Type	vpc.firewallGroups
Configure Rule Parameters	None

3.5.24.2 vpc-default-sg-closed

Rule Details

Table 3-94 Rule details

Parameter	Description
Rule Name	vpc-default-sg-closed
Description	If a default security group of a VPC allows all inbound or outbound traffic, this security group is non-compliant.
Tag	vpc
Trigger Type	Configuration change
Filter Type	vpc.securityGroups
Configure Rule Parameters	None

3.5.24.3 vpc-flow-logs-enabled

Rule Details

Table 3-95 Rule details

Parameter	Description
Rule Name	vpc-flow-logs-enabled
Description	If flow logs are not enabled for a VPC, this VPC is noncompliant.
Tag	vpc
Trigger Type	Configuration change
Filter Type	vpc.vpcs
Configure Rule Parameters	None

3.5.24.4 vpc-sg-ports-check

Rule Details

Table 3-96 Rule details

Parameter	Description
Rule Name	vpc-sg-ports-check
Description	If **Source** in an inbound rule of a security group is set to **0.0.0.0/0** and inbound traffic over all TCP/UDP ports are allowed, this security group is noncompliant.
Tag	vpc
Trigger Type	Configuration change
Filter Type	vpc.securityGroups
Configure Rule Parameters	None

3.5.24.5 vpc-sg-restricted-common-ports

Rule Details

Table 3-97 Rule details

Parameter	Description
Rule Name	vpc-sg-restricted-common-ports
Description	If a security group allows all IPv4 addresses (0.0.0.0/0) to access a port, this security group is noncompliant.
Tag	vpc
Trigger Type	Configuration change
Filter Type	vpc.securityGroups
Configure Rule Parameters	**blockedPorts**: indicates the list of ports to be restricted. This is an array type parameter. The default value is **20, 21, 3306, and 3389**. • **20**: File Transfer Protocol-data port • **21**: File Transfer Protocol-control port • **3306**: mysql port • **3389**: Remote Desktop Protocol port

3.5.24.6 vpc-sg-restricted-ssh

Rule Details

Table 3-98 Rule details

Parameter	Description
Rule Name	vpc-sg-restricted-ssh
Description	If the source address is set to **0.0.0.0/0** and the TCP 22 port is set to available, the security group is non-compliant.
Tag	vpc
Trigger Type	Configuration change
Filter Type	vpc.securityGroups
Configure Rule Parameters	None

3.5.25 Virtual Private Network (VPN)

3.5.25.1 vpn-connections-active

Rule Details

Table 3-99 Rule details

Parameter	Description
Rule Name	vpn-connections-active
Description	If the state of a VPN is not normal, this VPN is noncompliant.
Tag	vpnaas
Trigger Type	Configuration change
Filter Type	vpnaas.vpnConnections, vpnaas.ipsec-site-connections
Configure Rule Parameters	None

3.5.26 Cloud Eye

3.5.26.1 alarm-action-enabled-check

Rule Details

Table 3-100 Rule details

Parameter	Description
Rule Name	alarm-action-enabled-check
Description	If an alarm rule is not enabled, this rule is noncompliant.
Tag	ces
Trigger Type	Configuration change
Filter Type	ces.alarms
Configure Rule Parameters	None

3.5.26.2 alarm-kms-disable-or-delete-key

Rule Details

Table 3-101 Rule details

Parameter	Description
Rule Name	alarm-kms-disable-or-delete-key
Description	If there are no alarm rules configured for disabling KMS or deleting keys, the result is noncompliant.
Tag	ces, kms
Trigger Type	Periodic
Filter Type	ces.alarms
Configure Rule Parameters	None

3.5.26.3 alarm-obs-bucket-policy-change

Rule Details

Table 3-102 Rule details

Parameter	Description
Rule Name	alarm-obs-bucket-policy-change
Description	If there are no alarm rules configured for changing OBS bucket policies, the result is noncompliant.
Tag	ces, obs
Trigger Type	Periodic
Filter Type	ces.alarms
Configure Rule Parameters	None

3.5.26.4 alarm-resource-check

Rule Details

Table 3-103 Rule details

Parameter	Description
Rule Name	alarm-resource-check
Description	If a resource is not configured with a CES alarm rule, this resource is noncompliant.
Tag	ces
Trigger Type	Periodic
Filter Type	ces.alarms
Configure Rule Parameters	• **provider**: indicates a cloud service name. The value must be a string. • **resourceType**: indicates a resource type. The value must be a string. • **metricName**: indicates a metric name. The value must be a string.

3.5.26.5 alarm-settings-check

Rule Details

Table 3-104 Rule details

Parameter	Description
Rule Name	alarm-settings-check
Description	If there are no alarm rules configured for a specified metric, the result is noncompliant.
Tag	ces
Trigger Type	Configuration change
Filter Type	ces.alarms

Parameter	Description
Configure Rule Parameters	• **metricName**: indicates a metric name. The value must be a string. • **threshold**: indicates an alarm threshold. The value must be a string. • **count**: indicates the number of consecutive occurrences specified to trigger an alarm. The value must be a string. • **period**: indicates the monitoring data granularity. The value must be a string. • **comparisonOperator**: indicates the operator. This is a string type parameter. >, =, <, >=, and <= are supported. • **filter**: indicates data aggregation method. The value must be a string.

3.5.26.6 alarm-vpc-change

Rule Details

Table 3-105 Rule details

Parameter	Description
Rule Name	alarm-vpc-change
Description	If no alarm rules are configured for monitoring VPC changes, the result is noncompliant.
Tag	ces, vpc
Trigger Type	Periodic
Filter Type	ces.alarms
Configure Rule Parameters	None

3.5.27 Cloud Container Engine (CCE)

3.5.27.1 cce-cluster-end-of-maintenance-version

Rule Details

Table 3-106 Rule details

Parameter	Description
Rule Name	cce-cluster-end-of-maintenance-version
Description	If the version of a CCE cluster is not supported for maintenance, this cluster is non-compliant.
Tag	cce
Trigger Type	Configuration change
Filter Type	cce.clusters
Configure Rule Parameters	None

3.5.27.2 cce-cluster-oldest-supported-version

Rule Details

Table 3-107 Rule details

Parameter	Description
Rule Name	cce-cluster-oldest-supported-version
Description	If the version of a CCE cluster is the earliest among the versions supported, this cluster is non-compliant.
Tag	cce
Trigger Type	Configuration change
Filter Type	cce.clusters
Configure Rule Parameters	None

3.5.27.3 cce-endpoint-public-access

Rule Details

Table 3-108 Rule details

Parameter	Description
Rule Name	cce-endpoint-public-access
Description	If a public IP is attached to a CCE cluster, this cluster is non-compliant.
Tag	cce
Trigger Type	Configuration change
Filter Type	cce.clusters
Configure Rule Parameters	None

3.5.28 Cloud Trace Service (CTS)

3.5.28.1 cts-kms-encrypted-check

Rule Details

Table 3-109 Rule details

Parameter	Description
Rule Name	cts-kms-encrypted-check
Description	If a CTS tracker is not encrypted using KMS, this tracker is noncompliant.
Tag	cts
Trigger Type	Configuration change
Filter Type	cts.trackers
Configure Rule Parameters	None

3.5.28.2 cts-lts-enable

Rule Details

Table 3-110 Rule details

Parameter	Description
Rule Name	cts-lts-enable
Description	If trace analysis is not enabled for a CTS tracker, this tracker is noncompliant.
Tag	cts
Trigger Type	Configuration change
Filter Type	cts.trackers
Configure Rule Parameters	None

3.5.28.3 cts-obs-bucket-track

Rule Details

Table 3-111 Rule details

Parameter	Description
Rule Name	cts-obs-bucket-track
Description	An account is noncompliant if none of its CTS trackers track specified OBS buckets.
Tag	cts
Trigger Type	Periodic
Filter Type	cts.trackers
Configure Rule Parameters	**trackBucket**: indicates the name of a specified OBS bucket. The value must be a string.

3.5.28.4 cts-support-validate-check

Rule Details

Table 3-112 Rule details

Parameter	Description
Rule Name	cts-support-validate-check
Description	If a CTS tracker has trace file verification disabled, this tacker is noncompliant.
Tag	cts
Trigger Type	Configuration change
Filter Type	cts.trackers
Configure Rule Parameters	None

3.5.28.5 cts-tracker-exists

Rule Details

Table 3-113 Rule details

Parameter	Description
Rule Name	cts-tracker-exists
Description	An account is noncompliant if it does not have a CTS tracker.
Tag	cts
Trigger Type	Periodic
Filter Type	cts.trackers
Configure Rule Parameters	None

3.5.28.6 multi-region-cts-tracker-exists

Rule Details

Table 3-114 Rule details

Parameter	Description
Rule Name	multi-region-cts-tracker-exists
Description	An account is noncompliant if it does not have a CTS tracker in specified regions.
Tag	cts
Trigger Type	Periodic
Filter Type	cts.trackers
Configure Rule Parameters	**regionList**: indicates the specified region list. The value must be an array.

3.5.29 Relational Database Service (RDS)

3.5.29.1 gaussdb-instance-in-vpc

Rule Details

Table 3-115 Rule details

Parameter	Description
Rule Name	gaussdb-instance-in-vpc
Description	If a GaussDB instance is not in a specified VPC, this instance is noncompliant.
Tag	gaussdb
Trigger Type	Configuration change
Filter Type	gaussdb.instance
Configure Rule Parameters	**vpcId**: indicates the VPC ID. The value must be a string.

3.5.29.2 gaussdb-nosql-deploy-in-single-az

Rule Details

Table 3-116 Rule details

Parameter	Description
Rule Name	gaussdb-nosql-deploy-in-single-az
Description	If GaussDB NoSQL instances are deployed in a single AZ, the result is noncompliant.
Tag	gaussdb nosql
Trigger Type	Configuration change
Filter Type	nosql.instances
Configure Rule Parameters	None

3.5.29.3 gaussdb-nosql-enable-backup

Rule Details

Table 3-117 Rule details

Parameter	Description
Name	gaussdb-nosql-enable-backup
Description	If the backup is not enabled for a GaussDB NoSQL instance, this instance is noncompliant.
Tag	gaussdb nosql
Trigger Type	Configuration change
Filter Type	nosql.instances
Configure Rule Parameters	None

3.5.29.4 gaussdb-nosql-enable-disk-encryption

Rule Details

Table 3-118 Rule details

Parameter	Description
Name	gaussdb-nosql-enable-disk-encryption
Description	If KMS encryption is not enabled for a GaussDB NoSQL instance, this instance is noncompliant.
Tag	gaussdb nosql
Trigger Type	Configuration change
Filter Type	nosql.instances
Configure Rule Parameters	None

3.5.29.5 gaussdb-nosql-enable-error-log

Rule Details

Table 3-119 Rule details

Parameter	Description
Name	gaussdb-nosql-enable-error-log
Description	If error logs are not enabled for a GaussDB NoSQL instance, this instance is noncompliant.
Tag	gaussdb nosql
Trigger Type	Configuration change
Filter Type	nosql.instances
Configure Rule Parameters	None

3.5.29.6 gaussdb-nosql-support-slow-log

Rule Details

Table 3-120 Rule details

Parameter	Description
Name	gaussdb-nosql-support-slow-log
Description	If a GaussDB NoSQL does not support slow query logs, this instance is noncompliant.
Tag	gaussdb nosql
Trigger Type	Configuration change
Filter Type	nosql.instances
Configure Rule Parameters	None

3.5.29.7 rds-instance-enable-backup

Rule Details

Table 3-121 Rule details

Parameter	Description
Rule Name	rds-instance-enable-backup
Description	If the backup is not enabled for an RDS instance, this instance is noncompliant.
Tag	rds
Trigger Type	Configuration change
Filter Type	rds.instances
Configure Rule Parameters	None

3.5.29.8 rds-instance-enable-errorLog

Rule Details

Table 3-122 Rule details

Parameter	Description
Rule Name	rds-instance-enable-errorLog
Description	If the error logs is not enabled for an RDS instance, this instance is noncompliant.
Tag	rds
Trigger Type	Configuration change
Filter Type	rds.instances
Configure Rule Parameters	None

3.5.29.9 rds-instance-enable-slowLog

Rule Details

Table 3-123 Rule details

Parameter	Description
Rule Name	rds-instance-enable-slowLog
Description	If the slow query log is not enabled for an RDS instance, this instance is noncompliant.
Tag	rds
Trigger Type	Configuration change
Filter Type	rds.instances
Configure Rule Parameters	None

3.5.29.10 rds-instance-multi-az-support

Rule Details

Table 3-124 Rule details

Parameter	Description
Name	rds-instance-multi-az-support
Description	If RDS instances are all deployed in a single AZ, these instances are noncompliant.
Tag	rds
Trigger Type	Configuration change
Filter Type	rds.instances
Configure Rule Parameters	None

3.5.29.11 rds-instance-no-public-ip

Rule Details

Table 3-125 Rule details

Parameter	Description
Rule Name	rds-instance-no-public-ip
Description	If an RDS instance has an EIP, this instance is noncompliant.
Tag	rds
Trigger Type	Configuration change
Filter Type	rds.instances
Configure Rule Parameters	None

3.5.29.12 rds-instances-enable-kms

Rule Details

Table 3-126 Rule details

Parameter	Description
Rule Name	rds-instances-enable-kms
Description	If the storage encryption is not enabled for an RDS instance, this instance is noncompliant.
Tag	rds
Trigger Type	Configuration change
Filter Type	rds.instances
Configure Rule Parameters	None

3.5.29.13 rds-instances-in-vpc

Rule Details

Table 3-127 Rule details

Parameter	Description
Rule Name	rds-instances-in-vpc
Description	If an RDS instance is not in a specified VPC, this instance is noncompliant.
Tag	rds
Trigger Type	Configuration change
Filter Type	rds.instances
Configure Rule Parameters	**vpcId**: indicates the ID of a specified VPC. The value must be a string.

3.5.29.14 rds-instance-logging-enabled

Rule Details

Table 3-128 Rule details

Parameter	Description
Rule Name	rds-instance-logging-enabled
Description	RDS resources that do not enable any logs are considered non-compliant.
Tag	rds
Trigger Type	Configuration change
Filter Type	rds.instances
Configure Rule Parameters	None

3.5.30 Cloud Search Service (CSS)

3.5.30.1 css-cluster-authority-enable

Rule Details

Table 3-129 Rule details

Parameter	Description
Rule Name	css-cluster-authority-enable
Description	If authentication is not enabled for a CSS cluster, this cluster is noncompliant.
Tag	css
Trigger Type	Configuration change
Filter Type	css.clusters
Configure Rule Parameters	None

3.5.30.2 css-cluster-backup-available

Rule Details

Table 3-130 Rule details

Parameter	Description
Rule Name	css-cluster-backup-available
Description	If the snapshot is not enabled for a CSS cluster, this cluster is noncompliant.
Tag	css
Trigger Type	Configuration change
Filter Type	css.clusters
Configure Rule Parameters	None

3.5.30.3 css-cluster-disk-encryption-check

Rule Details

Table 3-131 Rule details

Parameter	Description
Rule Name	css-cluster-disk-encryption-check
Description	If disk encryption is not enabled for a CSS cluster, this cluster is noncompliant.
Tag	css
Trigger Type	Configuration change
Filter Type	css.clusters
Configure Rule Parameters	None

3.5.30.4 css-cluster-https-required

Rule Details

Table 3-132 Rule details

Parameter	Description
Rule Name	css-cluster-https-required
Description	If HTTPS is not enabled for a CSS cluster, this cluster is noncompliant.
Tag	css
Trigger Type	Configuration change
Filter Type	css.clusters
Configure Rule Parameters	None

3.5.30.5 css-cluster-in-vpc

Rule Details

Table 3-133 Rule details

Parameter	Description
Rule Name	css-cluster-in-vpc
Description	If a CSS cluster is not attached with specified VPCs, this cluster is noncompliant.
Tag	css
Trigger Type	Configuration change
Filter Type	css.clusters
Configure Rule Parameters	**authorizedVpcIds**: indicates the ID list of the specified VPCs. If the list is left blank, all values are allowed. The value must be an array with up to 10 elements.

3.5.30.6 css-cluster-multiple-az-check

Rule Details

Table 3-134 Rule details

Parameter	Description
Rule Name	css-cluster-multiple-az-check
Description	If a CSS cluster is deployed in a single AZ, this cluster is noncompliant.
Tag	css
Trigger Type	Configuration change
Filter Type	css.clusters
Configure Rule Parameters	None

3.5.30.7 css-cluster-multiple-instances-check

Rule Details

Table 3-135 Rule details

Parameter	Description
Rule Name	css-cluster-multiple-instances-check
Description	If a CSS cluster does not have multiple nodes deployed for disaster recovery, this cluster is noncompliant.
Tag	css
Trigger Type	Configuration change
Filter Type	css.clusters
Configure Rule Parameters	None

3.5.30.8 css-cluster-no-public-zone

Rule Details

Table 3-136 Rule details

Parameter	Description
Rule Name	css-cluster-no-public-zone
Description	If a CSS cluster can be accessed from a public network, this cluster is noncompliant.
Tag	css
Trigger Type	Configuration change
Filter Type	css.clusters
Configure Rule Parameters	None

3.5.30.9 css-cluster-security-mode-enable

Rule Details

Table 3-137 Rule details

Parameter	Description
Rule Name	css-cluster-security-mode-enable
Description	If the security mode is not enabled for a CSS cluster, this cluster is noncompliant.
Tag	css
Trigger Type	Configuration change
Filter Type	css.clusters
Configure Rule Parameters	None

3.5.30.10 css-cluster-not-enable-white-list

Rule Details

Table 3-138 Rule details

Parameter	Description
Rule Name	css-cluster-not-enable-white-list
Description	If a CSS cluster can be accessed by all IPs, this cluster is noncompliant.
Tag	css
Trigger Type	Configuration change
Filter Type	css.clusters
Configure Rule Parameters	None

3.5.30.11 css-cluster-kibana-not-enable-white-list

Rule Details

Table 3-139 Rule details

Parameter	Description
Rule Name	css-cluster-kibana-not-enable-white-list
Description	If all IPs can access Kibana in a CSS cluster, this cluster is noncompliant.
Tag	css
Trigger Type	Configuration change
Filter Type	css.clusters
Configure Rule Parameters	None

3.5.31 Elastic Volume Service (EVS)

3.5.31.1 allowed-volume-specs

Rule Details

Table 3-140 Rule details

Parameter	Description
Rule Name	allowed-volume-specs
Description	If an EVS disk is not in the specified disk range, this disk is noncompliant.
Tag	evs
Trigger Type	Configuration change
Filter Type	evs.volumes
Configure Rule Parameters	**listOfAllowedSpecs**: indicates the specified EVS disk list. The value must be an array with up to 10 elements. Optional fields to query EVS documentations are: SATA, SSD, SAS.

3.5.31.2 evs-use-in-specified-days

Rule Details

Table 3-141 Rule details

Parameter	Description
Rule Name	evs-use-in-specified-days
Description	If an EVS disk is not used within a specified number of days after being created, this EIP is noncompliant.
Tag	evs
Trigger Type	Periodic
Filter Type	evs.volumes
Configure Rule Parameters	**allowDays**: indicates the maximum number of days that an EIP is allowed to remain unused. This is a numeric type parameter.

3.5.31.3 volume-unused-check

Rule Details

Table 3-142 Rule details

Parameter	Description
Rule Name	volume-unused-check
Description	If an EVS disk is not mounted to any cloud server, this disk is noncompliant.
Tag	evs
Trigger Type	Configuration change
Filter Type	evs.volumes
Configure Rule Parameters	None

3.5.31.4 volumes-encrypted-check

Rule Details

Table 3-143 Rule details

Parameter	Description
Rule Name	volumes-encrypted-check
Description	If a mounted EVS disk is not encrypted, this disk is noncompliant.
Tag	evs, ecs
Trigger Type	Configuration change
Filter Type	evs.volumes
Configure Rule Parameters	None

3.5.32 Cloud Certificate Manager (CCM)

3.5.32.1 pca-certificate-authority-expiration-check

Rule Details

Table 3-144 Rule details

Parameter	Description
Rule Name	pca-certificate-authority-expiration-check
Description	If the expiration time is not specified for a private CA certificate, this certificate is noncompliant.
Tag	pca
Trigger Type	Periodic
Filter Type	pca.ca
Configure Rule Parameters	**daysToExpiration**: indicates the remaining days to expiration. This is an integer type parameter.

3.5.32.2 pca-certificate-expiration-check

Rule Details

Table 3-145 Rule details

Parameter	Description
Rule Name	pca-certificate-expiration-check
Description	If the expiration time is not specified for a private certificate, the certificate is noncompliant.
Tag	pca
Trigger Type	Periodic
Filter Type	pca.cert
Configure Rule Parameters	**daysToExpiration**: indicates the remaining days to expiration. This is an integer type parameter.

3.5.33 Distributed Message Service (for Kafka)

3.5.33.1 dms-kafka-not-enable-private-ssl

Rule Details

Table 3-146 Rule details

Parameter	Description
Rule Name	dms-kafka-not-enable-private-ssl
Description	If SSL is not enabled for intranet network access to a DMS Kafka instance, this instance is noncompliant.
Tag	dms
Trigger Type	Configuration change
Filter Type	dms.kafkas
Configure Rule Parameters	None

3.5.33.2 dms-kafka-not-enable-public-ssl

Rule Details

Table 3-147 Rule details

Parameter	Description
Rule Name	dms-kafka-not-enable-public-ssl
Description	If SSL is not enabled for internet access to a DMS Kafka instance, this instance is noncompliant.
Tag	dms
Trigger Type	Configuration change
Filter Type	dms.kafkas
Configure Rule Parameters	None

3.5.33.3 dms-kafka-public-access-enabled-check

Rule Details

Table 3-148 Rule Details

Parameter	Description
Rule Name	dms-kafka-public-access-enabled-check
Description	If a DMS Kafka instance can be accessed over internet, this instance is noncompliant.
Tag	dms
Trigger Type	Configuration change
Filter Type	dms.kafkas
Configure Rule Parameters	None

3.5.34 Distributed Message Service (for RabbitMQ)

3.5.34.1 dms-rabbitmq-not-enable-ssl

Rule Details

Table 3-149 Rule details

Parameter	Description
Rule Name	dms-rabbitmq-not-enable-ssl
Description	If SSL is not enabled for a DMS RabbitMQ instance, this instance is noncompliant.
Tag	dms
Trigger Type	Configuration change
Filter Type	dms.rabbitmqs
Configure Rule Parameters	None

3.5.35 Distributed Message Service (for RocketMQ)

3.5.35.1 dms-rocketmq-not-enable-ssl

Rule Details

Table 3-150 Rule details

Parameter	Description
Rule Name	dms-rocketmq-not-enable-ssl
Description	If SSL is not enabled for a DMS RocketMQ instance, this instance is noncompliant.
Tag	dms
Trigger Type	Configuration change
Filter Type	dms.reliabilitys
Configure Rule Parameters	None

3.6 Event Monitoring

Event monitoring allows you to query events and receive alarms when there are unexpected events. With event monitoring, resource compliance events are reported to Cloud Eye and alarms are generated when exceptional events occur.

Event monitoring is enabled by default. You can view monitoring details about system events on the Event Monitoring page. For details about event monitoring operations, see **Viewing Event Monitoring Data** and **Creating Alarm Notifications for Event Monitoring**.

NOTE

Currently, Config only supports Cloud Eye event monitoring in the CN North-Beijing4 region.

The following table lists supported events of Config.

Table 3-151 Config events supported by Cloud Eye

Event Source	Event Name	Event Level	Description	Solution	Impact
SYS.RMS	Noncompliance notification	Major	The evaluation result of a rule is noncompliant.	Modify noncompliant resource configurations.	None

Event Source	Event Name	Event Level	Description	Solution	Impact
SYS.RMS	Compliance notification	Info	The evaluation result of a rule changes from noncompliant to complaint.	None	None
SYS.RMS	Storing Config snapshots failed	Major	Config fails to store resource snapshots to OBS buckets.	Check related OBS bucket permissions.	Resource changes cannot be recorded.
SYS.RMS	Resource snapshots stored	Info	Config successfully stores resource snapshots to OBS buckets.	None	None
SYS.RMS	Storing resource history failed	Major	Config fails to store resource history to OBS buckets.	Check related OBS bucket permissions.	Resource history cannot be recorded.
SYS.RMS	Resource history stored	Info	Config successfully stores resource history to OBS buckets.	None	None
SYS.RMS	Sending resource change notifications failed	Major	Config fails to send resource change notifications through SMN.	Check related SMN topic permissions	Customers cannot receive resource change notifications.

Event Source	Event Name	Event Level	Description	Solution	Impact
SYS.RMS	Notifications of resource change sent	Info	Config successfully send resource change notifications through SMN.	None	None
SYS.RMS	Sending resource relationship change notifications failed	Major	Config fails to send resource relationship change notifications through SMN.	Check related SMN topic permissions.	Customers cannot receive resource relationship change notifications.
SYS.RMS	Resource relationship change notifications sent	Info	Config successfully send resource relationship change notifications through SMN.	None	None

4 Conformance Packages

4.1 Overview

Functions

A conformance package is a collection of rules. Config provides conformance packages for you to evaluate resource compliance against multiple rules at the same time and centrally query conformance data.

After a conformance package is created, the compliance rules included will be displayed in the rule list. These rules cannot be updated, disabled, or deleted separately. They can only be deleted together with the conformance package.

If you are an organization administrator or a delegated administrator of Config, you can add organization conformance packages and then deploy organization conformance packages to all member accounts in your organization.

Constraints and Limitation

- You can add up to 20 conformance packages (including organization conformance packages) and 500 rules in an account.
- The resource recorder must be enabled before you create a conformance package.

Concepts

Sample template

Sample templates are provided by Config for you to create conformance packages quickly. Sample templates are scenario-based with proper compliance rules and parameters.

Pre-defined conformance package

A pre-defined conformance package is created using a sample template. You only need to specify values for the package parameters.

Custom conformance package

A custom conformance package is created using a custom template with compliance rules defined by you. You can upload a package template or use a package template stored in an OBS bucket to create a package. A custom template must be a JSON file. Other file formats, such as tf or zip, are not supported.

Compliance data

Compliance data is the results of resource compliance evaluation against a conformance package. Conformance data includes the following:

- Package-level data: indicates the data generated when all compliance rules in a package is used to evaluate resources. If there is any noncompliant resource, the evaluation result is noncompliant. If no resources are noncompliant, the evaluation result is compliant.
- Rule-level data: indicates the data generated when a single rule in a package is used to evaluate resources. If there is any noncompliant resource, the evaluation result is noncompliant. If no resources are evaluated to be noncompliant, the evaluation result is compliant.
- Compliance score: specifies the percentage of compliant resources in a conformance package compared to the total number of resources evaluated with the package. A compliance score of 100 indicates that all resources evaluated are compliant. A score of 0 indicates that all resources evaluated are noncompliant.

  Figure 4-1 Compliance score formula:

$$\text{score} = \frac{\sum_{\text{policy\_assignment}} \text{compliant resource count}}{\sum_{\text{policy\_assignment}} \text{resource count}} \times 100\%$$

Stack:

A stack allows a rule to be created or deleted in a conformance package. Stack is a concept of RFS. For details, see **stack**.

Status

When you deploy a conformance package, the package may be in the status of:

- Deployed: A conformance package has been deployed.
- Deploying: A conformance package is being deployed.
- Abnormal: Conformance package deployment failed.
- Rolled back: Some rules in a conformance package failed to be created and were rolled back, and other created rules were deleted.
- Rolling back: Some rules in a conformance package failed to be created and were rolled back, and other created rules were being deleted.
- Rollback failed: Some rules in a conformance package failed to be created and to be rolled back. You can access RFS to check out the reasons.
- Deleting: Rules in a conformance package and the package are being deleted.

- Exception: Deleting a conformance package failed.

Authorization

Config rules are created and deleted using stacks of RFS. To deploy a conformance package, you need to obtain a corresponding RFS agency to grant you necessary permissions.

- Quick authorization: This option creates an agency named rms_conformance_pack_agency for you to create, update, or delete rules, and to create or delete a conformance package.
- Custom authorization: You can create an agency and perform custom authorization through IAM. The agency must contain required permissions for a compliance package to work properly. This agency must contain the permissions for RFS to create, update, or delete rules. For details about how to create an agency, see **Creating an Agency (by a Delegating Party)**.

4.2 Managing Conformance Packages

4.2.1 Creating a Conformance Package

Scenarios

A conformance package is a collection of compliance rules. The conformance package is compliance-scenario-based. You can use a sample or custom template to create a conformance package.

After a conformance package is created, your resources are evaluated against the rules of the package. Evaluations will continue to be initiated each time the package is triggered. You can also trigger evaluation for a single rule in the rule list page.

Constraints and Limitation

- You can add up to 20 conformance packages (including organization conformance packages) and 500 rules in an account.
- The resource recorder must be enabled before you create a conformance package.

Procedure

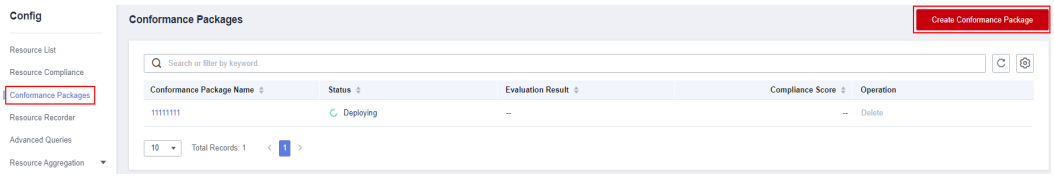
Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

Step 3 On the left navigation pane, choose **Conformance Package**.

Step 4 Click **Create Conformance Package**.

Figure 4-2 Creating conformance packages



Step 5 On the **Select Template** page, select a sample template, upload a local template, or enter an OBS template URL, and click **Next**.

- Sample template: templates provided by Config. You can select a sample template from the dropdown list.

  For details about the rules contained in each sample template, see **conformance package sample template**.

- Local template: templates uploaded locally. You can create a custom template and upload the template.

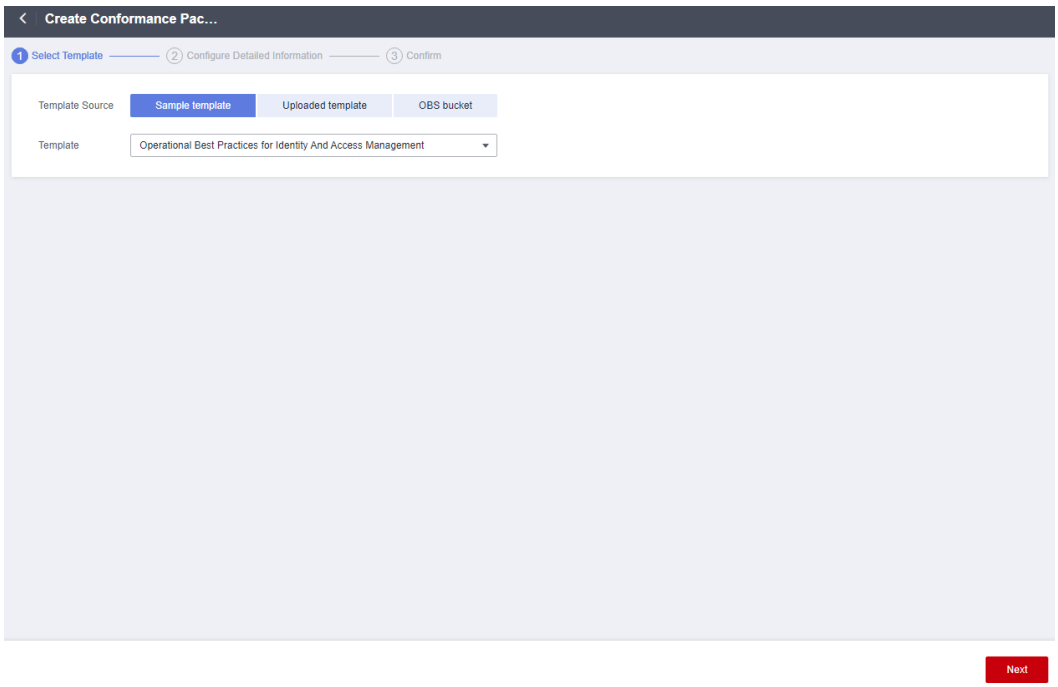
  Both the template file and content formats must be JSON. That is, the file name extension must be .tf.json. For details, see **custom conformance packages**.

- OBS bucket: URLs of the OBS buckets where custom conformance package templates are stored. If your local template file exceeds 50 KB, upload it to an OBS bucket and enter the OBS URL when you need to select a package template.

  NOTE

  The OBS URL specifies the location of an object stored in an OBS bucket. To obtain an OBS URL on the OBS console, you need to locate the object and choose **More** > **Copy Object URL** in the **Operation** column on the **Objects** page.

Figure 4-3 Selecting a conformance package template



Step 6 On the details page that is displayed, enter a package name, select quick authorization or custom authorization, set the parameters required, and click **Next**.

Figure 4-4 Detailed information

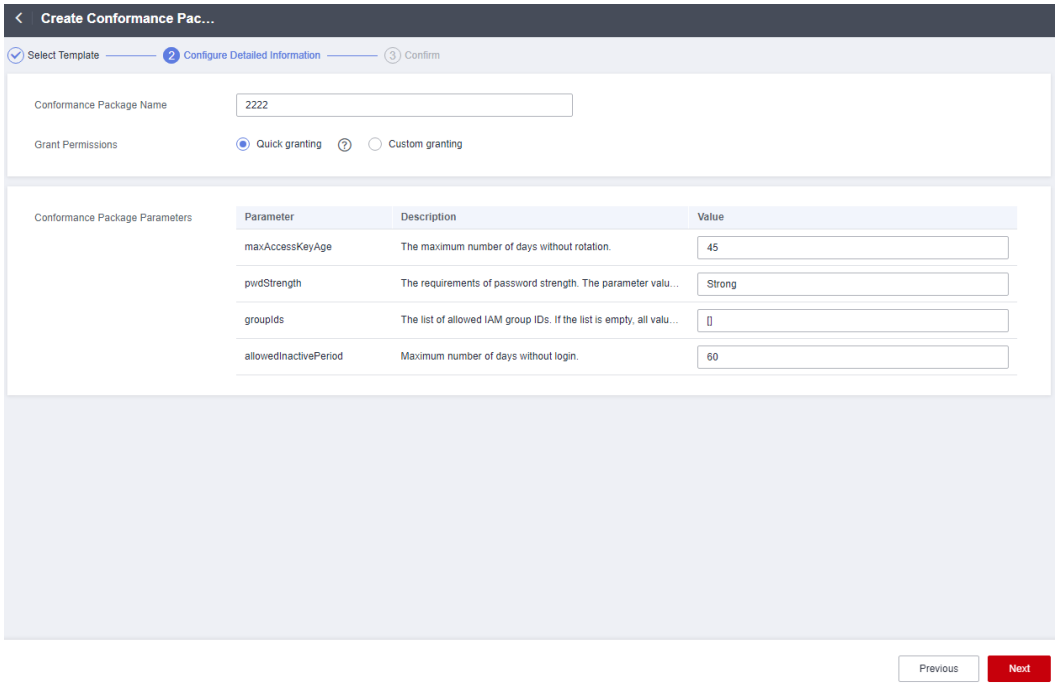
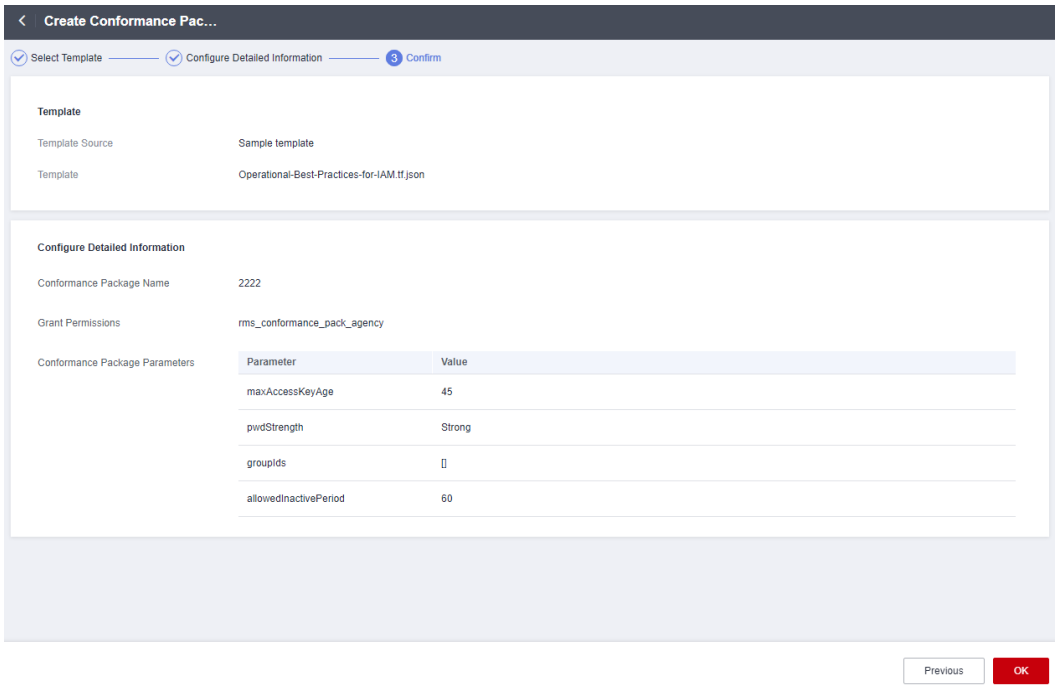


Table 4-1 Package parameters

Parameter	Description
Name	Conformance package name. A conformance package name is customized and must be unique. The name can contain letters, numbers, underscores (_), and hyphens (-) and cannot exceed 64 characters.
Authorization	The authorization is to grant RFS required permissions to create, update, and delete individual rules, and allow the stacks of RFS to create and delete rules in a conformance package. • Quick authorization: This option creates an agency named rms_conformance_pack_agency for you to create, update, or delete rules, and to create or delete a conformance package. • Custom authorization: You can create an agency and perform custom authorization through IAM. The agency must contain required permissions for a compliance package to work properly. This agency must contain the permissions for RFS to create, update, or delete rules. For details about how to create an agency, see **Creating an Agency (by a Delegating Party)**.
Parameters	Parameters of a conformance package are consistent with rules in the package. For details, see **Built-in Policies**.

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

Figure 4-5 Confirming configurations



NOTE

After a conformance package is created, the first evaluation will be automatically triggered immediately.

----End

4.2.2 Viewing Conformance Packages and Compliance Data

Scenarios

You can view all conformance packages created and their details. You can also set search options to filter conformance packages.

Procedure

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

Step 3 On the left navigation pane, choose **Conformance Package**.

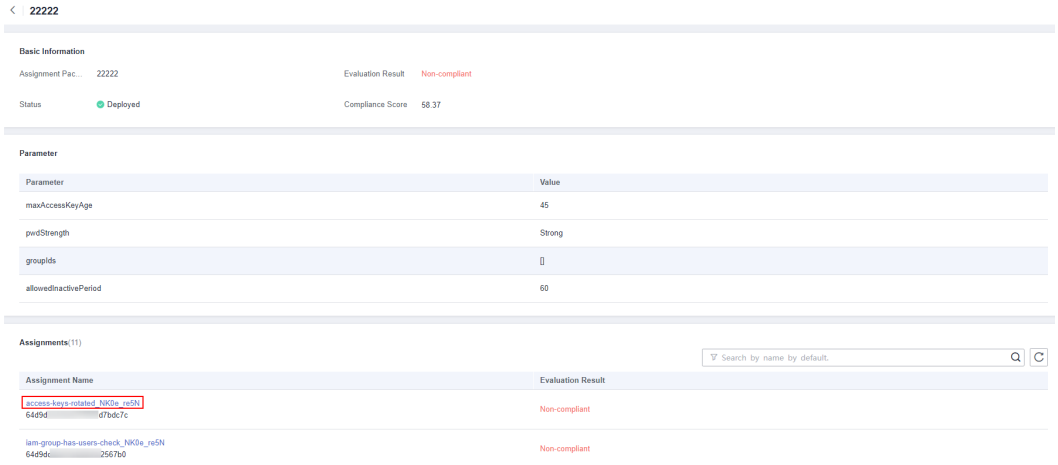
Step 4 View all the conformance packages created and their details, such as evaluation results, compliance scores, and status.

Step 5 Locate a target package and click the package name to go to the details page.

On the details page, view package basic information, parameters, and evaluation result of each rule.

Locate a target rule and click the rule name to go to the details page. Non-compliant resources evaluated against the rule are displayed by default.

Figure 4-6 Conformance package details page



NOTE

A conformance package may be in a status of:

- Deployed: A conformance package has been deployed.
- Deploying: A conformance package is being deployed.
- Abnormal: Conformance package deployment failed.
- Rolled back: Some rules in a conformance package failed to be created and were rolled back, and other created rules were deleted.
- Rolling back: Some rules in a conformance package failed to be created and were rolled back, and other created rules were being deleted.
- Rollback failed: Some rules in a conformance package failed to be created and to be rolled back. You can access RFS to check out the reasons.
- Deleting: Rules in a conformance package and the package are being deleted.
- Exception: Deleting a conformance package failed.

----End

4.2.3 Deleting a Conformance Package

Scenario

If you do not need a conformance package any longer, you can follow the procedure below to delete it.

Procedure

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

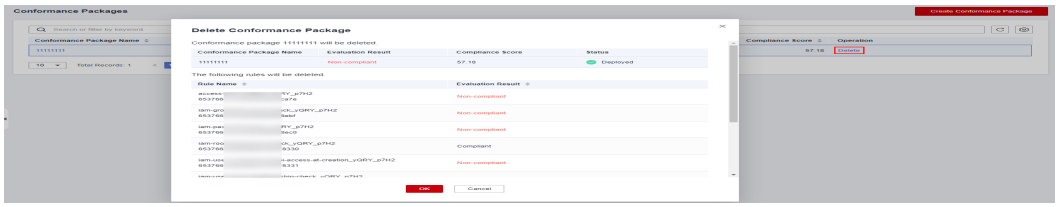
Step 3 On the left navigation pane, choose **Conformance Package**.

Step 4 Locate a target package and click **Delete** in the **Operation** column.

Step 5 In the displayed dialog box, click **OK**.

After a conformance package is deleted, the rules included are also automatically deleted from the list.

Figure 4-7 Deleting conformance packages



----End

4.3 Organization Conformance Packages

4.3.1 Creating an Organization Conformance Package

Scenario

If you are an organization administrator or a delegated administrator of Config, you can add organization conformance packages and deploy these packages to all member accounts in your organization.

Each member can view organization packages that are deployed to their accounts in the conformance package list. If you create an organization conformance package using an account, you can only use the same account to delete the package. Members can only initiate resource evaluation and view evaluation results.

After an organization conformance package is created, your resources are evaluated against the rules in the package by default. Evaluations will continue to be initiated each time the package is triggered. You can also trigger evaluation against a single rule in the rule list page.

Restrictions and Limitations

- You can add up to 20 conformance packages (including organization conformance packages) and 500 rules in an account.
- The resource recorder must be enabled before you create an organization conformance package.
- The **Organization Conformance Package** tab is inaccessible for non-organization members on Config console.
- The Organizations service is in open beta test (OBT). To use organization conformance packages, apply for OBT.

Procedure

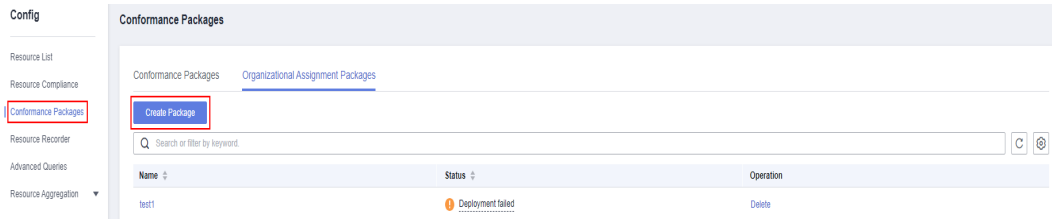
Step 1 Sign in to the Config console as an organization administrator or an agency administrator of Config.

Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

Step 3 On the left navigation pane, choose **Conformance Package**.

Step 4 Select the **Organization Conformance Package** tab and click **Create Organization Conformance Package**.

Figure 4-8 Creating an organization conformance package



Step 5 On the **Select Template** page, select a sample template, upload a local template, or enter an OBS template URL, and click **Next**.

- Sample template: templates provided by Config. You can select a sample template from the dropdown list.

  For details about the rules contained in each sample template, see **conformance package sample template**.

- Local template: templates uploaded locally. You can create a custom template and upload the template.

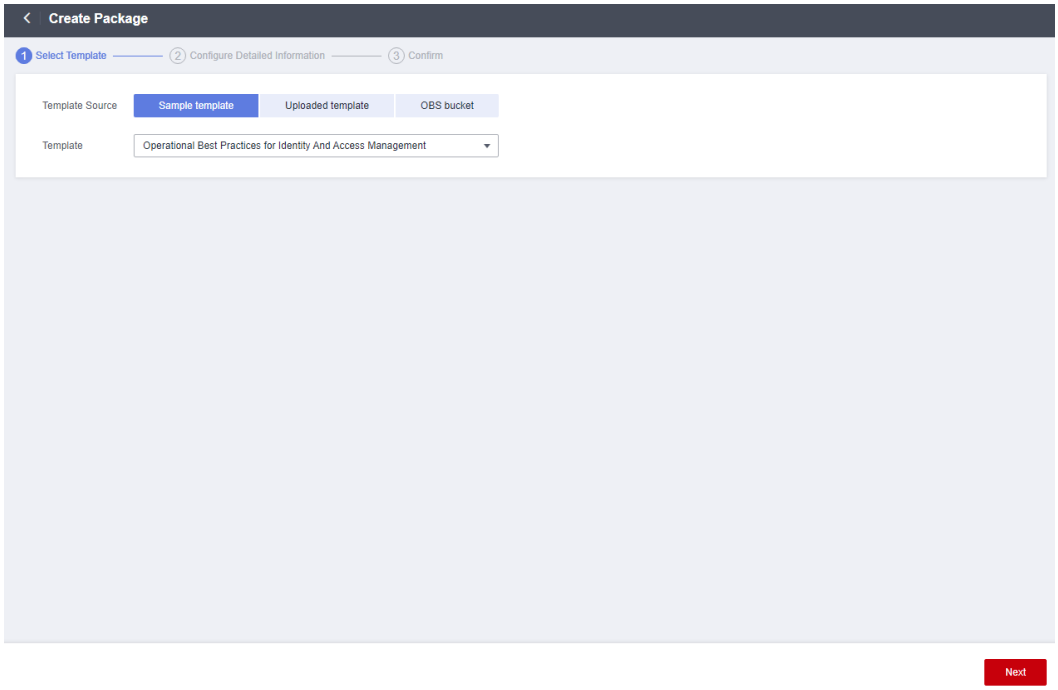
  Both the template file and content formats must be JSON. That is, the file name extension must be .tf.json. For details, see **custom conformance packages**.

- OBS bucket: URLs of the OBS buckets where custom conformance package templates are stored. If your local template file exceeds 50 KB, upload it to an OBS bucket and enter the OBS URL when you need to select a package template.

  NOTE

  The OBS URL specifies the location of an object stored in an OBS bucket. To obtain an OBS URL on the OBS console, you need to locate the object and choose **More** > **Copy Object URL** in the **Operation** column on the **Objects** page.

Figure 4-9 Selecting a conformance package template



Step 6 Configure detailed information and click **Next**.

Figure 4-10 Detailed information

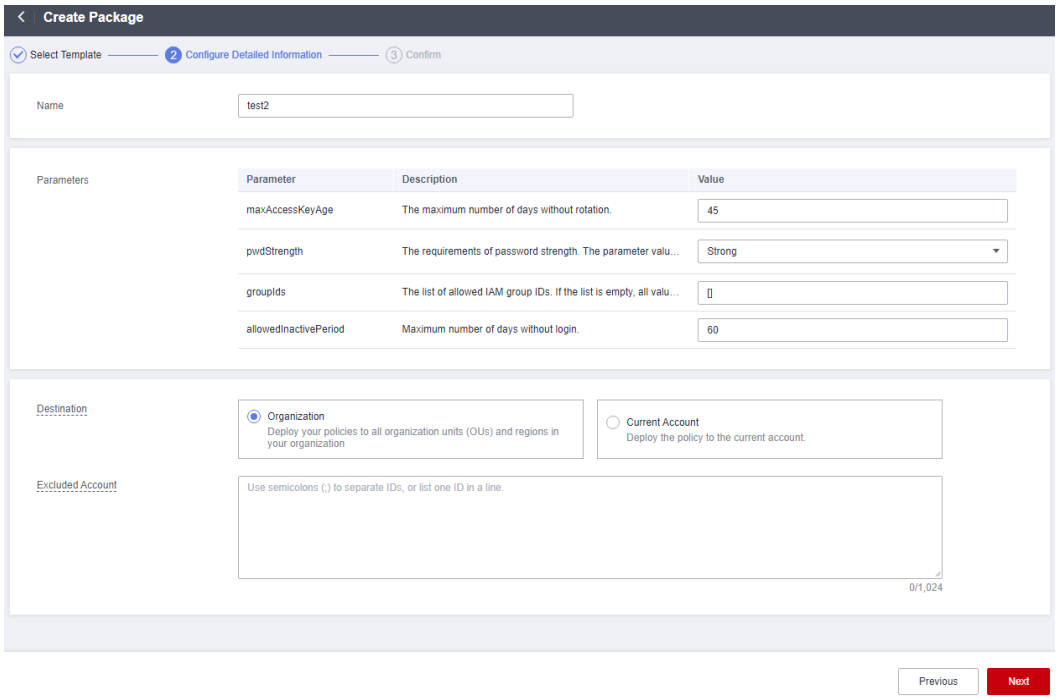
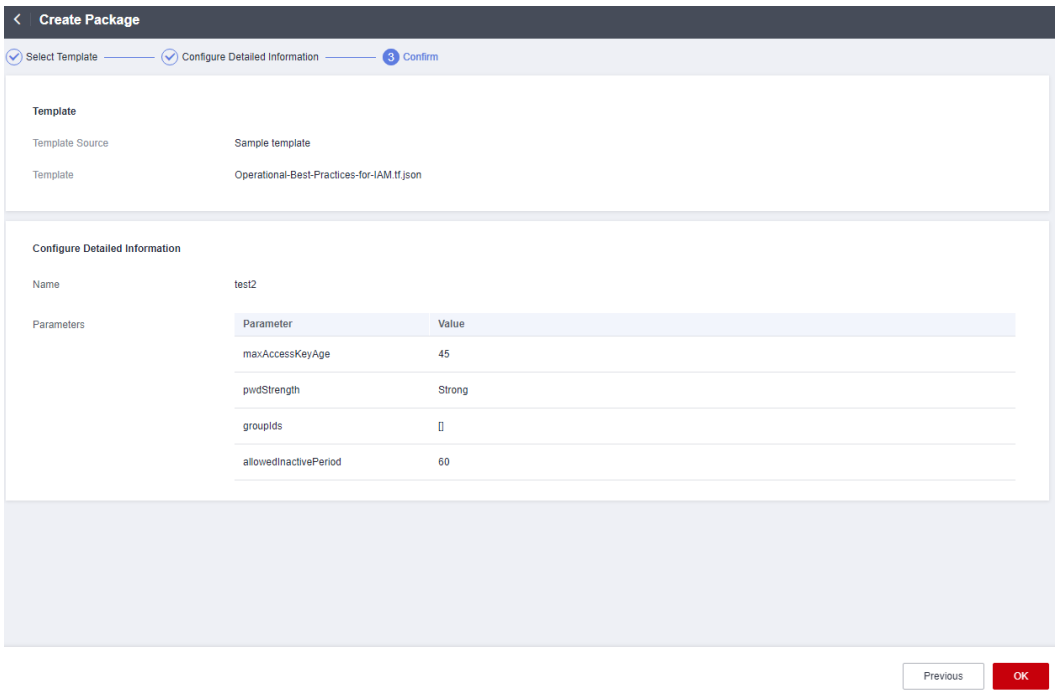


Table 4-2 Detailed information

Parameter	Description
Name	The name of an organization conformance package. An organization conformance package name is customized and must be unique. The name can contain letters, numbers, underscores (_), and hyphens (-) and cannot exceed 64 characters.
Parameters	Parameters of an organization conformance package are consistent with rules in the package. For details, see **Built-in Policies**.
Destination	Specifies where an organization conformance package will be deployed. • **Organization** indicates that a conformance package will be deployed to all members in a specified organization. • **Current Account** indicates that a conformance package will be deployed to the current account. When creating an organization conformance package, select **Organization**.
Excluded Account	Member accounts that an organization conformance package will not be deployed to. This parameter is only required when **Destination** is set to **Organization**.

Step 7 On the confirm information page, confirm configuration and click **OK**.

Figure 4-11 Confirming configurations



NOTE

After an organization conformance package is created, the first evaluation using the package will be automatically triggered immediately.

----End

4.3.2 Viewing Organization Conformance Packages

Scenario

An organization administrator or a delegated administrator of Config can only view organization conformance packages created by themselves.

Each member can view organization packages that are deployed to their accounts in the conformance package list. If you create an organization conformance package using an account, you can only use the same account to delete the package. Members can only initiate resource evaluation and view evaluation results.

This section mainly contains **Viewing Organization Conformance Packages (for Administrators)** and **Viewing Organization Conformance Packages (for Organization Members)**.

Viewing Organization Conformance Packages (for Administrators)

Step 1 Sign in to the management console as an organization administrator or a delegated administrator of Config.

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

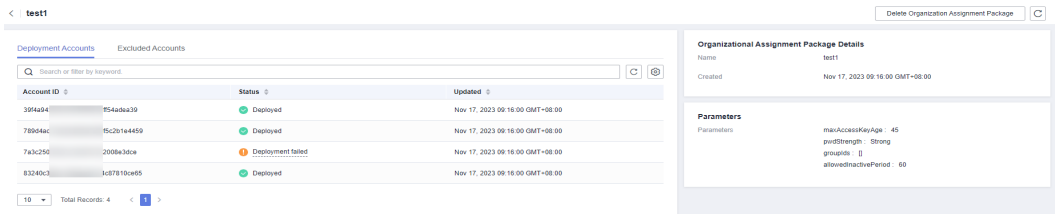
Step 3 On the left navigation pane, choose **Conformance Package**.

Step 4 Select the **Organization Conformance Package** tab to view all created organization conformance packages and their deployment statuses.

Step 5 Click the name of a target organization conformance package to view details.

On the left, view deployed and excluded member accounts. On the right, view package details.

Figure 4-12 Organization conformance package details



NOTE

The deployment status of an organization conformance package may be:

- Deployed: A conformance package has been deployed.
- Deploying: A conformance package is being deployed.
- Abnormal: Conformance package deployment failed.
- Rolled back: Some rules in a conformance package failed to be created and were rolled back, and other created rules were deleted.
- Rolling back: Some rules in a conformance package failed to be created and were rolled back, and other created rules were being deleted.
- Rollback failed: Some rules in a conformance package failed to be created and to be rolled back. You can access RFS to check out the reasons.
- Deleting: Rules in a conformance package and the package are being deleted.
- Exception: Deleting a conformance package failed.

----End

Viewing Organization Conformance Packages (for Organization Members)

Step 1 Sign in to the management console as an organization member.

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

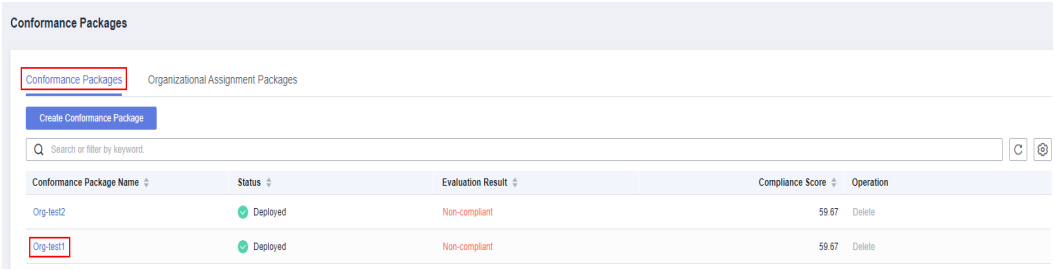
Step 3 On the left navigation pane, choose **Conformance Package**.

Step 4 On the **Conformance Packages** tab, click the name of a target organization conformance package in the list to view details.

On the details page, view package basic information, parameters, and evaluation result of each rule.

Locate a target rule and click the rule name to go to the details page. Non-compliant resources evaluated against the rule are displayed by default.

Figure 4-13 Viewing organization conformance packages (for organization members)



NOTE

Organization conformance packages will be displayed with the **Org** field added before each package name in the package list of each deployed member account.

Members can only trigger rules in an organization conformance package and view the evaluation results. They cannot delete an organization conformance package.

----End

4.3.3 Deleting Organization Conformance Packages

Scenario

If you do not need an organization conformance package any longer, you can follow the procedure below to delete it.

Procedure

Step 1 Sign in to the management console as an organization administrator or a delegated administrator of Config.

Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

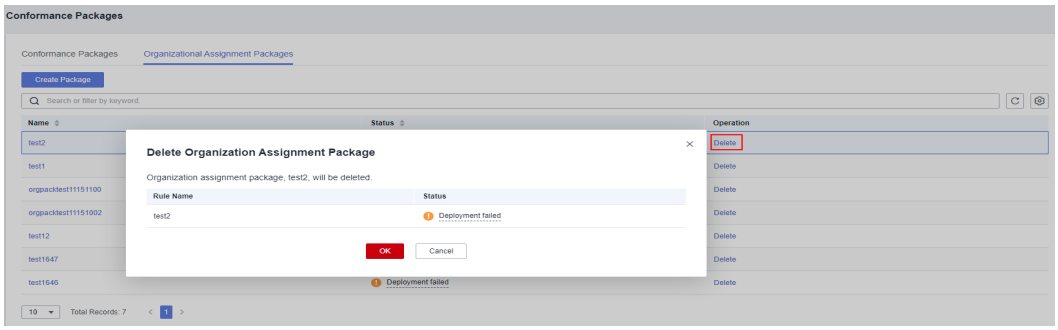
Step 3 On the left navigation pane, choose **Conformance Package**.

Step 4 Select the **Organizational Conformance Package** tab. In the list, locate a target package and click **Delete** in the **Operation** column.

Step 5 In the displayed dialog box, click **OK**.

After an organization conformance package is deleted, the package is also automatically deleted from the package lists of the member accounts.

Figure 4-14 Deleting organization conformance packages



----End

4.4 Custom Conformance Packages

If you need to create a custom conformance package, you can write a package template based on the sample template provided in this section. Then you can upload the template directly or through an OBS bucket when creating a conformance package.

Template Sections

Resource: the most important section of a template. Currently, only the **huaweicloud_rms_policy_assignment** resource (including predefined rules and custom rules) is supported. You need to specify the name or other information about a rule for this section.

variable: Specifies parameters included in a template. By defining defining parameters through the section variable, you can flexibly modify related configurations without altering template source code. If there are no parameters, this section does not need to be declared.

terraform: Specifies service providers. For details see **Provider**. The following example shows a template format:

```
"terraform": {
  "required_providers": {
    "huaweicloud": {
      "source": "huawei.com/provider/huaweicloud",
      "version": "1.46.0"
    }
  }
}
```

The version must be 1.46.0 or later. For details about the supported versions, see **Supported Provider Versions**.

Conformance package sample file: example-conformance-pack.tf.json

```
{
  "resource": {
    "huaweicloud_rms_policy_assignment": {
      "AccessKeysRotated": {
        "name": "access-keys-rotated",
        "description": "An IAM users is noncompliant if the access keys have not been rotated for more than maxAccessKeyAge number of days.",
        "policy_definition_id": "2a2938894ae786dc306a647a",
        "period": "TwentyFour_Hours",
        "parameters": {
          "maxAccessKeyAge": "${jsonencode(var.maxAccessKeyAge)}"
        }
      },
      "IamGroupHasUsersCheck": {
        "name": "iam-group-has-users-check",
        "description": "An IAM groups is noncompliant if it does not add any IAM user.",
        "policy_definition_id": "f7dd9c02266297f6e8c8445e",
        "policy_filter": {
          "resource_provider": "iam",
          "resource_type": "groups"
        },
        "parameters": {}
      },
      "IamPasswordPolicy": {
        "name": "iam-password-policy",
        "description": "An IAM users is noncompliant if password policy for IAM users matches the specified password strength.",
        "policy_definition_id": "2d8d3502539a623ba1907644",
        "policy_filter": {
          "resource_provider": "iam",
          "resource_type": "users"
        },
        "parameters": {
          "pwdStrength": "${jsonencode(var.pwdStrength)}"
        }
      },
      "IamRootAccessKeyCheck": {
        "name": "iam-root-access-key-check",
        "description": "An account is noncompliant if the the root iam user have active access key.",
        "policy_definition_id": "66cac2ddc17b6a25ad077253",
        "period": "TwentyFour_Hours",
        "parameters": {}
      },
      "IamUserConsoleAndApiAccessAtCreation": {
        "name": "iam-user-console-and-api-access-at-creation",
```



```
      "description": "An IAM user with console access is noncompliant if access keys are setup during the
initial user setup.",
      "policy_definition_id": "a5f29eb45cddce8e6baa033d",
      "policy_filter": {
        "resource_provider": "iam",
        "resource_type": "users"
      },
      "parameters": {}
    },
    "IamUserGroupMembershipCheck": {
      "name": "iam-user-group-membership-check",
      "description": "An IAM user is noncompliant if it does not belong to any IAM user group.",
      "policy_definition_id": "846f5708463c1490c4eebd60",
      "policy_filter": {
        "resource_provider": "iam",
        "resource_type": "users"
      },
      "parameters": {
        "groupIds": "${jsonencode(var.groupIds)}"
      }
    },
    "IamUserLastLoginCheck": {
      "name": "iam-user-last-login-check",
      "description": "An IAM user is noncompliant if it has never signed in within the allowed number of
days.",
      "policy_definition_id": "6e4bf7ee7053b683f28d7f57",
      "period": "TwentyFour_Hours",
      "parameters": {
        "allowedInactivePeriod": "${jsonencode(var.allowedInactivePeriod)}"
      }
    },
    "IamUserMfaEnabled": {
      "name": "iam-user-mfa-enabled",
      "description": "An IAM user is noncompliant if it does not have multi-factor authentication (MFA)
enabled.",
      "policy_definition_id": "b92372b5eb51330306cec9c2",
      "policy_filter": {
        "resource_provider": "iam",
        "resource_type": "users"
      },
      "parameters": {}
    },
    "IamUserSingleAccessKey": {
      "name": "iam-user-single-access-key",
      "description": "An IAM user with console access is noncompliant if iam user have multiple active
access keys.",
      "policy_definition_id": "6deae3856c41b240b3c0bf8d",
      "policy_filter": {
        "resource_provider": "iam",
        "resource_type": "users"
      },
      "parameters": {}
    },
    "MfaEnabledForIamConsoleAccess": {
      "name": "mfa-enabled-for-iam-console-access",
      "description": "An IAM user is noncompliant if it uses a console password and does not have multi-
factor authentication (MFA) enabled.",
      "policy_definition_id": "63f8301e47b122062a68b868",
      "policy_filter": {
        "resource_provider": "iam",
        "resource_type": "users"
      },
      "parameters": {}
    },
    "RootAccountMfaEnabled": {
      "name": "root-account-mfa-enabled",
      "description": "An account is noncompliant if the the root iam user does not have multi-factor
authentication (MFA) enabled.",
      "policy_definition_id": "61d787a75cf7f5965da5d647",
```



```
      "period": "TwentyFour_Hours",
      "parameters": {}
    }
   }
  },
  "variable": {
   "maxAccessKeyAge": {
    "description": "The maximum number of days without rotation. ",
    "type": "string",
    "default": "90"
   },
   "pwdStrength": {
    "description": "The requirements of password strength. The parameter value can only be 'Strong',
'Medium', or 'Low'.",
    "type": "string",
    "default": "Strong"
   },
   "groupIds": {
    "description": "The list of allowed IAM    group IDs. If the list is empty, all values are allowed.",
    "type": "list(string)",
    "default": []
   },
   "allowedInactivePeriod": {
    "description": "Maximum number of days without login.",
    "type": "number",
    "default": 90
   }
  },
  "terraform": {
   "required_providers": {
    "huaweicloud": {
     "source": "huawei.com/provider/huaweicloud",
     "version": "1.46.0"
    }
   }
  }
}
```

Conformance package sample file: example-conformance-pack-with-custom-policy.tf.json

```
{
   "resource": {
      "huaweicloud_rms_policy_assignment": {
         "CustomPolicyAssignment": {
            "name": "customPolicy${var.name_suffix}",
"description": Custom rules. All resources are non-compliant.
            "policy_filter": {
               "resource_provider": "obs",
               "resource_type": "buckets"
            },
            "parameters": {},
            "custom_policy": {
               "function_urn": "${var.function_urn}",
               "auth_type": "agency",
               "auth_value": {
                  "agency_name": "\"config_custom_policy_agency\""
               }
            }
         }
      }
   },
   "variable": {
      "name_suffix": {
         "description": "",
         "type": "string"
      },
      "function_urn": {
         "description": "",
```



```
            "type": "string"
        }
    },
    "terraform": {
        "required_providers": {
            "huaweicloud": {
                "source": "huawei.com/provider/huaweicloud",
                "version": "1.46.0"
            }
        }
    }
}
```

4.5 Conformance Package Templates

4.5.1 Overview

Config provides sample templates to help users quickly create a compliance package. Each template contains multiple rules created with predefined policies. For details about predefined policies, see **Predefined Policies**. You can call the **Querying Built-in Assignment Package Templates** API to view all sample conformance package templates.

The following sample templates are provided on Config console:

- **Compliance Package for Classified Protection of Cybersecurity Level 3 (2.0)**
- **Conformance Package for Financial Industry**
- **Conformance Package for Network Security**
- **Conformance Package for Identity and Access Management**
- **Conformance Package for CES**
- **Conformance Package for Compute Services**
- **Conformance Package for ECS**
- **Conformance Package for ELB**
- **Conformance Package for Management and Regulatory Services**
- **Conformance Package for RDS**
- **Conformance Package for AS**
- **Conformance Package for CTS**
- **Conformance Package for AI and Machine Learning**
- **Conformance Package for Autopilot**
- **Conformance Package for for Enabling Public Access**
- **Conformance Package for Logging and Monitoring**
- **Conformance Package for Idle Asset Management**
- **Conformance Package for Architecture Reliability**
- **Conformance Package for China Hong Kong (China) Monetary Authority Requirements**
- **Conformance Package for ENISA Requirements**
- **Compliance Package for SWIFT CSP**

- **Compliance Package for Germany Cloud Computing Compliance Criteria Catalogue**

4.5.2 Compliance Package for Classified Protection of Cybersecurity Level 3 (2.0)

This template contains the following rules:

- cts-tracker-exists
- dcs-redis-in-vpc
- dds-instance-in-vpc
- ecs-instance-in-vpc
- ecs-instance-no-public-ip
- eip-bandwidth-limit
- elb-loadbalancers-no-public-ip
- elb-tls-https-listeners-only
- iam-user-mfa-enabled
- rds-instance-multi-az-support
- rds-instance-no-public-ip
- rds-instances-in-vpc
- volumes-encrypted-check

4.5.3 Conformance Package for Financial Industry

This template contains the following rules:

- access-keys-rotated
- as-group-elb-healthcheck-required
- css-cluster-https-required
- css-cluster-in-vpc
- cts-kms-encrypted-check
- cts-lts-enable
- cts-obs-bucket-track
- cts-support-validate-check
- cts-tracker-exists
- ecs-instance-in-vpc
- ecs-instance-no-public-ip
- eip-unbound-check
- elb-tls-https-listeners-only
- function-graph-concurrency-check
- iam-group-has-users-check
- iam-password-policy
- iam-root-access-key-check
- iam-user-group-membership-check

- iam-user-last-login-check
- iam-user-mfa-enabled
- kms-rotation-enabled
- mfa-enabled-for-iam-console-access
- mrs-cluster-in-vpc
- mrs-cluster-kerberos-enabled
- mrs-cluster-no-public-ip
- private-nat-gateway-authorized-vpc-only
- rds-instance-multi-az-support
- rds-instance-no-public-ip
- root-account-mfa-enabled
- stopped-ecs-date-diff
- volume-unused-check
- volumes-encrypted-check
- vpc-acl-unused-check
- vpc-flow-logs-enabled
- vpc-sg-ports-check
- vpn-connections-active (vpnaas.vpnConnections)
- vpn-connections-active (vpnaas.ipsec-site-connections)
- waf-instance-policy-not-empty

4.5.4 Conformance Package for Network Security

This template contains the following rules:

- access-keys-rotated
- alarm-kms-disable-or-delete-key
- alarm-obs-bucket-policy-change
- alarm-vpc-change
- css-cluster-https-required
- css-cluster-in-vpc
- cts-kms-encrypted-check
- cts-lts-enable
- cts-obs-bucket-track
- cts-support-validate-check
- cts-tracker-exists
- ecs-instance-in-vpc
- ecs-instance-no-public-ip
- eip-unbound-check
- elb-tls-https-listeners-only
- iam-group-has-users-check
- iam-password-policy

- iam-root-access-key-check
- iam-user-console-and-api-access-at-creation
- iam-user-group-membership-check
- iam-user-last-login-check
- iam-user-mfa-enabled
- iam-user-single-access-key
- mfa-enabled-for-iam-console-access
- mrs-cluster-kerberos-enabled
- mrs-cluster-no-public-ip
- private-nat-gateway-authorized-vpc-only
- rds-instance-multi-az-support
- rds-instance-no-public-ip
- root-account-mfa-enabled
- stopped-ecs-date-diff
- volume-unused-check
- volumes-encrypted-check
- vpn-connections-active (vpnaas.vpnConnections)
- vpn-connections-active (vpnaas.ipsec-site-connections)

4.5.5 Conformance Package for Identity and Access Management

This template contains the following rules:

- access-keys-rotated
- iam-group-has-users-check
- iam-password-policy
- iam-root-access-key-check
- iam-user-console-and-api-access-at-creation
- iam-user-group-membership-check
- iam-user-last-login-check
- iam-user-mfa-enabled
- iam-user-single-access-key
- mfa-enabled-for-iam-console-access
- root-account-mfa-enabled

4.5.6 Conformance Package for CES

This template contains the following rules:

- alarm-action-enabled-check
- alarm-kms-disable-or-delete-key
- alarm-obs-bucket-policy-change
- alarm-vpc-change

4.5.7 Conformance Package for Compute Services

This template contains the following rules:

- as-capacity-rebalancing
- as-group-elb-healthcheck-required
- as-multiple-az
- ecs-instance-key-pair-login
- ecs-instance-no-public-ip
- ecs-multiple-public-ip-check
- eip-bandwidth-limit
- function-graph-concurrency-check
- function-graph-public-access-prohibited
- stopped-ecs-date-diff
- volume-unused-check
- volumes-encrypted-check

4.5.8 Conformance Package for ECS

This template contains the following rules:

- ecs-instance-key-pair-login
- ecs-instance-no-public-ip
- ecs-multiple-public-ip-check
- stopped-ecs-date-diff
- volumes-encrypted-check

4.5.9 Conformance Package for ELB

This template contains the following rules:

- elb-tls-https-listeners-only
- elb-predefined-security-policy-https-check
- elb-loadbalancers-no-public-ip

4.5.10 Conformance Package for Management and Regulatory Services

This template contains the following rules:

- alarm-action-enabled-check
- alarm-kms-disable-or-delete-key
- alarm-obs-bucket-policy-change
- alarm-vpc-change
- tracker-config-enabled-check
- cts-kms-encrypted-check

- cts-lts-enable
- cts-support-validate-check
- cts-tracker-exists

4.5.11 Conformance Package for RDS

This template contains the following rules:

- rds-instance-enable-backup
- rds-instance-enable-errorLog
- rds-instance-enable-slowLog
- rds-instance-multi-az-support
- rds-instance-no-public-ip
- rds-instances-enable-kms

4.5.12 Conformance Package for AS

This template contains the following rules:

- as-capacity-rebalancing
- as-group-elb-healthcheck-required
- as-multiple-az

4.5.13 Conformance Package for CTS

This template contains the following rules:

- cts-kms-encrypted-check
- cts-lts-enable
- cts-support-validate-check
- cts-tracker-exists

4.5.14 Conformance Package for AI and Machine Learning

This template contains the following rules:

- cce-cluster-end-of-maintenance-version
- cce-cluster-oldest-supported-version
- cce-endpoint-public-access
- cts-obs-bucket-track
- mrs-cluster-kerberos-enabled
- mrs-cluster-no-public-ip
- sfsturbo-encrypted-check

4.5.15 Conformance Package for Autopilot

This template contains the following rules:

- css-cluster-disk-encryption-check

- css-cluster-no-public-zone
- css-cluster-security-mode-enable
- css-cluster-https-required
- cts-obs-bucket-track
- cts-support-validate-check
- cts-tracker-exists
- cts-kms-encrypted-check
- ecs-instance-no-public-ip
- elb-loadbalancers-no-public-ip
- elb-tls-https-listeners-only
- iam-password-policy
- iam-user-last-login-check
- iam-user-mfa-enabled
- rds-instance-no-public-ip
- root-account-mfa-enabled
- volumes-encrypted-check
- vpc-flow-logs-enabled
- vpc-sg-ports-check
- dcs-redis-no-public-ip
- dcs-redis-password-access

4.5.16 Conformance Package for for Enabling Public Access

This template contains the following rules:

- css-cluster-in-vpc
- drs-data-guard-job-not-public
- drs-migration-job-not-public
- drs-synchronization-job-not-public
- ecs-instance-in-vpc
- ecs-instance-no-public-ip
- function-graph-inside-vpc
- function-graph-public-access-prohibited
- mrs-cluster-no-public-ip
- rds-instance-no-public-ip

4.5.17 Conformance Package for Logging and Monitoring

This template contains the following rules:

- alarm-action-enabled-check
- apig-instances-execution-logging-enabled
- as-group-elb-healthcheck-required
- cts-kms-encrypted-check

- cts-lts-enable
- cts-obs-bucket-track
- cts-support-validate-check
- cts-tracker-exists
- dws-enable-log-dump
- function-graph-concurrency-check
- multi-region-cts-tracker-exists
- rds-instance-logging-enabled
- vpc-flow-logs-enabled

4.5.18 Conformance Package for Idle Asset Management

This template contains the following rules:

- stopped-ecs-date-diff
- eip-use-in-specified-days
- evs-use-in-specified-days
- eip-unbound-check
- iam-group-has-users-check
- iam-user-last-login-check
- volume-unused-check
- vpc-acl-unused-check
- cce-cluster-end-of-maintenance-version

4.5.19 Conformance Package for Architecture Reliability

This template contains the following rules:

- apig-instances-execution-logging-enabled
- as-group-elb-healthcheck-required
- cts-lts-enable
- cts-obs-bucket-track
- cts-tracker-exists
- dws-enable-kms
- ecs-instance-in-vpc
- function-graph-concurrency-check
- gaussdb-nosql-enable-disk-encryption
- kms-not-scheduled-for-deletion
- multi-region-cts-tracker-exists
- rds-instance-enable-backup
- rds-instance-multi-az-support
- rds-instances-enable-kms
- sfsturbo-encrypted-check
- volumes-encrypted-check

- vpc-flow-logs-enabled
- vpn-connections-active-for-ipsec-site-connections
- vpn-connections-active-for-vpnConnections

4.5.20 Conformance Package for China Hong Kong (China) Monetary Authority Requirements

This section describes the background, applicable scenarios, and the compliance package to meet requirements by the Hong Kong (China) Monetary Authority.

Background

Hong Kong (China) Monetary Authority provided guidelines and regulations on cloud computing based on the results of a thematic reviews conducted between 2021 and 2022. Before adopting cloud computing, you need to pay attention to the key principles proposed by the Hong Kong (China) Monetary Authority.

For more details, see **HKMA.2022.08.31**, **SA-2**, **OR-2**, and **TM-G-1**.

Applicable Scenarios

The conformance package in this section is intended to help financial enterprises in Hong Kong (China) migrate to the cloud.

Exemption Clauses

This package provides you with general guide to help you quickly create scenario-based conformance packages. The conformance package and rules included only apply to cloud service and do not represent any legal advice. This conformance package does not ensure compliance with specific laws, regulations, or industry standards. You are responsible for the compliance and legality of your business and technical operations and assume all related responsibilities.

Conformance Rules

The guideline No. in the following table are in consistent with the chapter No. in **HKMA.2022.08.31**.

Table 4-3 Guidance on Cloud Computing (HKMA)

Guideline No.	Guideline Description	Rule	Solution
I-2	Depending on the cloud deployment model adopted, these may include multi-tenancy risks, as well as those concerning concentration risk and supply chain risks more generally.	iam-group-has-users-check	Assign different permissions to IAM users or user groups to implement least privilege and separation of duty (SOD) principles.
I-2	Depending on the cloud deployment model adopted, these may include multi-tenancy risks, as well as those concerning concentration risk and supply chain risks more generally.	iam-user-group-membership-check	Assign different permissions to IAM users or user groups to perform access control.
I-2	Depending on the cloud deployment model adopted, these may include multi-tenancy risks, as well as those concerning concentration risk and supply chain risks more generally.	iam-root-access-key-check	Delete root access keys to prevent unintended authorization.
II-5	AIs should implement layers of security control measures to protect the integrity and confidentiality of customer information stored in the cloud.	kms-rotation-enabled	Enable key rotation.

Guideline No.	Guideline Description	Rule	Solution
II-5	AIs should implement layers of security control measures to protect the integrity and confidentiality of customer information stored in the cloud.	iam-password-policy	Set thresholds for password strength.
II-5	AIs should implement layers of security control measures to protect the integrity and confidentiality of customer information stored in the cloud.	cts-support-validate-check	Use CTS trackers to verify whether logs are modified, deleted, or unchanged after being dumped.
II-5	AIs should implement layers of security control measures to protect the integrity and confidentiality of customer information stored in the cloud.	rds-instances-enable-kms	Enable encryption for RDS instances.
II-5	AIs should implement layers of security control measures to protect the integrity and confidentiality of customer information stored in the cloud.	dcs-redis-enable-ssl	Enable SSL for Redis to protect sensitive data.

The guideline No. in the following table are in consistent with the chapter No. in **SA-2**.

Table 4-4 SA-2 on "Outsourcing"

Guideline No.	Guideline Description	Rule	Solution
2.5.1	AIs should ensure that the proposed outsourcing arrangement complies with relevant statutory requirements and common law customer confidentiality.	cts-kms-encrypted-check	Enable file encryption for CTS trackers.
2.5.1	AIs should ensure that the proposed outsourcing arrangement complies with relevant statutory requirements and common law customer confidentiality.	rds-instances-enable-kms	Enable encryption for cloud databases
2.5.1	AIs should ensure that the proposed outsourcing arrangement complies with relevant statutory requirements and common law customer confidentiality.	css-cluster-disk-encryption-check	Enable disk encryption for Cloud Search Service (CSS) clusters.
2.8.1	AIs should ensure that the proposed outsourcing arrangement complies with relevant statutory requirements and common law customer confidentiality.	vpc-flow-logs-enabled	Use VPC flow logs to obtain VPC traffic information.

Guideline No.	Guideline Description	Rule	Solution
2.8.1	AIs should ensure that appropriate up-to-date records are maintained in their premises and kept available for inspection by the HKMA.	apig-instances-execution-logging-enabled	User API gateway logs to visualize users accessing APIs and obtain their access methods and activities.
2.8.1	AIs should ensure that appropriate up-to-date records are maintained in their premises and kept available for inspection by the HKMA.	cts-lts-enable	Use CTS to centrally collect and manage log events
2.8.1	AIs should ensure that appropriate up-to-date records are maintained in their premises and kept available for inspection by the HKMA.	cts-support-validate-check	Use CTS trackers to verify whether logs are modified, deleted, or unchanged after being dumped.

The guideline numbers in the following table are in consistent with the chapter numbers in **OR-2**.

Table 4-5 OR-2 on "Operational Resilience"

Guideline No.	Guideline Description	Rule	Solution
4.2.2	AIs should be aware that their operational capabilities may vary during different business cycles or as a result of seasonal factors. For instance, during the periods of time when more initial public offerings are launched.	as-group-elb-healthcheck-required	User elastic load balancers to monitor cloud server (in AS groups) status by periodically sending requests.
6.1	AIs should be prepared to manage all risks with potential to affect critical operations delivery.	as-multiple-az	Deploy AS groups across AZs to ensure high capacity and availability.
6.1	AIs should be prepared to manage all risks with potential to affect critical operations delivery.	css-cluster-multiple-az-check	Use CSS across AZs to ensure high capacity and availability.
6.1	AIs should be prepared to manage all risks with potential to affect critical operations delivery.	elb-multiple-az-check	Deploy elastic load balancers across AZs to ensure high capacity and availability.
6.1	AIs should be prepared to manage all risks with potential to affect critical operations delivery.	rds-instance-multi-az-support	Deploy cloud databases across AZs to ensure high capacity and availability.

Guideline No.	Guideline Description	Rule	Solution
6.2	As operational risk management focuses on preventing and minimizing operational losses, it contributes to an AI's efforts to maintain operational resilience.	kms-not-scheduled-for-deletion	Check KMS key status to prevent accidental or malicious deletion.

The guideline numbers in the following table are in consistent with the chapter numbers in **TM-G-1**.

Table 4-6 TM-G-1 on "General Principles for Technology Risk Management"

Guideline No.	Guideline Description	Rule	Solution
3.1.4	AIs should adopt industry-accepted cryptographic solutions and implement sound key management practices to safeguard the associated cryptographic keys.	kms-not-scheduled-for-deletion	Check key status to prevent accidental deletion.
3.1.4	AIs should adopt industry-accepted cryptographic solutions and implement sound key management practices to safeguard the associated cryptographic keys.	kms-rotation-enabled	Enable key rotation.

Guideline No.	Guideline Description	Rule	Solution
3.2.2	AIs should implement effective password rules to ensure that easy-to-guess passwords are avoided and passwords are changed on a periodic basis.	iam-password-policy	Set thresholds for password strength.
3.2.2	AIs should implement effective password rules to ensure that easy-to-guess passwords are avoided and passwords are changed on a periodic basis.	access-keys-rotated	Periodically change access keys.
3.2.2	AIs should implement effective password rules to ensure that easy-to-guess passwords are avoided and passwords are changed on a periodic basis.	iam-user-mfa-enabled	Enable multi-factor authentication (MFA) for all users.
3.2.2	AIs should implement effective password rules to ensure that easy-to-guess passwords are avoided and passwords are changed on a periodic basis.	root-account-mfa-enabled	Enable multi-factor authentication (MFA) for root users.
3.3.1	Monitor the use of system resources to detect any unusual or unauthorized activities.	cts-tracker-exists	Use CTS to record operations on the Huawei Cloud management console and API calls.

Guideline No.	Guideline Description	Rule	Solution
3.3.1	Monitor the use of system resources to detect any unusual or unauthorized activities.	cts-lts-enable	Use CTS to centrally collect and manage log events.
3.3.2	Proper segregation of duties within the security administration function or other compensating controls should be in place to mitigate the risk of unauthorized activities.	iam-role-has-all-permissions	Only grant IAM users necessary permissions to perform required operations to ensure compliance with the least privilege and SOD principles.
5.2.1	AIs should implement a process to ensure that the performance of application systems is continuously monitored and exceptions are reported in a timely and comprehensive manner.	alarm-action-enabled-check	Ensure that CES alarm rules are not disabled.
6.2.1	AIs should implement a process to ensure that the performance of application systems is continuously monitored and exceptions are reported in a timely and comprehensive manner.	ecs-instance-no-public-ip	The ECSs may contain sensitive information. Restrict access to ECSs from public networks.

Guideline No.	Guideline Description	Rule	Solution
6.2.1	To prevent insecure connections to an AI's network, procedures concerning the use of networks and network services need to be established and enforced.	function-graph-public-access-prohibited	Restrict access to FunctionGraph functions from public networks. Public network access may cause data leakage or lower availability.

4.5.21 Conformance Package for ENISA Requirements

This section describes the background, applicable scenarios, and the compliance package to meet requirements by European Union Agency for Cybersecurity (ENISA).

Background

ENISA has issued a guide for small- and medium-sized enterprises (SMEs)to enhance cyber security. The guide highlights the importance of cyber security for SMEs and describes how to implement related best practices to protect their services from cyber threats. For more information about this guide, see **cybersecurity-guide-for-smes**.

Applicable Scenarios

This conformance package helps SMEs to meet ENISA requirements of cyber security. It needs to be reviewed and implemented based on specific conditions and

Exemption Clauses

This package provides you with general guide to help you quickly create scenario-based conformance packages. The conformance package and rules included only apply to cloud service and do not represent any legal advice. This conformance package does not ensure compliance with specific laws, regulations, or industry standards. You are responsible for the compliance and legality of your business and technical operations and assume all related responsibilities.

Compliance Rules

The guideline No. in the following table are in consistent with the chapter No. in **cybersecurity-guide-for-smes**.

Table 4-7 Rules in the conformance package

Guideline No.	Guideline Description	Rule	Solution
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate security controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place.	drs-data-guard-job-not-public	Ensure that DRS real-time DR tasks are not publicly accessible.
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate security controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place.	drs-migration-job-not-public	Ensure that DRS real-time migration tasks are not publicly accessible.

Guideline No.	Guideline Description	Rule	Solution
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate security controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place.	drs-synchronization-job-not-public	Ensure that DRS real-time synchronization tasks are not publicly accessible.
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate security controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place.	ecs-instance-no-public-ip	Restrict public access to ECSs to protect sensitive data.

Guideline No.	Guideline Description	Rule	Solution
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate security controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place.	mrs-cluster-no-public-ip	Block access to MapReduce Service (MRS) using public networks. MRS instances may contain sensitive information, and access control is required.
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate security controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place.	function-graph-public-access-prohibited	Block public access to FunctionGraph functions and manage access to Huawei Cloud resources. Public access may reduce resource availability.

Guideline No.	Guideline Description	Rule	Solution
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate security controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place.	rds-instance-no-public-ip	Block access to cloud databases from public networks and manage access to Huawei Cloud resources. Cloud databases may contain sensitive information, and access control is required.
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate security controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place.	apig-instances-ssl-enabled	Enable SSL for APIG REST APIs to authenticate API requests.

Guideline No.	Guideline Description	Rule	Solution
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate security controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place.	cts-kms-encrypted-check	Enable trace file encryption for CTS trackers.
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate security controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place.	sfsturbo-encrypted-check	Enable KMS encryption for SFS Turbo file systems.

Guideline No.	Guideline Description	Rule	Solution
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate security controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place.	volumes-encrypted-check	Enable encryption for EVS to protect data.
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate security controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place.	cts-support-validate-check	Enable file verification for CTS trackers to prevent log files from being modified or deleted after being stored.

Guideline No.	Guideline Description	Rule	Solution
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate security controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place.	css-cluster-disk-encryption-check	Enable disk encryption for CSS clusters to protect sensitive data.
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate security controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place.	css-cluster-disk-encryption-check	Enable disk encryption for CSS clusters to protect sensitive data.

Guideline No.	Guideline Description	Rule	Solution
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate security controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place.	elb-tls-https-listeners-only	Ensure that your load balancer listeners are configured with the HTTPS protocol.
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate security controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place.	volumes-encrypted-check	Enable encryption for EVS to protect data.

Guideline No.	Guideline Description	Rule	Solution
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate security controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place.	iam-policy-no-statements-with-admin-access	Grant IAM users only necessary permissions to perform required operations to ensure compliance with the least privilege and SOD principles
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate security controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place.	iam-role-has-all-permissions	Grant IAM users only necessary permissions to perform required operations to ensure compliance with the least privilege and SOD principles

Guideline No.	Guideline Description	Rule	Solution
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate security controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place.	vpc-sg-restricted-ssh	Configure security groups to only allow connections to SSH port 22 of ECSs with specified IPs, so remote access to ECS can be secure.
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate security controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place.	private-nat-gateway-authorized-vpc-only	Use private NAT gateways to control VPC connections.

Guideline No.	Guideline Description	Rule	Solution
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate security controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place.	rds-instances-enable-kms	Enable encryption for RDS instances to protect sensitive data.
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate security controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place.	dws-enable-ssl	Enable SSL for DWS clusters to protect sensitive data.

Guideline No.	Guideline Description	Rule	Solution
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate security controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place.	dws-enable-kms	Enable KMS disk encryption for DWS clusters.
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate security controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place.	gaussdb-nosql-enable-disk-encryption	Enable KMS disk encryption for GaussDB NoSQL instances.

Guideline No.	Guideline Description	Rule	Solution
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate security controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place.	vpc-sg-ports-check	Use security groups to control prot connections for VPCs.
5_SECURE ACCESS TO SYSTEMS	Encourage everyone to use a passphrase, a collection of at least three random common words combined into a phrase that provide a very good combination of memorability and security.	iam-password-policy	Set thresholds for IAM user password strength.
5_SECURE ACCESS TO SYSTEMS	Encourage everyone to use a passphrase, a collection of at least three random common words combined into a phrase that provide a very good combination of memorability and security.	iam-user-mfa-enabled	Enable MFA for all IAM users to prevent account theft.

Guideline No.	Guideline Description	Rule	Solution
5_SECURE ACCESS TO SYSTEMS	Encourage everyone to use a passphrase, a collection of at least three random common words combined into a phrase that provide a very good combination of memorability and security.	mfa-enabled-for-iam-console-access	Enable MFA for all IAM users who can access Huawei Cloud management console. MFA enhances account security to prevent account theft and protect sensitive data.
5_SECURE ACCESS TO SYSTEMS	Encourage everyone to use a passphrase, a collection of at least three random common words combined into a phrase that provide a very good combination of memorability and security.	root-account-mfa-enabled	Enable MFA for root users. MFA enhances account security.
6_SECURE DEVICES: KEEP SOFTWARE PATCHED AND UP TO DATE	Ideally using a centralized platform to manage patching. .It is highly recommended for SMEs to: Regularly update all of their software; turn on automatic updates whenever possible; identify software and hardware that requires manual updates; take into account mobile and IoT devices.	cce-cluster-end-of-maintenance-version	Ensure that CCE cluster versions can be maintained.

Guideline No.	Guideline Description	Rule	Solution
6_SECURE DEVICES: KEEP SOFTWARE PATCHED AND UP TO DATE	Ideally using a centralized platform to manage patching. It is highly recommended for SMEs to: Regularly update all of their software; turn on automatic updates whenever possible; identify software and hardware that requires manual updates; take into account mobile and IoT devices.	cce-cluster-oldest-supported-version	Ensure that there are no CCE cluster versions that cannot be maintained. For CCE clusters of supported versions, The system automatically deploys security patches to upgrade your CCE clusters. If any security issue is identified, Huawei Cloud will fix the issue.

Guideline No.	Guideline Description	Rule	Solution
6_SECURE DEVICES: ENCRYPTION	Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferred over public networks, such as hotel or airport WiFi networks, ensure that data is encrypted, either by employing a Virtual Private Network (VPN) or accessing websites over secure connections using SSL/TLS protocol. Ensure their own websites are employing suitable encryption technology to protect client data as it travels over the Internet.	cts-kms-encrypted-check	Enable trace file encryption for CTS trackers.

Guideline No.	Guideline Description	Rule	Solution
6_SECURE DEVICES: ENCRYPTION	Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferred over public networks, such as hotel or airport WiFi networks, ensure that data is encrypted, either by employing a Virtual Private Network (VPN) or accessing websites over secure connections using SSL/TLS protocol. Ensure their own websites are employing suitable encryption technology to protect client data as it travels over the Internet.	cts-support-validate-check	Enable file verification for CTS trackers to prevent log files from being modified or deleted after being stored.

Guideline No.	Guideline Description	Rule	Solution
6_SECURE DEVICES: ENCRYPTION	Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferred over public networks, such as hotel or airport WiFi networks, ensure that data is encrypted, either by employing a Virtual Private Network (VPN) or accessing websites over secure connections using SSL/TLS protocol. Ensure their own websites are employing suitable encryption technology to protect client data as it travels over the Internet.	sfsturbo-encrypted-check	Enable KMS encryption for SFS Turbo file systems.

Guideline No.	Guideline Description	Rule	Solution
6_SECURE DEVICES: ENCRYPTION	Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferred over public networks, such as hotel or airport WiFi networks, ensure that data is encrypted, either by employing a Virtual Private Network (VPN) or accessing websites over secure connections using SSL/TLS protocol. Ensure their own websites are employing suitable encryption technology to protect client data as it travels over the Internet.	css-cluster-disk-encryption-check	Enable disk encryption for CSS clusters to protect sensitive data.

Guideline No.	Guideline Description	Rule	Solution
6_SECURE DEVICES: ENCRYPTION	Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferred over public networks, such as hotel or airport WiFi networks, ensure that data is encrypted, either by employing a Virtual Private Network (VPN) or accessing websites over secure connections using SSL/TLS protocol. Ensure their own websites are employing suitable encryption technology to protect client data as it travels over the Internet.	css-cluster-disk-encryption-check	Enable disk encryption for CSS clusters to protect sensitive data.

Guideline No.	Guideline Description	Rule	Solution
6_SECURE DEVICES: ENCRYPTION	Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferred over public networks, such as hotel or airport WiFi networks, ensure that data is encrypted, either by employing a Virtual Private Network (VPN) or accessing websites over secure connections using SSL/TLS protocol. Ensure their own websites are employing suitable encryption technology to protect client data as it travels over the Internet.	css-cluster-https-required	Enable HTTPS for CSS clusters to ensure data security and allow access over public networks.

Guideline No.	Guideline Description	Rule	Solution
6_SECURE DEVICES: ENCRYPTION	Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferred over public networks, such as hotel or airport WiFi networks, ensure that data is encrypted, either by employing a Virtual Private Network (VPN) or accessing websites over secure connections using SSL/TLS protocol. Ensure their own websites are employing suitable encryption technology to protect client data as it travels over the Internet.	volumes-encrypted-check	Enable encryption for EVS to protect data.

Guideline No.	Guideline Description	Rule	Solution
6_SECURE DEVICES: ENCRYPTION	Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferred over public networks, such as hotel or airport WiFi networks, ensure that data is encrypted, either by employing a Virtual Private Network (VPN) or accessing websites over secure connections using SSL/TLS protocol. Ensure their own websites are employing suitable encryption technology to protect client data as it travels over the Internet.	rds-instances-enable-kms	Enable KMS encryption for RDS instances to protect sensitive data.

Guideline No.	Guideline Description	Rule	Solution
6_SECURE DEVICES: ENCRYPTION	Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferred over public networks, such as hotel or airport WiFi networks, ensure that data is encrypted, either by employing a Virtual Private Network (VPN) or accessing websites over secure connections using SSL/TLS protocol. Ensure their own websites are employing suitable encryption technology to protect client data as it travels over the Internet.	dws-enable-kms	Enable KMS encryption for DWS clusters.

Guideline No.	Guideline Description	Rule	Solution
6_SECURE DEVICES: ENCRYPTION	Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferred over public networks, such as hotel or airport WiFi networks, ensure that data is encrypted, either by employing a Virtual Private Network (VPN) or accessing websites over secure connections using SSL/TLS protocol. Ensure their own websites are employing suitable encryption technology to protect client data as it travels over the Internet.	gaussdb-nosql-enable-disk-encryption	Enable KMS disk encryption for GaussDB NoSQL instances.

Guideline No.	Guideline Description	Rule	Solution
6_SECURE DEVICES: ENCRYPTION	Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferred over public networks, such as hotel or airport WiFi networks, ensure that data is encrypted, either by employing a Virtual Private Network (VPN) or accessing websites over secure connections using SSL/TLS protocol. Ensure their own websites are employing suitable encryption technology to protect client data as it travels over the Internet.	elb-tls-https-listeners-only	Ensure that your load balancer listeners are configured with the HTTPS protocol.

Guideline No.	Guideline Description	Rule	Solution
6_SECURE DEVICES: ENCRYPTION	Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferred over public networks, such as hotel or airport WiFi networks, ensure that data is encrypted, either by employing a Virtual Private Network (VPN) or accessing websites over secure connections using SSL/TLS protocol. Ensure their own websites are employing suitable encryption technology to protect client data as it travels over the Internet.	apig-instances-ssl-enabled	Enable SSL for APIG REST APIs to authenticate API requests.

Guideline No.	Guideline Description	Rule	Solution
6_SECURE DEVICES: ENCRYPTION	Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferred over public networks, such as hotel or airport WiFi networks, ensure that data is encrypted, either by employing a Virtual Private Network (VPN) or accessing websites over secure connections using SSL/TLS protocol. Ensure their own websites are employing suitable encryption technology to protect client data as it travels over the Internet.	dws-enable-ssl	Enable SSL for DWS clusters to protect data.
7_SECURE YOUR NETWORK: EMPLOY FIREWALLS	Firewalls should be deployed to protect all critical systems, in particular a firewall should be employed to protect the SME's network from the Internet.	vpc-sg-restricted-ssh	Configure security groups to only allow connections to SSH port 22 of ECSs with specified IPs, so remote access to ECS can be secure.

Guideline No.	Guideline Description	Rule	Solution
7_SECURE YOUR NETWORK: EMPLOY FIREWALLS	Firewalls manage the traffic that enters and leaves a network and are a critical tool in protecting SMEs systems. Firewalls should be deployed to protect all critical systems, in particular a firewall should be employed to protect the SME's network from the Internet.	vpc-sg-restricted-common-ports	Configure security groups to control connections to common ports in a VPC.
7_SECURE YOUR NETWORK: EMPLOY FIREWALLS	Firewalls manage the traffic that enters and leaves a network and are a critical tool in protecting SMEs systems. Firewalls should be deployed to protect all critical systems, in particular a firewall should be employed to protect the SME's network from the Internet.	vpc-default-sg-closed	Use security groups to control access within a VPC. You can directly use the default security group for resource access control.

Guideline No.	Guideline Description	Rule	Solution
7_SECURE YOUR NETWORK: EMPLOY FIREWALLS	Firewalls manage the traffic that enters and leaves a network and are a critical tool in protecting SMEs systems. Firewalls should be deployed to protect all critical systems, in particular a firewall should be employed to protect the SME's network from the Internet.	vpc-sg-ports-check	Use security groups to control prot connections for VPCs.

Guideline No.	Guideline Description	Rule	Solution
7_SECURE YOUR NETWORK: REVIEW REMOTE ACCESS SOLUTIONS	SMEs should regularly review any remote access tools to ensure they are secure, particularly: 1. Ensure all remote access software is patched and up date. 2. Restrict remote access from suspicious geographical locations or certain IP addresses. 3. Restrict staff remote access only to the systems and computers they need for their work. 4. Enforce strong passwords for remote access and where possible enable multi-factor authentication. 5. Ensure monitoring and alerting is enabled to warn of suspected attacks or unusual suspicious activity.	iam-password-policy	Set thresholds for IAM user password strength.

Guideline No.	Guideline Description	Rule	Solution
7_SECURE YOUR NETWORK: REVIEW REMOTE ACCESS SOLUTIONS	SMEs should regularly review any remote access tools to ensure they are secure, particularly: - Ensure all remote access software is patched and up date. 2. Restrict remote access from suspicious geographical locations or certain IP addresses. 3. Restrict staff remote access only to the systems and computers they need for their work. 4. Enforce strong passwords for remote access and where possible enable multi-factor authentication. 5. Ensure monitoring and alerting is enabled to warn of suspected attacks or unusual suspicious activity.	iam-user-mfa-enabled	Enable MFA for all IAM users to prevent account theft.

Guideline No.	Guideline Description	Rule	Solution
7_SECURE YOUR NETWORK: REVIEW REMOTE ACCESS SOLUTIONS	SMEs should regularly review any remote access tools to ensure they are secure, particularly: - Ensure all remote access software is patched and up date. 2. Restrict remote access from suspicious geographical locations or certain IP addresses. 3. Restrict staff remote access only to the systems and computers they need for their work. 4. Enforce strong passwords for remote access and where possible enable multi-factor authentication. 5. Ensure monitoring and alerting is enabled to warn of suspected attacks or unusual suspicious activity.	mfa-enabled-for-iam-console-access	Enable MFA for all IAM users who can access Huawei Cloud management console. MFA enhances account security to prevent account theft and protect sensitive data.

Guideline No.	Guideline Description	Rule	Solution
7_SECURE YOUR NETWORK: REVIEW REMOTE ACCESS SOLUTIONS	SMEs should regularly review any remote access tools to ensure they are secure, particularly: - Ensure all remote access software is patched and up date. 2. Restrict remote access from suspicious geographical locations or certain IP addresses. 3. Restrict staff remote access only to the systems and computers they need for their work. 4. Enforce strong passwords for remote access and where possible enable multi-factor authentication. 5. Ensure monitoring and alerting is enabled to warn of suspected attacks or unusual suspicious activity.	root-account-mfa-enabled	Enable MFA for root users. MFA enhances account security.

Guideline No.	Guideline Description	Rule	Solution
7_SECURE YOUR NETWORK: REVIEW REMOTE ACCESS SOLUTIONS	SMEs should regularly review any remote access tools to ensure they are secure, particularly: - Ensure all remote access software is patched and up date. 2. Restrict remote access from suspicious geographical locations or certain IP addresses. 3. Restrict staff remote access only to the systems and computers they need for their work. 4. Enforce strong passwords for remote access and where possible enable multi-factor authentication. 5. Ensure monitoring and alerting is enabled to warn of suspected attacks or unusual suspicious activity.	apig-instances-execution-logging-enabled	Enable CTS for your dedicated API gateways. APIG supports custom log analysis templates, which you can use to collect and manage logs and trace and analyze API request exceptions.

Guideline No.	Guideline Description	Rule	Solution
7_SECURE YOUR NETWORK: REVIEW REMOTE ACCESS SOLUTIONS	SMEs should regularly review any remote access tools to ensure they are secure, particularly: - Ensure all remote access software is patched and up date. 2. Restrict remote access from suspicious geographical locations or certain IP addresses. 3. Restrict staff remote access only to the systems and computers they need for their work. 4. Enforce strong passwords for remote access and where possible enable multi-factor authentication. 5. Ensure monitoring and alerting is enabled to warn of suspected attacks or unusual suspicious activity.	cts-lts-enable	Use LTS to centrally collect CTS data.

Guideline No.	Guideline Description	Rule	Solution
7_SECURE YOUR NETWORK: REVIEW REMOTE ACCESS SOLUTIONS	SMEs should regularly review any remote access tools to ensure they are secure, particularly: - Ensure all remote access software is patched and up date. 2. Restrict remote access from suspicious geographical locations or certain IP addresses. 3. Restrict staff remote access only to the systems and computers they need for their work. 4. Enforce strong passwords for remote access and where possible enable multi-factor authentication. 5. Ensure monitoring and alerting is enabled to warn of suspected attacks or unusual suspicious activity.	cts-tracker-exists	Ensure that a CTS tracker has been created for your account to record operations on the Huawei Cloud management console.

Guideline No.	Guideline Description	Rule	Solution
7_SECURE YOUR NETWORK: REVIEW REMOTE ACCESS SOLUTIONS	SMEs should regularly review any remote access tools to ensure they are secure, particularly: - Ensure all remote access software is patched and up date. 2. Restrict remote access from suspicious geographical locations or certain IP addresses. 3. Restrict staff remote access only to the systems and computers they need for their work. 4. Enforce strong passwords for remote access and where possible enable multi-factor authentication. 5. Ensure monitoring and alerting is enabled to warn of suspected attacks or unusual suspicious activity.	multi-region-cts-tracker-exists	Create CTS trackers for different regions to satisfy different customer requirements and meets the laws and regulations of different regions.

Guideline No.	Guideline Description	Rule	Solution
7_SECURE YOUR NETWORK: REVIEW REMOTE ACCESS SOLUTIONS	SMEs should regularly review any remote access tools to ensure they are secure, particularly: - Ensure all remote access software is patched and up date. 2. Restrict remote access from suspicious geographical locations or certain IP addresses. 3. Restrict staff remote access only to the systems and computers they need for their work. 4. Enforce strong passwords for remote access and where possible enable multi-factor authentication. 5. Ensure monitoring and alerting is enabled to warn of suspected attacks or unusual suspicious activity.	vpc-flow-logs-enabled	Enable flow logs for VPCs to monitor network traffic, analyze network attacks, and optimize security group and ACL configurations.

Guideline No.	Guideline Description	Rule	Solution
9_SECURE BACKUPS	To enable the recovery of key formation, backups should be maintained as they are an effective way to recover from disasters such as a ransomware attack. The following backup rules should apply: 1. Backup is regular and automated whenever possible. 2. Backup is held separately from the SME's production environment. 3. Backups are encrypted, especially if they are going to be moved between locations. 4. The ability to regularly restore data from the backups is tested. Ideally, a regular test of a full restore from start to finish should be done.	rds-instance-enable-backup	Enable backups for RDS instances.

Guideline No.	Guideline Description	Rule	Solution
9_SECURE BACKUPS	To enable the recovery of key formation, backups should be maintained as they are an effective way to recover from disasters such as a ransomware attack. The following backup rules should apply: 1. Backup is regular and automated whenever possible. 2. Backup is held separately from the SME's production environment. 3. Backups are encrypted, especially if they are going to be moved between locations. 4. The ability to regularly restore data from the backups is tested. Ideally, a regular test of a full restore from start to finish should be done.	dws-enable-snapshot	Enable snapshots for DWS clusters. Automated snapshots are enabled by default when a cluster is created. Snapshots are periodically taken of a cluster based on the specified time and interval, usually every eight hours. Users can configure one or more automated snapshot policies for the cluster as needed.

Guideline No.	Guideline Description	Rule	Solution
9_SECURE BACKUPS	To enable the recovery of key formation, backups should be maintained as they are an effective way to recover from disasters such as a ransomware attack. The following backup rules should apply: Backup is regular and automated whenever possible; backup is held separately from the SME's production environment; backups are encrypted, especially if they are going to be moved between locations; the ability to regularly restore data from the backups is tested. Ideally, a regular test of a full restore from start to finish should be done.	gaussdb-nosql-enable-backup	Enable backups for GaussDB NoSQL.

4.5.22 Compliance Package for SWIFT CSP

This section describes the background, applicable scenarios, and the compliance package to meet requirements by SWIFT Customer Security Program (CSP).

Background

SWIFT CSP is a cloud security solution launched by SWIFT. It aims to provide more secure and reliable transaction services for financial institutions. For more information about SWIFT CSP, visit the SWFIT official website: **https://www.swift.com/**.

Exemption Clauses

This package provides you with general guide to help you quickly create scenario-based conformance packages. The conformance package and rules included only apply to cloud service and do not represent any legal advice. This conformance package does not ensure compliance with specific laws, regulations, or industry standards. You are responsible for the compliance and legality of your business and technical operations and assume all related responsibilities.

Compliance Rules

The guideline No. in the following table are in consistent with the chapter No. in **https://www.swift.com/**.

Table 4-8 Rules in the conformance package

Guideline No.	Rule	Solution
1.1	ecs-instance-no-public-ip	Restrict public access to ECSs to protect sensitive data.
1.1	ecs-instance-in-vpc	Include all ECSs in VPCs.
1.1	vpc-default-sg-closed	Use security groups to control access within a VPC. You can directly use the default security group for resource access control.
1.1	vpc-acl-unused-check	Use this rule to identity unattached ACLs. An ACL helps control traffic in and out of a subnet.
1.1	vpc-sg-ports-check	Use security groups to control prot connections for VPCs.
1.2	iam-customer-policy-blocked-kms-actions	Use this rule to identity policies that disable KMS encryption.
1.2	iam-group-has-users-check	Add IAM users to at least one user group so that users can inherit permissions attached to the user group that they are in.
1.2	vpc-sg-restricted-ssh	Configure security groups to only allow connections to SSH port 22 of ECSs with specified IPs, so remote access to ECS can be secure.
1.2	smn-lts-enable	Enable LTS for SMN topics.
1.4	private-nat-gateway-authorized-vpc-only	Use private NAT gateways to control VPC connections.
1.4	vpc-sg-restricted-common-ports	Configure security groups to control connections to common ports in a VPC.

Guideline No.	Rule	Solution
1.4	function-graph-public-access-prohibited	Block public access to FunctionGraph functions and manage access to Huawei Cloud resources. Public access may reduce resource availability.
2.3	ecs-multiple-public-ip-check	Use this rule to identify ECSs that allow access from multiple public IPs. ECSs that can be accessed by multiple public IPs may have security risks.
2.3	volume-unused-check	Use this rule to identity idle cloud disks.
2.3	kms-not-scheduled-for-deletion	Use this rule to identify KMS keys that are scheduled for deletion.
2.5A	sfsturbo-encrypted-check	Enable KMS encryption for SFS Turbo file systems.
2.5A	volumes-encrypted-check	Enable encryption for EVS to protect data.
4.1	iam-password-policy	Set thresholds for IAM user password strength.
4.1	access-keys-rotated	Enable key rotation.
4.2	iam-user-mfa-enabled	Enable MFA for all IAM users to prevent account theft.
4.2	mfa-enabled-for-iam-console-access	Enable MFA for all IAM users who can access Huawei Cloud management console. MFA enhances account security to prevent account theft and protect sensitive data.
4.2	root-account-mfa-enabled	Enable MFA for root users. MFA enhances account security.
5.1	iam-role-has-all-permissions	Grant IAM users only necessary permissions to perform required operations to ensure compliance with the least privilege and SOD principles
5.1	iam-root-access-key-check	Ensure that the root access key has been deleted.
5.1	iam-user-group-membership-check	Add IAM users to user groups so that users can inherit permissions attached to user groups that they are in.
6.4	cts-lts-enable	Use LTS to centrally collect CTS data.
6.4	cts-tracker-exists	Ensure that a CTS tracker has been created for your account to record operations on the Huawei Cloud management console.

Guideline No.	Rule	Solution
6.4	multi-region-cts-tracker-exists	Create CTS trackers for different regions where your services are deployed. When you enable CTS for the first time, a management tracker named system is created automatically. You can create multiple trackers for different regions to help make services better satisfy customer needs as well as legal or regulatory requirements.
6.4	cts-kms-encrypted-check	Enable trace file encryption for CTS trackers.
6.4	cts-support-validate-check	Enable file verification for CTS trackers to prevent log files from being modified or deleted after being stored.
6.4	stopped-ecs-date-diff	Use this rule to identify ECSs that have been stopped for more than the allowed time period.
6.4	vpc-flow-logs-enabled	Enable flow logs for VPCs to monitor network traffic, analyze network attacks, and optimize security group and ACL configurations.

4.5.23 Compliance Package for Germany Cloud Computing Compliance Criteria Catalogue

This section describes the background, applicable scenarios, and the compliance package to meet requirements by Germany Cloud Computing Compliance Criteria Catalogue (C5).

Background

C5 is a guide on how to adopt cloud computing. It provides best practices on data protection, data sovereignty, transparency, responsibility, and cloud service provider selection. For more information about this guide, see **C5_2020**.

Applicable Scenarios

This compliance package is intended to help enterprises to develop cloud computing in Germany and meet C5 requirements related laws and regulations. This package needs to be reviewed and implemented based on specific conditions.

Exemption Clauses

This package provides you with general guide to help you quickly create scenario-based conformance packages. The conformance package and rules included only apply to cloud service and do not represent any legal advice. This conformance

package does not ensure compliance with specific laws, regulations, or industry standards. You are responsible for the compliance and legality of your business and technical operations and assume all related responsibilities.

Rules

The guideline No. in the following table are in consistent with the chapter No. in **C5_2020**.

Table 4-9 Rules in this conformance package

Guideline No.	Rule	Solution
COS-03	drs-data-guard-job-not-public	Block public access to DRS real-time DR tasks.
COS-03	drs-migration-job-not-public	Block public access to DRS real-time migration tasks.
COS-03	drs-synchronization-job-not-public	Block public access to DRS real-time synchronization tasks.
COS-03	ecs-instance-no-public-ip	Block public access to ECSs to protect sensitive data.
COS-03	ecs-instance-in-vpc	Include all ECSs in VPCs.
COS-03	css-cluster-in-vpc	Include all CSS clusters in VPCs.
COS-03	css-cluster-in-vpc	Include all CSS clusters in VPCs.
COS-03	mrs-cluster-no-public-ip	Block access to MRS clusters through public networks to protect sensitive data.
COS-03	function-graph-public-access-prohibited	Block public access to FunctionGraph functions. Public access may reduce resource availability.
COS-03	rds-instance-no-public-ip	Block access to cloud databases from public networks to protect sensitive data.
COS-03	vpc-sg-restricted-common-ports	Configure security groups to control connections to common ports in a VPC.
COS-03	vpc-sg-restricted-ssh	Configure security groups to only allow connections to SSH port 22 of ECSs with specified IPs, so remote access to ECS can be secure.
COS-03	vpc-default-sg-closed	Use security groups to control access within a VPC. You can directly use the default security group for resource access control.

Guideline No.	Rule	Solution
COS-03	vpc-sg-ports-check	Use security groups to control prot connections for VPCs.
COS-05	iam-user-mfa-enabled	Enable MFA for all IAM users to prevent account theft.
COS-05	mfa-enabled-for-iam-console-access	Enable MFA for all IAM users who can access Huawei Cloud management console. MFA enhances account security to prevent account theft and protect sensitive data.
COS-05	root-account-mfa-enabled	Enable MFA for root users. MFA enhances account security.
COS-05	ecs-instance-no-public-ip	Block public access to ECSs to protect sensitive data.
COS-05	mrs-cluster-no-public-ip	Block access to MRS clusters through public networks to protect sensitive data.
COS-05	rds-instance-no-public-ip	Block access to cloud databases from public networks to protect sensitive data.
COS-05	vpc-sg-restricted-common-ports	Configure security groups to control connections to common ports in a VPC.
COS-05	vpc-sg-restricted-ssh	Configure security groups to only allow connections to SSH port 22 of ECSs with specified IPs, so remote access to ECS can be secure.
COS-05	vpc-default-sg-closed	Use security groups to control access within a VPC. You can directly use the default security group for resource access control.
COS-05	vpc-sg-ports-check	Use security groups to control connections to specified ports.
CRY-02	apig-instances-ssl-enabled	Enable SSL for APIG REST APIs to authenticate API requests.
CRY-02	elb-predefined-security-policy-https-check	Ensure that your dedicated load balancers are configured with specified security policy to enhance service security.
CRY-02	css-cluster-https-required	Enable HTTPS for CSS clusters to ensure data security and allow access over public networks.
CRY-02	css-cluster-disk-encryption-check	Enable disk encryption for CSS clusters to protect sensitive data.
CRY-02	elb-tls-https-listeners-only	Ensure that your load balancer listeners are configured with the HTTPS protocol.

Guideline No.	Rule	Solution
CRY-02	dws-enable-ssl	Enable SSL for DWS clusters to protect data.
CRY-02	css-cluster-disk-encryption-check	Enable disk encryption for CSS clusters to protect sensitive data.
CRY-03	cts-kms-encrypted-check	Enable trace file encryption for CTS trackers.
CRY-03	sfsturbo-encrypted-check	Enable KMS encryption for SFS Turbo file systems.
CRY-03	volumes-encrypted-check	Enable encryption for EVS to protect data.
CRY-03	rds-instances-enable-kms	Enable KMS encryption for RDS instances to protect sensitive data.
CRY-04	kms-rotation-enabled	Enable KMS key rotation.
DEV-07	cts-lts-enable	Use LTS to centrally collect CTS data.
DEV-07	cts-tracker-exists	Ensure that a CTS tracker has been created for your account to record operations on the Huawei Cloud management console.
DEV-07	multi-region-cts-tracker-exists	Create CTS trackers for different regions where your services are deployed. When you enable CTS for the first time, a management tracker named system is created automatically. You can create multiple trackers for different regions to help make services better satisfy customer needs as well as legal or regulatory requirements.
DEV-07	cts-obs-bucket-track	Create at least one CTS tracker for specified OBS buckets
DEV-07	multi-region-cts-tracker-exists	Create CTS trackers for different regions to satisfy different customer requirements and meets the laws and regulations of different regions.
IDM-01	access-keys-rotated	Enable key rotation.
IDM-01	mrs-cluster-kerberos-enabled	Enable Kerberos for MRS clusters.
IDM-01	iam-password-policy	Set thresholds for IAM user password strength.

Guideline No.	Rule	Solution
IDM-01	iam-root-access-key-check	Ensure that the root access key has been deleted.
IDM-01	iam-user-group-membership-check	Add IAM users to user groups so that users can inherit permissions attached to user groups that they are in.
IDM-01	iam-user-mfa-enabled	Enable MFA for all IAM users to prevent account theft.
IDM-01	mfa-enabled-for-iam-console-access	Enable MFA for all IAM users who can access Huawei Cloud management console. MFA enhances account security to prevent account theft and protect sensitive data.
IDM-01	root-account-mfa-enabled	Enable MFA for root users. MFA enhances account security.
IDM-01	iam-group-has-users-check	Add IAM users to at least one user group so that users can inherit permissions attached to the user group that they are in.
IDM-01	iam-role-has-all-permissions	Grant IAM users only necessary permissions to perform required operations to ensure compliance with the least privilege and SOD principles
IDM-08	iam-password-policy	Set thresholds for IAM user password strength.
CRY-01	iam-password-policy	Set thresholds for IAM user password strength.
IDM-09	iam-user-mfa-enabled	Enable MFA for all IAM users to prevent account theft.
IDM-09	mfa-enabled-for-iam-console-access	Enable MFA for all IAM users who can access Huawei Cloud management console. MFA enhances account security to prevent account theft and protect sensitive data.
IDM-09	root-account-mfa-enabled	Enable MFA for root users. MFA enhances account security.
OPS-01	rds-instance-multi-az-support	Deploy RDS instance across AZs to increase service availability. RDS automatically creates a primary DB instance and replicates data to standby DB instances in different AZs that are physically separate. If an infrastructure fault occurs, RDS automatically fails over to the standby database so that you can restore databases in a timely manner.

Guideline No.	Rule	Solution
OPS-02	as-group-elb-healthcheck-required	Enable health check for AS groups. Elastic Load Balance (ELB) automatically distributes incoming traffic across multiple backend cloud servers based on forwarding policies.
OPS-02	rds-instance-multi-az-support	Deploy RDS instance across AZs to increase service availability. RDS automatically creates a primary DB instance and replicates data to standby DB instances in different AZs that are physically separate. If an infrastructure fault occurs, RDS automatically fails over to the standby database so that you can restore databases in a timely manner.
OPS-07	rds-instance-enable-backup	Enable backups for RDS instances.
OPS-07	dws-enable-snapshot	Enable snapshots for DWS clusters. Automated snapshots are enabled by default when a cluster is created. Snapshots are periodically taken of a cluster based on the specified time and interval, usually every eight hours. Users can configure one or more automated snapshot policies for the cluster as needed.
OPS-07	gaussdb-nosql-enable-backup	Enable backups for GaussDB NoSQL.
OPS-14	cts-support-validate-check	Enable file verification for CTS trackers to prevent log files from being modified or deleted after being stored.
OPS-14	cts-kms-encrypted-check	Enable trace file encryption for CTS trackers.
OPS-15	apig-instances-execution-logging-enabled	Enable CTS for your dedicated API gateways. APIG supports custom log analysis templates, which you can use to collect and manage logs and trace and analyze API request exceptions.
OPS-15	cts-lts-enable	Use LTS to centrally collect CTS data.
OPS-15	dws-enable-log-dump	Enable log dumps to obtain access information for DWS clusters.
OPS-15	vpc-flow-logs-enabled	Enable flow logs for VPCs to monitor network traffic, analyze network attacks, and optimize security group and ACL configurations.

Guideline No.	Rule	Solution
OPS-15	cts-tracker-exists	Ensure that a CTS tracker has been created for your account to record operations on the Huawei Cloud management console.
OPS-15	multi-region-cts-tracker-exists	Create CTS trackers for different regions where your services are deployed. When you enable CTS for the first time, a management tracker named system is created automatically. You can create multiple trackers for different regions to help make services better satisfy customer needs as well as legal or regulatory requirements.
OPS-15	cts-obs-bucket-track	Create at least one CTS tracker for each OBS bucket.
OPS-15	multi-region-cts-tracker-exists	Create CTS trackers for different regions where your services are deployed. When you enable CTS for the first time, a management tracker named system is created automatically. You can create multiple trackers for different regions to help make services better satisfy customer needs as well as legal or regulatory requirements.
PSS-05	iam-user-mfa-enabled	Enable MFA for all IAM users to prevent account theft.
PSS-05	mfa-enabled-for-iam-console-access	Enable MFA for all IAM users who can access Huawei Cloud management console. MFA enhances account security to prevent account theft and protect sensitive data.
PSS-05	root-account-mfa-enabled	Enable MFA for root users. MFA enhances account security.
PSS-07	iam-password-policy	Set thresholds for IAM user password strength.

4.5.24 Compliance Package for PCI DSS

This section describes the background, applicable scenarios, and the compliance package to meet requirements of the Payment Card Industry Data Security Standard (PCI-DSS).

Background

PCI DSS is an information security standard for safe payments worldwide. PCI DSS contains technical and operational baselines to ensure data security of paying

accounts. Although specifically designed to focus on environments with payment card account data, PCI DSS can also help reduce payment threats and protect the people, processes, and technologies across the payment ecosystem. For more information about PCI DSS, see **PCI DSS: v3.2.1**.

Applicable Scenarios

This conformance package helps enterprises meet PCI DSS and legal requirements for safe card payments. It needs to be reviewed and implemented based on specific conditions.

Exemption Clauses

This package provides you with general guide to help you quickly create scenario-based conformance packages. The conformance package and rules included only apply to cloud service and do not represent any legal advice. This conformance package does not ensure compliance with specific laws, regulations, or industry standards. You are responsible for the compliance and legality of your business and technical operations and assume all related responsibilities.

Rules

The guideline numbers in the following table are in consistent with the chapter numbers in **PCI DSS: v3.2.1**.

Table 4-10 Rules in the conformance package

Guideline No.	Guideline Description	Rule Name	Solution
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	css-cluster-in-vpc	Deploy all CSS clusters within VPCs.
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	css-cluster-in-vpc	Deploy all CSS clusters within VPCs.
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	drs-data-guard-job-not-public	Block public access to DRS real-time DR tasks.

Guideline No.	Guideline Description	Rule Name	Solution
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	drs-migration-job-not-public	Block public access to DRS real-time migration tasks.
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	drs-synchronization-job-not-public	Block public access to DRS real-time synchronization tasks.
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	ecs-instance-in-vpc	Deploy all ECSs within VPCs.
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	ecs-instance-no-public-ip	Block public access to ECSs to protect data.
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	function-graph-inside-vpc	Configure VPC access for all functions using the FunctionGraph service.
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	function-graph-public-access-prohibited	Block public access to FunctionGraph functions. Public access may affect resource availability.
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	mrs-cluster-no-public-ip	Block public access to MRS clusters. MRS instances may contain sensitive information, and access control is required.

Guideline No.	Guideline Description	Rule Name	Solution
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	rds-instance-no-public-ip	Block access to RDS instances over public networks. RDS instances may contain sensitive information, and access control is required.
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	vpc-default-sg-closed	Use security groups to control access within a VPC. You can directly use the default security group for resource access control.
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	vpc-sg-ports-check	Use security groups to control connections to specified ports.
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	vpc-sg-restricted-common-ports	Configure security groups to control connections to common ports in a VPC.
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	vpc-sg-restricted-ssh	Configure security groups to restrict connections to SSH port 22 of ECSs.

Guideline No.	Guideline Description	Rule Name	Solution
2.1	Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.).	root-account-mfa-enabled	Enable MFA for root users. MFA provides additional protection to login credentials.
2.1	Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.).	vpc-default-sg-closed	Use security groups to control access within a VPC. You can directly use the default security group for resource access control.

Guideline No.	Guideline Description	Rule Name	Solution
2.2	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardIPng standards. Sources of industry-accepted system hardIPng standards may include, but are not limited to: Center for Internet Security (CIS), International Organization for Standardization (ISO), SysAdmin Audit Network Security (SANS), and Institute National Institute of Standards Technology (NIST).	access-keys-rotated	Enable key rotation.

Guideline No.	Guideline Description	Rule Name	Solution
2.2	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardIPng standards may include, but are not limited to: Center for Internet Security (CIS), International Organization for Standardization (ISO), SysAdmin Audit Network Security (SANS), and Institute National Institute of Standards Technology (NIST).	access-keys-rotated	Enable key rotation.

Guideline No.	Guideline Description	Rule Name	Solution
2.2	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardIPng standards may include, but are not limited to: Center for Internet Security (CIS), International Organization for Standardization (ISO), SysAdmin Audit Network Security (SANS), and Institute National Institute of Standards Technology (NIST).	cts-kms-encrypted-check	Enable trace file encryption for CTS trackers.

Guideline No.	Guideline Description	Rule Name	Solution
2.2	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardIPng standards may include, but are not limited to: Center for Internet Security (CIS), International Organization for Standardization (ISO), SysAdmin Audit Network Security (SANS), and Institute National Institute of Standards Technology (NIST).	cts-lts-enable	Enable **Transfer to LTS** for CTS trackers.

Guideline No.	Guideline Description	Rule Name	Solution
2.2	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources for guidance on configuration standards include but are not limited to: Center for Internet Security (CIS), International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), Cloud Security Alliance, and product vendors.	cts-obs-bucket-track	Create at least one CTS tracker for each OBS bucket.

Guideline No.	Guideline Description	Rule Name	Solution
2.2	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardIPng standards may include, but are not limited to: Center for Internet Security (CIS), International Organization for Standardization (ISO), SysAdmin Audit Network Security (SANS), and Institute National Institute of Standards Technology (NIST).	cts-support-validate-check	Enable trace file verification for CTS trackers to prevent logs from being modified or deleted after being stored.

Guideline No.	Guideline Description	Rule Name	Solution
2.2	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardIPng standards may include, but are not limited to: Center for Internet Security (CIS), International Organization for Standardization (ISO), SysAdmin Audit Network Security (SANS), and Institute National Institute of Standards Technology (NIST).	ecs-in-allowed-security-groups	Use security groups to control access to ECSs. The rules of a security group will apply to all ECSs that are added to this security group.

Guideline No.	Guideline Description	Rule Name	Solution
2.2	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardIPng standards may include, but are not limited to: Center for Internet Security (CIS), International Organization for Standardization (ISO), SysAdmin Audit Network Security (SANS), and Institute National Institute of Standards Technology (NIST).	ecs-multiple-public-ip-check	Use this rule to identify ECSs that allow access from multiple public IPs. ECSs that can be accessed by multiple public IPs may increase security risks.

Guideline No.	Guideline Description	Rule Name	Solution
2.2	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardIPng standards may include, but are not limited to: Center for Internet Security (CIS), International Organization for Standardization (ISO), SysAdmin Audit Network Security (SANS), and Institute National Institute of Standards Technology (NIST).	iam-policy-no-statements-with-admin-access	Grant IAM users only necessary permissions for performing specific operations. Granting users more permissions than they need may violate the principles of least privilege and separation of duties.

Guideline No.	Guideline Description	Rule Name	Solution
2.2	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardIPng standards may include, but are not limited to: Center for Internet Security (CIS), International Organization for Standardization (ISO), SysAdmin Audit Network Security (SANS), and Institute National Institute of Standards Technology (NIST).	iam-root-access-key-check	Grant IAM users only necessary permissions for performing specific operations. Granting users more permissions than they need may violate the principles of least privilege and separation of duties.
2.2	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.	iam-user-group-membership-check	Ensure each user is in at least one user group for permission management. Granting users more permissions than they need may violate the principles of least privilege and separation of duties.

Guideline No.	Guideline Description	Rule Name	Solution
2.2	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardIPng standards may include, but are not limited to: Center for Internet Security (CIS), International Organization for Standardization (ISO), SysAdmin Audit Network Security (SANS), and Institute National Institute of Standards Technology (NIST).	kms-rotation-enabled	Enable KMS key rotation.

Guideline No.	Guideline Description	Rule Name	Solution
2.2	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardIPng standards may include, but are not limited to: Center for Internet Security (CIS), International Organization for Standardization (ISO), SysAdmin Audit Network Security (SANS), and Institute National Institute of Standards Technology (NIST).	mfa-enabled-for-iam-console-access	Enable MFA for all IAM users who can access Huawei Cloud management console. MFA enhances account security to prevent account theft and protect sensitive data.

Guideline No.	Guideline Description	Rule Name	Solution
2.2	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardIPng standards may include, but are not limited to: Center for Internet Security (CIS), International Organization for Standardization (ISO), SysAdmin Audit Network Security (SANS), and Institute National Institute of Standards Technology (NIST).	multi-region-cts-tracker-exists	Create CTS trackers for different regions where your services are deployed. When you enable CTS for the first time, a management tracker named system is created automatically. You can create multiple trackers for different regions to help make services better satisfy customer needs as well as legal or regulatory requirements.

Guideline No.	Guideline Description	Rule Name	Solution
2.2	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardIPng standards. Sources of industry-accepted system hardIPng standards may include, but are not limited to: Center for Internet Security (CIS), International Organization for Standardization (ISO), SysAdmin Audit Network Security (SANS), and Institute National Institute of Standards Technology (NIST).	root-account-mfa-enabled	Enable MFA for root users. MFA provides additional protection to login credentials.

Guideline No.	Guideline Description	Rule Name	Solution
2.2	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardIPng standards may include, but are not limited to: Center for Internet Security (CIS), International Organization for Standardization (ISO), SysAdmin Audit Network Security (SANS), and Institute National Institute of Standards Technology (NIST).	volumes-encrypted-check	Enable encryption for every EVS disks to protect data.

Guideline No.	Guideline Description	Rule Name	Solution
2.2	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardIPng standards may include, but are not limited to: Center for Internet Security (CIS), International Organization for Standardization (ISO), SysAdmin Audit Network Security (SANS), and Institute National Institute of Standards Technology (NIST).	vpc-default-sg-closed	Use security groups to control access within a VPC. You can directly use the default security group for resource access control.

Guideline No.	Guideline Description	Rule Name	Solution
2.2	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardIPng standards may include, but are not limited to: Center for Internet Security (CIS), International Organization for Standardization (ISO), SysAdmin Audit Network Security (SANS), and Institute National Institute of Standards Technology (NIST).	vpc-flow-logs-enabled	Enable flow logs for VPCs to help monitor network traffic, analyze network attacks, and optimize security group and ACL configurations.

Guideline No.	Guideline Description	Rule Name	Solution
2.2	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardIPng standards may include, but are not limited to: Center for Internet Security (CIS), International Organization for Standardization (ISO), SysAdmin Audit Network Security (SANS), and Institute National Institute of Standards Technology (NIST).	vpc-sg-restricted-common-ports	Configure security groups to control access to resources in a VPC using common ports.

Guideline No.	Guideline Description	Rule Name	Solution
2.2	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardIPng standards may include, but are not limited to: Center for Internet Security (CIS), International Organization for Standardization (ISO), SysAdmin Audit Network Security (SANS), and Institute National Institute of Standards Technology (NIST).	vpc-sg-restricted-ssh	Configure security groups to restrict connections to SSH port 22.
2.3	Encrypt all non-console administrative access using strong cryptography.	apig-instances-ssl-enabled	Enable SSL for APIG REST APIs to authenticate API requests.
2.3	Encrypt all non-console administrative access using strong cryptography.	css-cluster-https-required	Enable HTTPS on clusters. After HTTPS is disabled, HTTP protocol is used for cluster communication. In this case, data security cannot be ensured and public IP address cannot be used.
2.3	Encrypt all non-console administrative access using strong cryptography.	dws-enable-ssl	Enable SSL for DWS clusters to protect data.

Guideline No.	Guideline Description	Rule Name	Solution
2.3	Encrypt all non-console administrative access using strong cryptography.	elb-tls-https-listeners-only	Ensure that your load balancer listeners are configured with the HTTPS protocol.
2.4	Maintain an inventory of system components that are in scope for PCI DSS.	ecs-in-allowed-security-groups	Use security groups to control access to ECSs. The rules of a security group will apply to all ECSs that are added to this security group. You can also associate more strict security groups to specific ECSs.
2.4	Maintain an inventory of system components that are in scope for PCI DSS.	eip-unbound-check	Ensure that there are no unattached EIPs.
2.4	Maintain an inventory of system components that are in scope for PCI DSS.	eip-use-in-specified-days	Ensure that there are no unattached EIPs.
2.4	Maintain an inventory of system components that are in scope for PCI DSS.	vpc-acl-unused-check	Use this rule to identity unattached ACLs. An ACL helps control traffic in and out of a subnet.

Guideline No.	Guideline Description	Rule Name	Solution
3.4	Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: one-way hashes based on strong cryptography (hash must be of the entire PAN), truncation (hashing cannot be used to replace the truncated segment of PAN), index tokens and pads (pads must be securely stored), and strong cryptography with associated key-management processes and procedures. Note: It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.	cts-kms-encrypted-check	Enable trace file encryption for CTS trackers.

Guideline No.	Guideline Description	Rule Name	Solution
3.4	Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: one-way hashes based on strong cryptography (hash must be of the entire PAN), truncation (hashing cannot be used to replace the truncated segment of PAN), index tokens and pads (pads must be securely stored), and strong cryptography with associated key-management processes and procedures. Note: It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.	rds-instances-enable-kms	Enable KMS encryption for RDS instances to protect data.

Guideline No.	Guideline Description	Rule Name	Solution
3.4	Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: one-way hashes based on strong cryptography (hash must be of the entire PAN), truncation (hashing cannot be used to replace the truncated segment of PAN), index tokens and pads (pads must be securely stored), and strong cryptography with associated key-management processes and procedures. Note: It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.	sfsturbo-encrypted-check	Enable KMS encryption for SFS Turbo file systems.

Guideline No.	Guideline Description	Rule Name	Solution
3.4	Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: one-way hashes based on strong cryptography (hash must be of the entire PAN), truncation (hashing cannot be used to replace the truncated segment of PAN), index tokens and pads (pads must be securely stored), and strong cryptography with associated key-management processes and procedures. Note: It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.	volumes-encrypted-check	Enable encryption for EVS to protect data.

Guideline No.	Guideline Description	Rule Name	Solution
4.1	Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: Only trusted keys and certificates are accepted. The protocol in use only supports secure versions or configurations. The encryption strength is appropriate for the encryption methodology in use. Examples of open, public networks include but are not limited to: The Internet Wireless technologies, including 802.11 and Bluetooth Cellular technologies, for example, Global System for Mobile communications (GSM), code division multiple access (CDMA), General Packet Radio Service (GPRS), and satellite communications.	apig-instances-ssl-enabled	Enable SSL for API Gateway REST APIs to authenticate API requests.

Guideline No.	Guideline Description	Rule Name	Solution
4.1	Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: Only trusted keys and certificates are accepted. The protocol in use only supports secure versions or configurations. The encryption strength is appropriate for the encryption methodology in use. Examples of open, public networks include but are not limited to: The Internet Wireless technologies, including 802.11 and Bluetooth Cellular technologies, for example, Global System for Mobile communications (GSM), code division multiple access (CDMA), General Packet Radio Service (GPRS), and satellite communications.	css-cluster-disk-encryption-check	Enable disk encryption for CSS clusters to protect data.

Guideline No.	Guideline Description	Rule Name	Solution
4.1	Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: Only trusted keys and certificates are accepted. The protocol in use only supports secure versions or configurations. The encryption strength is appropriate for the encryption methodology in use. Examples of open, public networks include but are not limited to: The Internet Wireless technologies, including 802.11 and Bluetooth Cellular technologies, for example, Global System for Mobile communications (GSM), code division multiple access (CDMA), General Packet Radio Service (GPRS), and satellite communications.	css-cluster-disk-encryption-check	Enable disk encryption for CSS clusters to protect sensitive data.

Guideline No.	Guideline Description	Rule Name	Solution
4.1	Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: Only trusted keys and certificates are accepted. The protocol in use only supports secure versions or configurations. The encryption strength is appropriate for the encryption methodology in use. Examples of open, public networks include but are not limited to: The Internet Wireless technologies, including 802.11 and Bluetooth Cellular technologies, for example, Global System for Mobile communications (GSM), code division multiple access (CDMA), General Packet Radio Service (GPRS), and satellite communications.	css-cluster-https-required	Enable HTTPS for CSS clusters to ensure data security and allow access over public networks. After HTTPS is disabled, HTTP protocol is used for cluster communication. In this case, data security cannot be ensured and public IP address cannot be used.

Guideline No.	Guideline Description	Rule Name	Solution
4.1	Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: Only trusted keys and certificates are accepted. The protocol in use only supports secure versions or configurations. The encryption strength is appropriate for the encryption methodology in use. Examples of open, public networks include but are not limited to: The Internet Wireless technologies, including 802.11 and Bluetooth Cellular technologies, for example, Global System for Mobile communications (GSM), code division multiple access (CDMA), General Packet Radio Service (GPRS), and satellite communications.	dws-enable-ssl	Enable SSL for DWS clusters to protect data.

Guideline No.	Guideline Description	Rule Name	Solution
4.1	Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: Only trusted keys and certificates are accepted. The protocol in use only supports secure versions or configurations. The encryption strength is appropriate for the encryption methodology in use. Examples of open, public networks include but are not limited to: The Internet Wireless technologies, including 802.11 and Bluetooth Cellular technologies, for example, Global System for Mobile communications (GSM), code division multiple access (CDMA), General Packet Radio Service (GPRS), and satellite communications.	elb-tls-https-listeners-only	Ensure that your load balancer listeners are configured with the HTTPS protocol.

Guideline No.	Guideline Description	Rule Name	Solution
4.1	Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: Only trusted keys and certificates are accepted. The protocol in use only supports secure versions or configurations. The encryption strength is appropriate for the encryption methodology in use. Examples of open, public networks include but are not limited to: The Internet Wireless technologies, including 802.11 and Bluetooth Cellular technologies, for example, Global System for Mobile communications (GSM), code division multiple access (CDMA), General Packet Radio Service (GPRS), and satellite communications.	pca-certificate-authority-expiration-check	Use **Private Certificate Authority** (PCA) to create and manage your private CAs and ensure that there are no expired certificates.

Guideline No.	Guideline Description	Rule Name	Solution
4.1	Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: Only trusted keys and certificates are accepted. The protocol in use only supports secure versions or configurations. The encryption strength is appropriate for the encryption methodology in use. Examples of open, public networks include but are not limited to: The Internet Wireless technologies, including 802.11 and Bluetooth Cellular technologies, for example, Global System for Mobile communications (GSM), code division multiple access (CDMA), General Packet Radio Service (GPRS), and satellite communications.	pca-certificate-expiration-check	Use **Private Certificate Authority** (PCA) to create and manage your private CAs and ensure that there are no expired certificates.

Guideline No.	Guideline Description	Rule Name	Solution
6.2	Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor- supplied security patches. Install critical security patches within one month of release. Note: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.	cce-cluster-end-of-maintenance-version	Ensure that CCE cluster versions can be maintained.
6.2	Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor- supplied security patches. Install critical security patches within one month of release. Note: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.	cce-cluster-oldest-supported-version	Ensure that there are no CCE cluster versions that cannot be maintained. For CCE clusters of supported versions, The system automatically deploys security patches to upgrade your CCE clusters. If any security issue is identified, Huawei Cloud will fix the issue.
10.1	Implement audit trails to link all access to system components to each individual user.	apig-instances-execution-logging-enabled	Enable CTS for your dedicated API gateways. APIG supports custom log analysis templates, which you can use to collect and manage logs and trace and analyze API request exceptions.

Guideline No.	Guideline Description	Rule Name	Solution
10.1	Implement audit trails to link all access to system components to each individual user.	cts-obs-bucket-track	Create at least one CTS tracker for each OBS bucket.
10.1	Implement audit trails to link all access to system components to each individual user.	cts-tracker-exists	Ensure that a CTS tracker has been created for your account to record operations on the Huawei Cloud management console.
10.1	Implement audit trails to link all access to system components to each individual user.	multi-region-cts-tracker-exists	Ensure that there are CTS trackers in regions where your services are deployed. Cloud Trace Service (CTS) allows you to collect, store, and query operation records of cloud resources. When you enable CTS for the first time, a management tracker named **system** is created automatically. You can create multiple trackers.
10.1	Implement audit trails to link all access to system components to each individual user.	vpc-flow-logs-enabled	Enable flow logs for VPCs to help monitor network traffic, analyze network attacks, and optimize security group and ACL configurations.
10.5	Secure audit trails so they cannot be altered.	cts-kms-encrypted-check	Enable trace file encryption for CTS trackers.

Guideline No.	Guideline Description	Rule Name	Solution
11.5	Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.	cts-support-validate-check	Enable trace file verification for CTS trackers to prevent logs from being modified or deleted.
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	css-cluster-in-vpc	Deploy all CSS clusters within VPCs.
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	css-cluster-in-vpc	Deploy all CSS clusters within VPCs.
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	drs-data-guard-job-not-public	Block public access to DRS real-time DR tasks.

Guideline No.	Guideline Description	Rule Name	Solution
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	drs-migration-job-not-public	Block public access to DRS real-time migration tasks.
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	drs-synchronization-job-not-public	Block public access to DRS real-time synchronization tasks.
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	ecs-instance-in-vpc	Deploy all ECSs within VPCs.
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	ecs-instance-no-public-ip	Block public access to ECSs to protect data.
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	function-graph-inside-vpc	Deploy FunctionGraph functions within VPCs.

Guideline No.	Guideline Description	Rule Name	Solution
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	function-graph-public-access-prohibited	Block public access to FunctionGraph functions. Public access may reduce resource availability.
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	mrs-cluster-no-public-ip	Block public access to MRS clusters. MRS instances may contain sensitive information, and access control is required.
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	rds-instance-no-public-ip	Block public access to RDS instances. RDS instances may contain sensitive information, and access control is required.
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	vpc-default-sg-closed	Use security groups to control access within a VPC. You can directly use the default security group for resource access control.
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	vpc-sg-ports-check	Use security groups to control connections to specified ports.

Guideline No.	Guideline Description	Rule Name	Solution
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	vpc-sg-restricted-common-ports	Configure security groups to control connections to common ports in a VPC.
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	vpc-sg-restricted-ssh	Configure security groups to restrict connections to SSH port 24.
1.3.1	Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	css-cluster-in-vpc	Deploy all CSS clusters within VPCs.
1.3.1	Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	css-cluster-in-vpc	Deploy all CSS clusters within VPCs.
1.3.1	Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	drs-data-guard-job-not-public	Block public access to DRS real-time DR tasks.

Guideline No.	Guideline Description	Rule Name	Solution
1.3.1	Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	drs-migration-job-not-public	Block public access to DRS real-time migration tasks.
1.3.1	Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	drs-synchronization-job-not-public	Block public access to DRS real-time synchronization tasks.
1.3.1	Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	ecs-instance-in-vpc	Deploy all ECSs within VPCs.
1.3.1	Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	ecs-instance-no-public-ip	Block public access to ECSs to protect data.
1.3.1	Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	function-graph-inside-vpc	Deploy FunctionGraph functions within VPCs.

Guideline No.	Guideline Description	Rule Name	Solution
1.3.1	Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	function-graph-public-access-prohibited	Block public access to FunctionGraph functions. Public access may reduce resource availability.
1.3.1	Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	mrs-cluster-no-public-ip	Block public access to MRS clusters. MRS instances may contain sensitive information, and access control is required.
1.3.1	Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	rds-instance-no-public-ip	Block public access to RDS instances. RDS instances may contain sensitive information, and access control is required.
1.3.1	Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	vpc-default-sg-closed	Use security groups to control access within a VPC. You can directly use the default security group for resource access control.
1.3.1	Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	vpc-sg-ports-check	Use security groups to control connections to specified ports.

Guideline No.	Guideline Description	Rule Name	Solution
1.3.1	Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	vpc-sg-restricted-common-ports	Configure security groups to control connections to common ports in a VPC.
1.3.1	Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	vpc-sg-restricted-ssh	Configure security groups to restrict connections to SSH port 25.
1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.	css-cluster-in-vpc	Deploy all CSS clusters within VPCs.
1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.	css-cluster-in-vpc	Deploy all CSS clusters within VPCs.
1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.	drs-data-guard-job-not-public	Block public access to DRS real-time DR tasks.
1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.	drs-migration-job-not-public	Block public access to DRS real-time migration tasks.
1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.	drs-synchronization-job-not-public	Block public access to DRS real-time synchronization tasks.
1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.	ecs-instance-in-vpc	Deploy all ECSs within VPCs.

Guideline No.	Guideline Description	Rule Name	Solution
1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.	ecs-instance-no-public-ip	Block public access to ECSs to protect data.
1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.	function-graph-inside-vpc	Deploy FunctionGraph functions within VPCs.
1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.	function-graph-public-access-prohibited	Block public access to FunctionGraph functions. Public access may reduce resource availability.
1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.	mrs-cluster-no-public-ip	Block public access to MRS clusters. MRS instances may contain sensitive information, and access control is required.
1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.	rds-instance-no-public-ip	Block public access to RDS instances. RDS instances may contain sensitive information, and access control is required.
1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.	vpc-default-sg-closed	Use security groups to control access within a VPC. You can directly use the default security group for resource access control.
1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.	vpc-sg-ports-check	Use security groups to control connections to specified ports.
1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.	vpc-sg-restricted-common-ports	Configure security groups to control connections to common ports in a VPC.

Guideline No.	Guideline Description	Rule Name	Solution
1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.	vpc-sg-restricted-ssh	Configure security groups to restrict connections to SSH port 26.
1.3.4	Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	css-cluster-in-vpc	Deploy all CSS clusters within VPCs.
1.3.4	Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	css-cluster-in-vpc	Deploy all CSS clusters within VPCs.
1.3.4	Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	drs-data-guard-job-not-public	Block public access to DRS real-time DR tasks.
1.3.4	Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	drs-migration-job-not-public	Block public access to DRS real-time migration tasks.
1.3.4	Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	drs-synchronization-job-not-public	Block public access to DRS real-time synchronization tasks.
1.3.4	Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	ecs-instance-in-vpc	Deploy all ECSs within VPCs.

Guideline No.	Guideline Description	Rule Name	Solution
1.3.4	Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	ecs-instance-no-public-ip	Block public access to ECSs to protect data.
1.3.4	Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	function-graph-inside-vpc	Deploy FunctionGraph functions within VPCs.
1.3.4	Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	function-graph-public-access-prohibited	Block public access to FunctionGraph functions. Public access may reduce resource availability.
1.3.4	Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	mrs-cluster-no-public-ip	Block public access to MRS clusters. MRS instances may contain sensitive information, and access control is required.
1.3.4	Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	rds-instance-no-public-ip	Block public access to RDS instances. RDS instances may contain sensitive information, and access control is required.
1.3.4	Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	vpc-default-sg-closed	Use security groups to control access within a VPC. You can directly use the default security group for resource access control.
1.3.4	Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	vpc-sg-ports-check	Use security groups to control connections to specified ports.

Guideline No.	Guideline Description	Rule Name	Solution
1.3.4	Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	vpc-sg-restricted-common-ports	Configure security groups to control connections to common ports in a VPC.
1.3.4	Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	vpc-sg-restricted-ssh	Configure security groups to restrict connections to SSH port 27.
1.3.6	Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	css-cluster-in-vpc	Deploy all CSS clusters within VPCs.
1.3.6	Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	css-cluster-in-vpc	Deploy all CSS clusters within VPCs.
1.3.6	Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	drs-data-guard-job-not-public	Block public access to DRS real-time DR tasks.
1.3.6	Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	drs-migration-job-not-public	Block public access to DRS real-time migration tasks.

Guideline No.	Guideline Description	Rule Name	Solution
1.3.6	Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	drs-synchronization-job-not-public	Block public access to DRS real-time synchronization tasks.
1.3.6	Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	ecs-instance-in-vpc	Deploy all ECSs within VPCs.
1.3.6	Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	ecs-instance-no-public-ip	Block public access to ECSs to protect data.
1.3.6	Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	rds-instance-no-public-ip	Block public access to RDS instances. RDS instances may contain sensitive information, and access control is required.
1.3.6	Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	vpc-default-sg-closed	Use security groups to control access within a VPC. You can directly use the default security group for resource access control.

Guideline No.	Guideline Description	Rule Name	Solution
1.3.6	Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	vpc-sg-ports-check	Use security groups to control connections to specified ports.
1.3.6	Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	vpc-sg-restricted-common-ports	Configure security groups to control connections to common ports in a VPC.
1.3.6	Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	vpc-sg-restricted-ssh	Configure security groups to restrict connections to SSH port 28.
10.2.1	Implement automated audit trails for all system components to reconstruct the following events: all individual user accesses to cardholder data.	apig-instances-execution-logging-enabled	Enable CTS for your dedicated API gateways. APIG supports custom log analysis templates, which you can use to collect and manage logs and trace and analyze API request exceptions.
10.2.1	Implement automated audit trails for all system components to reconstruct the following events: all individual user accesses to cardholder data.	cts-obs-bucket-track	Create at least one CTS tracker for each OBS bucket.

Guideline No.	Guideline Description	Rule Name	Solution
10.2.1	Implement automated audit trails for all system components to reconstruct the following events: all individual user accesses to cardholder data.	cts-tracker-exists	Ensure that a CTS tracker has been created for your account to record operations on the Huawei Cloud management console.
10.2.1	Implement automated audit trails for all system components to reconstruct the following events: all individual user accesses to cardholder data.	multi-region-cts-tracker-exists	Create CTS trackers for different regions where your services are deployed. When you enable CTS for the first time, a management tracker named system is created automatically. You can create multiple trackers for different regions to help make services better satisfy customer needs as well as legal or regulatory requirements.
10.2.2	Implement automated audit trails for all system components to reconstruct the following events: All actions taken by any individual with root or administrative privileges.	cts-tracker-exists	Ensure that a CTS tracker has been created for your account to record operations on the Huawei Cloud console.

Guideline No.	Guideline Description	Rule Name	Solution
10.2.2	Implement automated audit trails for all system components to reconstruct the following events: All actions taken by any individual with root or administrative privileges.	multi-region-cts-tracker-exists	Create CTS trackers for different regions where your services are deployed. When you enable CTS for the first time, a management tracker named system is created automatically. You can create multiple trackers for different regions to help make services better satisfy customer needs as well as legal or regulatory requirements.
10.2.3	Implement automated audit trails for all system components to reconstruct the following events: Access to all audit trails.	cts-obs-bucket-track	Create at least one CTS tracker for each OBS bucket.
10.2.3	Implement automated audit trails for all system components to reconstruct the following events: Access to all audit trails.	cts-tracker-exists	Ensure that a CTS tracker has been created for your account to record operations on the Huawei Cloud console.

Guideline No.	Guideline Description	Rule Name	Solution
10.2.3	Implement automated audit trails for all system components to reconstruct the following events: Access to all audit trails.	multi-region-cts-tracker-exists	Create CTS trackers for different regions where your services are deployed. When you enable CTS for the first time, a management tracker named system is created automatically. You can create multiple trackers for different regions to help make services better satisfy customer needs as well as legal or regulatory requirements.
10.2.4	Implement automated audit trails for all system components to reconstruct the following events: Invalid logical access attempts.	apig-instances-execution-logging-enabled	Enable CTS for your dedicated API gateways. APIG supports custom log analysis templates, which you can use to collect and manage logs and trace and analyze API request exceptions.
10.2.4	Implement automated audit trails for all system components to reconstruct the following events: Invalid logical access attempts.	cts-obs-bucket-track	Create at least one CTS tracker for each OBS bucket.
10.2.4	Implement automated audit trails for all system components to reconstruct the following events: Invalid logical access attempts.	cts-tracker-exists	Ensure that a CTS tracker has been created for your account to record operations on the Huawei Cloud console.

Guideline No.	Guideline Description	Rule Name	Solution
10.2.4	Implement automated audit trails for all system components to reconstruct the following events: Invalid logical access attempts.	multi-region-cts-tracker-exists	Create CTS trackers for different regions where your services are deployed. When you enable CTS for the first time, a management tracker named system is created automatically. You can create multiple trackers for different regions to help make services better satisfy customer needs as well as legal or regulatory requirements.
10.2.5	Implement automated audit trails for all system components to reconstruct the following events: Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges.	cts-tracker-exists	Ensure that a CTS tracker has been created for your account to record operations on the Huawei Cloud console.

Guideline No.	Guideline Description	Rule Name	Solution
10.2.5	Implement automated audit trails for all system components to reconstruct the following events: Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges.	multi-region-cts-tracker-exists	Create CTS trackers for different regions where your services are deployed. When you enable CTS for the first time, a management tracker named system is created automatically. You can create multiple trackers for different regions to help make services better satisfy customer needs as well as legal or regulatory requirements.
10.2.6	Implement automated audit trails for all system components to reconstruct the following events: Initialization, stopping, or pausing of the audit logs.	cts-tracker-exists	Ensure that a CTS tracker has been created for your account to record operations on the Huawei Cloud console.
10.2.6	Implement automated audit trails for all system components to reconstruct the following events: Initialization, stopping, or pausing of the audit logs.	multi-region-cts-tracker-exists	Create CTS trackers for different regions where your services are deployed. When you enable CTS for the first time, a management tracker named system is created automatically. You can create multiple trackers for different regions to help make services better satisfy customer needs as well as legal or regulatory requirements.

Guideline No.	Guideline Description	Rule Name	Solution
10.2.7	Implement automated audit trails for all system components to reconstruct the following events: Creation and deletion of system-level objects.	apig-instances-execution-logging-enabled	Enable CTS for your dedicated API gateways. APIG supports custom log analysis templates, which you can use to collect and manage logs and trace and analyze API request exceptions.
10.2.7	Implement automated audit trails for all system components to reconstruct the following events: Creation and deletion of system-level objects.	cts-tracker-exists	Ensure that a CTS tracker has been created for your account to record operations on the Huawei Cloud console.
10.2.7	Implement automated audit trails for all system components to reconstruct the following events: Creation and deletion of system-level objects.	multi-region-cts-tracker-exists	Create CTS trackers for different regions where your services are deployed. When you enable CTS for the first time, a management tracker named system is created automatically. You can create multiple trackers for different regions to help make services better satisfy customer needs as well as legal or regulatory requirements.

Guideline No.	Guideline Description	Rule Name	Solution
10.3.1	Record at least the following audit trail entries for all system components for each event: User identification.	apig-instances-execution-logging-enabled	Enable CTS for your dedicated API gateways. APIG supports custom log analysis templates, which you can use to collect and manage logs and trace and analyze API request exceptions.
10.3.1	Record at least the following audit trail entries for all system components for each event: User identification.	cts-obs-bucket-track	Create at least one CTS tracker for each OBS bucket.
10.3.1	Record at least the following audit trail entries for all system components for each event: User identification.	cts-tracker-exists	Ensure that a CTS tracker has been created for your account to record operations on the Huawei Cloud console.
10.3.1	Record at least the following audit trail entries for all system components for each event: User identification.	multi-region-cts-tracker-exists	Create CTS trackers for different regions where your services are deployed. When you enable CTS for the first time, a management tracker named system is created automatically. You can create multiple trackers for different regions to help make services better satisfy customer needs as well as legal or regulatory requirements.

Guideline No.	Guideline Description	Rule Name	Solution
10.3.1	Record at least the following audit trail entries for all system components for each event: User identification.	vpc-flow-logs-enabled	Enable flow logs for VPCs to help monitor network traffic, analyze network attacks, and optimize security group and ACL configurations.
10.5.2	Protect audit trail files from unauthorized modifications.	cts-kms-encrypted-check	Enable trace file encryption for CTS trackers.
10.5.3	Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	cts-lts-enable	Enable **Transfer to LTS** for CTS trackers.
10.5.5	Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	cts-support-validate-check	Enable trace file verification for CTS trackers to prevent logs from being modified or deleted.
2.2.2	Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	drs-data-guard-job-not-public	Block public access to DRS real-time DR tasks.
2.2.2	Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	drs-migration-job-not-public	Block public access to DRS real-time migration tasks.
2.2.2	Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	drs-synchronization-job-not-public	Block public access to DRS real-time synchronization tasks.

Guideline No.	Guideline Description	Rule Name	Solution
2.2.2	Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	ecs-instance-in-vpc	Deploy all ECSs within VPCs.
2.2.2	Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	ecs-instance-no-public-ip	Block public access to ECSs to protect data.
2.2.2	Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	function-graph-inside-vpc	Deploy FunctionGraph functions within VPCs.
2.2.2	Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	function-graph-public-access-prohibited	Block public access to FunctionGraph functions. Public access may reduce resource availability.
2.2.2	Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	mrs-cluster-no-public-ip	Block public access to MRS clusters. MRS instances may contain sensitive information, and access control is required.
2.2.2	Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	rds-instance-no-public-ip	Block public access to RDS instances. RDS instances may contain sensitive information, and access control is required.
2.2.2	Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	vpc-default-sg-closed	Use security groups to control access within a VPC. You can directly use the default security group for resource access control.

Guideline No.	Guideline Description	Rule Name	Solution
2.2.2	Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	vpc-sg-ports-check	Use security groups to control connections to specified ports.
2.2.2	Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	vpc-sg-restricted-common-ports	Configure security groups to control connections to common ports in a VPC.
2.2.2	Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	vpc-sg-restricted-ssh	Configure security groups to restrict connections to SSH port 29.
3.5.2	Restrict access to cryptographic keys to the fewest number of custodians necessary.	iam-customer-policy-blocked-kms-actions	Use this rule to identity policies that disable KMS encryption. Granting users more permissions than they need may violate the principles of least privilege and separation of duties.

Guideline No.	Guideline Description	Rule Name	Solution
3.6.4	Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).	kms-rotation-enabled	Enable KMS key rotation.
3.6.5	Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised. Note: If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key-encryption key). Archived cryptographic keys should only be used for decryption/ verification purposes.	kms-not-scheduled-for-deletion	Ensure that there are no KMS keys scheduled for deletion.

Guideline No.	Guideline Description	Rule Name	Solution
3.6.7	Prevention of unauthorized substitution of cryptographic keys.	kms-not-scheduled-for-deletion	Ensure that there are no KMS keys scheduled for deletion.
7.1.1	Define access needs for each role, including: system components and data resources that each role needs to access for their job function and level of privilege required (for example, user, administrator, etc.) for accessing resources.	iam-customer-policy-blocked-kms-actions	Use this rule to identity policies that disable KMS encryption. Granting users more permissions than they need may violate the principles of least privilege and separation of duties.
7.1.1	Define access needs for each role, including: system components and data resources that each role needs to access for their job function and level of privilege required (for example, user, administrator, etc.) for accessing resources.	iam-group-has-users-check	Add IAM users to at least one user group so that users can inherit permissions attached to the user group that they are in.
7.1.1	Define access needs for each role, including: system components and data resources that each role needs to access for their job function and level of privilege required (for example, user, administrator, etc.) for accessing resources.	iam-policy-no-statements-with-admin-access	Grant IAM users only necessary permissions for performing specific operations. Granting users more permissions than they need may violate the principles of least privilege and separation of duties.

Guideline No.	Guideline Description	Rule Name	Solution
7.1.1	Define access needs for each role, including: system components and data resources that each role needs to access for their job function and level of privilege required (for example, user, administrator, etc.) for accessing resources.	iam-role-has-all-permissions	Only grant IAM users necessary permissions for performing specific operations. Granting users more permissions than they need may violate the least privilege principle and damage separation of duties.
7.1.1	Define access needs for each role, including: system components and data resources that each role needs to access for their job function and level of privilege required (for example, user, administrator, etc.) for accessing resources.	iam-root-access-key-check	Grant IAM users only necessary permissions for performing specific operations. Granting users more permissions than they need may violate the principles of least privilege and separation of duties.
7.1.1	Define access needs for each role, including: system components and data resources that each role needs to access for their job function and level of privilege required (for example, user, administrator, etc.) for accessing resources.	iam-user-group-membership-check	Ensure each user is in at least one user group for permission management. Granting users more permissions than they need may violate the principles of least privilege and separation of duties.

Guideline No.	Guideline Description	Rule Name	Solution
7.1.1	Define access needs for each role, including: system components and data resources that each role needs to access for their job function and level of privilege required (for example, user, administrator, etc.) for accessing resources.	mrs-cluster-kerberos-enabled	Enable Kerberos for MRS clusters.
7.1.2	Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	iam-customer-policy-blocked-kms-actions	Use this rule to identity policies that disable KMS encryption. Granting users more permissions than they need may violate the principles of least privilege and separation of duties.
7.1.2	Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	iam-group-has-users-check	Add IAM users to at least one user group so that users can inherit permissions attached to the user group that they are in.
7.1.2	Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities	iam-policy-no-statements-with-admin-access	Grant IAM users only necessary permissions for performing specific operations. Granting users more permissions than they need may violate the principles of least privilege and separation of duties.

Guideline No.	Guideline Description	Rule Name	Solution
7.1.2	Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	iam-role-has-all-permissions	Only grant IAM users necessary permissions for performing specific operations. Granting users more permissions than they need may violate the least privilege principle and damage separation of duties.
7.1.2	Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	iam-root-access-key-check	Grant IAM users only necessary permissions for performing specific operations. Granting users more permissions than they need may violate the principles of least privilege and separation of duties.
7.1.2	Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	iam-user-group-membership-check	Ensure each user is in at least one user group for permission management. Granting users more permissions than they need may violate the principles of least privilege and separation of duties.
7.2.1	Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: Coverage of all system components.	iam-customer-policy-blocked-kms-actions	Use this rule to identity policies that disable KMS encryption. Granting users more permissions than they need may violate the principles of least privilege and separation of duties.

Guideline No.	Guideline Description	Rule Name	Solution
7.2.1	Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: Coverage of all system components.	iam-group-has-users-check	Add IAM users to at least one user group so that users can inherit permissions attached to the user group that they are in.
7.2.1	Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: Coverage of all system components.	iam-policy-no-statements-with-admin-access	Grant IAM users only necessary permissions for performing specific operations. Granting users more permissions than they need may violate the principles of least privilege and separation of duties.
7.2.1	Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: Coverage of all system components.	iam-role-has-all-permissions	Only grant IAM users necessary permissions for performing specific operations. Granting users more permissions than they need may violate the least privilege principle and damage separation of duties.

Guideline No.	Guideline Description	Rule Name	Solution
7.2.1	Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: Coverage of all system components.	iam-root-access-key-check	Grant IAM users only necessary permissions for performing specific operations. Granting users more permissions than they need may violate the principles of least privilege and separation of duties.
7.2.1	Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: Coverage of all system components.	iam-user-group-membership-check	Ensure that each user is in at least one user group for permission management. Granting users more permissions than they need may violate the principles of least privilege and separation of duties.
7.2.1	Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: Coverage of all system components.	mrs-cluster-kerberos-enabled	Enable Kerberos for MRS clusters.

Guideline No.	Guideline Description	Rule Name	Solution
7.2.2	Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: Coverage of all system components	iam-customer-policy-blocked-kms-actions	Use this rule to identity policies that disable KMS encryption. Granting users more permissions than they need may violate the principles of least privilege and separation of duties.
7.2.2	Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: Coverage of all system components	iam-group-has-users-check	Add IAM users to at least one user group so that users can inherit permissions attached to the user group that they are in.
7.2.2	Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: Coverage of all system components	iam-policy-no-statements-with-admin-access	Grant IAM users only necessary permissions for performing specific operations. Granting users more permissions than they need may violate the principles of least privilege and separation of duties.

Guideline No.	Guideline Description	Rule Name	Solution
7.2.2	Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: Coverage of all system components	iam-role-has-all-permissions	Only grant IAM users necessary permissions for performing specific operations. Granting users more permissions than they need may violate the least privilege principle and damage separation of duties.
7.2.2	Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: Coverage of all system components	iam-root-access-key-check	Grant IAM users only necessary permissions for performing specific operations. Granting users more permissions than they need may violate the principles of least privilege and separation of duties.
7.2.2	Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: Coverage of all system components	iam-user-group-membership-check	Ensure that each user is in at least one user group for permission management. Granting users more permissions than they need may violate the principles of least privilege and separation of duties.

Guideline No.	Guideline Description	Rule Name	Solution
7.2.2	Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: Coverage of all system components	mrs-cluster-kerberos-enabled	Enable Kerberos for MRS clusters.
8.1.1	Assign all users a unique ID before allowing them to access system components or cardholder data.	iam-root-access-key-check	Grant IAM users only necessary permissions for performing specific operations. Granting users more permissions than they need may violate the principles of least privilege and separation of duties.
8.1.4	Remove/disable inactive user accounts within 90 days.	access-keys-rotated	Enable key rotation.
8.2.1	Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	apig-instances-ssl-enabled	Enable SSL for API Gateway REST APIs to authenticate API requests.
8.2.1	Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	elb-tls-https-listeners-only	Ensure that your load balancer listeners are configured with the HTTPS protocol.

Guideline No.	Guideline Description	Rule Name	Solution
8.2.1	Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	rds-instances-enable-kms	Enable KMS for RDS to encrypt data at rest.
8.2.1	Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	sfsturbo-encrypted-check	Enable KMS for SFS Turbo file systems.
8.2.1	Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	volumes-encrypted-check	Enable encryption for EVS to protect data.
8.2.3	Passwords/ passphrases must meet the following: Require a minimum length of at least seven characters; only digits and letters are allowed; and alternatively, the complexity and strength of the password/passphrase must be at least comparable to the parameters specified above.	iam-password-policy	Set thresholds for IAM user password strength.

Guideline No.	Guideline Description	Rule Name	Solution
8.2.4	Change user passwords/ passphrases at least once every 90 days.	access-keys-rotated	Enable key rotation.
8.2.4	Change user passwords/ passphrases at least once every 90 days.	access-keys-rotated	Enable key rotation.
8.2.4	Change user passwords/ passphrases at least once every 90 days.	iam-password-policy	Set thresholds for IAM user password strength.
8.2.5	Do not allow an individual to submit a new password/ passphrase that is the same as any of the last four passwords/ passphrases he or she has used.	iam-password-policy	Set thresholds for IAM user password strength.
8.3.1	Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.	iam-user-mfa-enabled	Enable MFA for all IAM users. MFA provides an additional layer of protection in addition to the username and password.
8.3.1	Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.	mfa-enabled-for-iam-console-access	Enable MFA for all IAM users who can access Huawei Cloud console. MFA provides an additional layer of protection in addition to the username and password.
8.3.1	Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.	root-account-mfa-enabled	Enable MFA for root users. MFA adds additional protection to login credentials.

Guideline No.	Guideline Description	Rule Name	Solution
8.3.2	Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.	iam-user-mfa-enabled	Enable MFA for all IAM users. MFA provides an additional layer of protection in addition to the username and password.
8.3.2	Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the entity's network.	mfa-enabled-for-iam-console-access	Enable MFA for all IAM users who can access Huawei Cloud console. MFA provides an additional layer of protection in addition to the username and password.
8.3.2	Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the entity's network.	root-account-mfa-enabled	Enable MFA for root users. MFA adds additional protection to login credentials.

4.5.25 Conformance Package for Healthcare Industry

This template contains the following rules:

- apig-instances-execution-logging-enabled
- apig-instances-ssl-enabled
- as-group-elb-healthcheck-required
- css-cluster-disk-encryption-check
- css-cluster-https-required
- css-cluster-in-vpc
- cts-kms-encrypted-check

- cts-lts-enable
- cts-obs-bucket-track
- cts-support-validate-check
- cts-tracker-exists
- drs-data-guard-job-not-public
- drs-migration-job-not-public
- drs-synchronization-job-not-public
- dws-enable-log-dump
- dws-enable-snapshot
- dws-enable-ssl
- ecs-instance-in-vpc
- ecs-instance-no-public-ip
- eip-unbound-check
- eip-use-in-specified-days
- elb-predefined-security-policy-https-check
- elb-tls-https-listeners-only
- function-graph-public-access-prohibited
- gaussdb-nosql-enable-backup
- gaussdb-nosql-enable-disk-encryption
- iam-customer-policy-blocked-kms-actions
- iam-password-policy
- iam-policy-no-statements-with-admin-access
- iam-role-has-all-permissions
- iam-root-access-key-check
- iam-user-mfa-enabled
- kms-not-scheduled-for-deletion
- mfa-enabled-for-iam-console-access
- mrs-cluster-kerberos-enabled
- mrs-cluster-no-public-ip
- multi-region-cts-tracker-exists
- pca-certificate-authority-expiration-check
- pca-certificate-expiration-check
- private-nat-gateway-authorized-vpc-only
- rds-instance-enable-backup
- rds-instance-multi-az-support
- rds-instance-no-public-ip
- rds-instances-enable-kms
- root-account-mfa-enabled
- sfsturbo-encrypted-check
- stopped-ecs-date-diff

- volumes-encrypted-check
- vpc-acl-unused-check
- vpc-default-sg-closed
- vpc-flow-logs-enabled
- vpc-sg-ports-check
- vpc-sg-restricted-common-ports
- vpc-sg-restricted-ssh
- vpn-connections-active

5 Advanced Queries

5.1 Overview

Advanced Queries allows you to query your resource configuration states for one or more regions using ResourceQL.

You can directly use default advanced queries or creat custom advanced queries.

ResourceQL is a subset of structured query language (SQL) SELECT syntax to help you perform property-based queries and aggregations. The query complexity varies. You can query resources by tag or resource identifier, or by using complex SQL statements. For example, you can query an ECS with a specified OS version.

You can use Advanced Queries to:

- Manage inventory. For example, you can query ECSs with certain specifications.
- Check security compliance of your resources. For example, you can query resources for which specific configuration attributes (EIP and encrypted EVS disks) have been enabled or disabled.
- Optimize costs. For example, you can query the EVS disks that are not attached to any ECS to avoid generating unnecessary fees.

5.2 Restrictions

To use advanced queries, you must have the **rms:resources:runQuery** permissions and enable the resource recorder.

To prevent a single user from occupying resources for queries for a long time, note the following restrictions:

- If the execution duration of a query statement exceeds15 seconds, a timeout error will be returned.
- If a query generates a large amount of data and an error is returned, you need to simplify the query statement.
- Only the first 4,000 records are returned for a single query.

- A single query statement can be used to perform a maximum of two join queries for tables.
- A maximum of 200 advanced queries can be created for each account.

NOTE

You can only use advanced queries to query, view, or export cloud resources. If you need to modify or delete resources, go to related service consoles.

5.3 Creating a Query

Scenarios

You can use the query statements preset by Config or customize query statements based on resource configuration attributes to query specific cloud resource configurations.

To use advanced queries, you must have the **rms:resources:runQuery** permissions and enable the resource recorder.

Procedure

Step 1 Sign in to Config console.

Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

Step 3 In the left navigation, choose **Advanced Queries**.

Step 4 Choose the **Custom Queries** tab and click **New Query** at the upper right corner.

Step 5 In the query editor, enter the query statement as prompted.

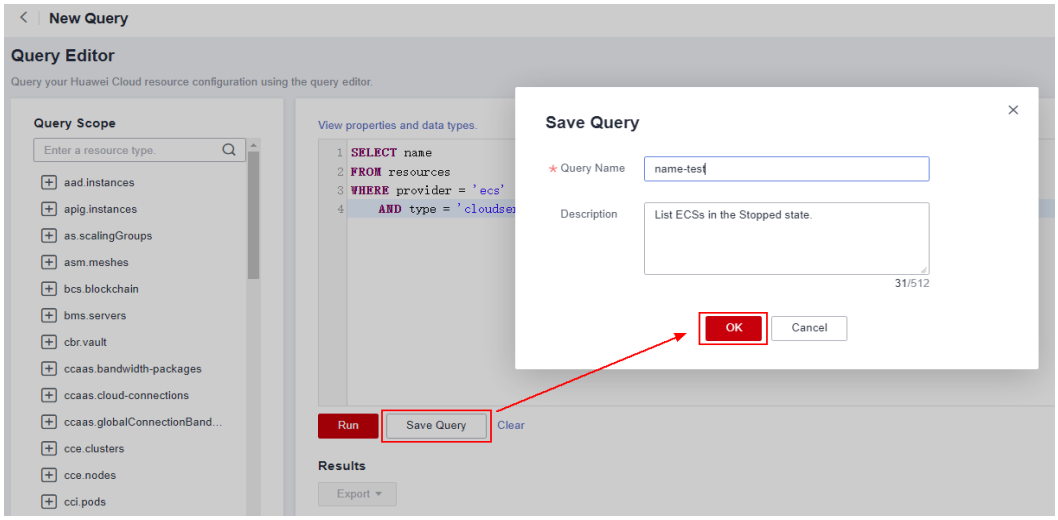
The Schema information used for advanced query is displayed on the left of the page. The properties parameter included in a request should be set to the Schema information which shows the detailed attributes of a cloud service resource. For details about the configuration example of the query statement, see **Configuration Examples of Advanced Queries**.

Step 6 Click **Save Query** and enter the query name and description.

The query name can contain only digits, letters, underscores (_), and hyphens (-).

Step 7 Click **OK**.

Figure 5-1 Save Query



NOTE

If the maximum number of custom queries has been reached, you cannot click **Save Query**. In addition, the message **The maximum number of custom queries has been reached. Delete unnecessary queries.** is displayed in the upper right corner of the page.

When the maximum number of custom queries has been reached, you can run the queries and export the query results.

Step 8 Click **Run** and then view the query results. Only the first 4000 query results can be displayed and saved.

Step 9 Click **Export** and select the format of the file to be exported (CSV or JSON).

----End

Other Operations

You can modify the name, description, and query statement of a query. After you click **Save As**, a new query is created. The following procedure uses a default query as an example to describe how to modify a query.

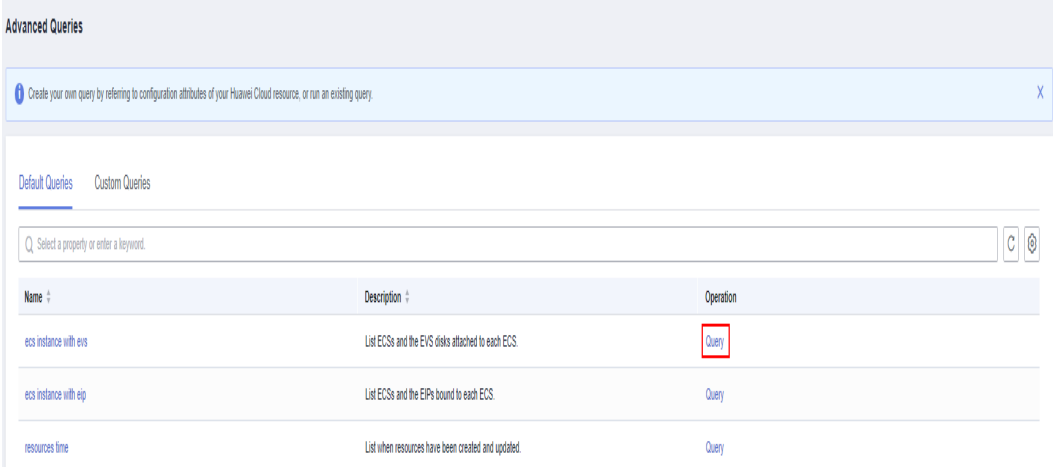
Step 1 Choose **Advanced Queries** > **Default Queries**.

All default queries are displayed in a list.

Step 2 Click **Query** in the **Operation** column for the target query.

Alternatively, click the query name and then click **Query** in the lower right corner of the query overview page.

Figure 5-2 Default queries



Step 3 In the query editor, modify the query statement as prompted.

For details, see **Configuration Examples of Advanced Queries**.

Step 4 Click **Save As** and enter the query name and description.

Step 5 In the dialog box that is displayed, click **OK**.

NOTE

New queries generated through the **Save As** operation is updated in the custom query list.

----End

Configuration Examples of Advanced Queries

Advanced queries uses ResourceQL, a subset of SQL SELECT syntax, to query resource configuration data. You do not need to call specific APIs for the query or use multiple APIs to download full data and manually analyze the data. ResourceQL can only query data from the **resources** table.

Table 5-1 Parameter descriptions in table **resources**

Parameter	Type	Description
id	String	Specifies the resource ID.
name	String	Specifies the resource name.
provider	String	Specifies the cloud service name.
type	String	Specifies the resource type.
region_id	String	Specifies the region ID.
project_id	String	Specifies the project ID.

Parameter	Type	Description
ep_id	String	Specifies the enterprise project ID.
checksum	String	Specifies the resource checksum.
created	Date	Specifies the time when the resource was created.
updated	Date	Specifies the time when the resource was updated.
provisioning_state	String	Specifies the the result of an operation on resources.
tag	Array(Map<String,String>)	Specifies the resource tag.
properties	Map<String,Object>	Specifies the resource attribute details.

Example quires are as follows:

- Example 1: List ECSs in the **Stopped** state.

```
SELECT name
FROM resources
WHERE provider = 'ecs'
    AND type = 'cloudservers'
    AND properties.status = 'SHUTOFF'
```

- Example 2: List EVS disks with certain specifications.

```
SELECT *
FROM resources
WHERE provider = 'evs'
    AND type = 'volumes'
    AND properties.size = 100
```

- Example 3: List OBS buckets queried by fuzzy search.

```
SELECT *
FROM resources
WHERE provider = 'obs'
    AND 'type' = 'buckets'
    AND name LIKE '%figure%'
```

- Example 4: List ECSs and the EVS disks attached to each ECS.

```
SELECT ECS_EVS.id AS ecs_id, EVS.id AS evs_id
FROM (
    SELECT id, evs_id
    FROM (
    SELECT id, transform(properties.ExtVolumesAttached, x -> x.id) AS evs_list
    FROM resources
    WHERE provider = 'ecs'
        AND type = 'cloudservers'
    ) ECS
       CROSS JOIN UNNEST(evs_list) AS t (evs_id)
) ECS_EVS, (
    SELECT id
    FROM resources
```



```
    WHERE provider = 'evs'
      AND type = 'volumes'
  ) EVS
WHERE ECS_EVS.evs_id = EVS.id
```

- Example 5: List ECSs and the EIPs bound to each ECS.

```
SELECT ECS.id AS ECS_id, publicIpAddress AS ip_address
FROM (
  SELECT id, transform(properties.addresses, x -> x.addr) AS ip_list
  FROM resources
  WHERE provider = 'ecs'
    AND type = 'cloudservers'
) ECS, (
    SELECT name, properties.publicIpAddress
    FROM resources
    WHERE provider = 'vpc'
      AND type = 'publicips'
      AND properties.type = 'EIP'
      AND properties.status = 'ACTIVE'
  ) EIP
WHERE CONTAINS (ECS.ip_list, EIP.name)
```

- Example 6: List resources with a quantity greater than 100 in each region.

```
WITH counts AS (
  SELECT region_id, provider, type, count(*) AS number
  FROM resources
  GROUP BY region_id, provider, type
)
SELECT *
FROM counts
WHERE number > 100
```

For details about query statements, see **ResourceQL Syntax**.

5.4 Viewing a Query

Scenarios

You can view the name, description, and SQL statement of a query.

Procedure

Step 1 Sign in to Config console.

Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

Step 3 In the left navigation, choose **Advanced Queries**.

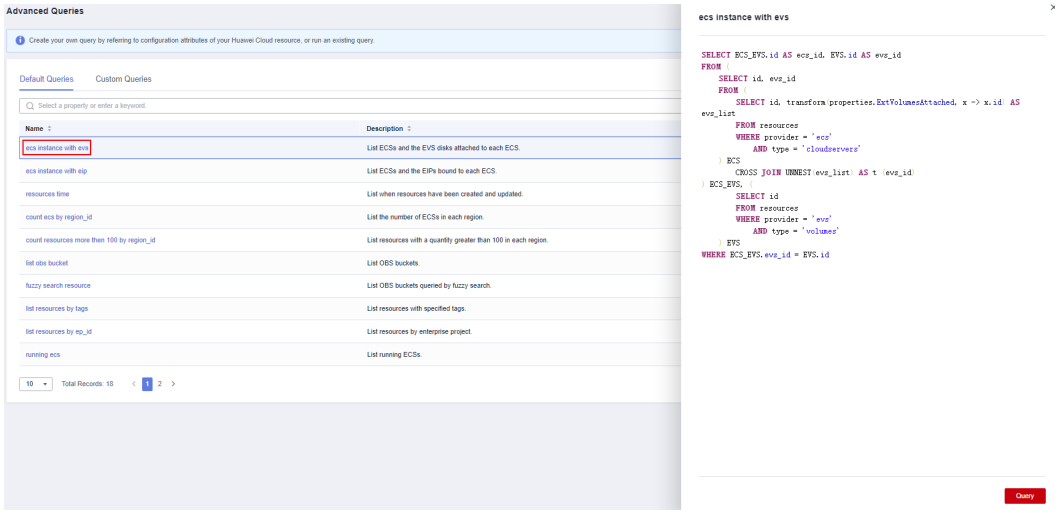
By default, the default query list is displayed. To view custom queries, click **Custom Queries**.

View the query name and description in the query list.

Step 4 Locate the query and click its name.

The SQL statement details in the query are displayed.

Figure 5-3 Query details



----End

5.5 Modifying a Query

Scenarios

You can modify the statement of a custom query if needed.

NOTE

Default queries cannot be modified.

Procedure

Step 1 Sign in to Config console.

Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

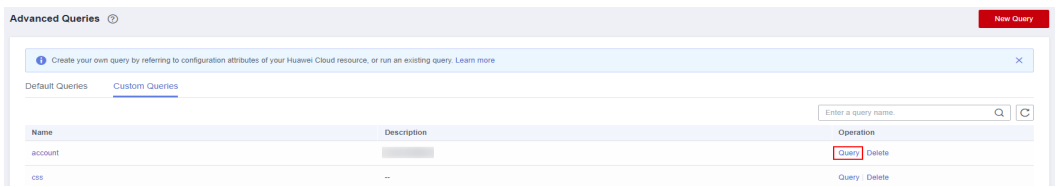
Step 3 In the left navigation, choose **Advanced Queries**.

Step 4 Click the **Custom Queries** tab.

Step 5 Locate the row that contains the query to be modified, and click **Query** in the **Operation** column.

Alternatively, click the query name to go to the query overview page, and then click **Query** in the lower right corner to go to the **Query** page.

Figure 5-4 Modifying a custom query



Step 6 In the query editor, modify the query statement as prompted.

For details, see **Configuration Examples of Advanced Queries**.

Step 7 Click **Save**.

----End

5.6 Deleting a Query

Scenarios

You can delete a custom query if you no longer need it.

Preset queries cannot be deleted.

Procedure

Step 1 Sign in to Config console.

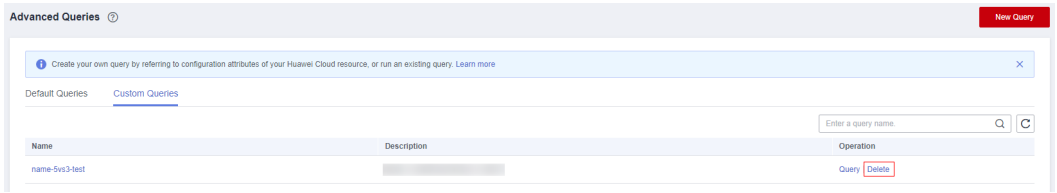
Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

Step 3 In the left navigation, choose **Advanced Queries**.

Step 4 Click **Custom Queries**.

Step 5 Locate the custom query to be deleted and click **Delete** in the **Operation** column.

Figure 5-5 Deleting a custom query



Step 6 In the dialog box that is displayed, click **OK**.

----End

6 Resource Aggregation

6.1 Overview

Functions

A resource aggregator enables you to aggregate resource configurations and compliance data from multiple accounts or an organization, so that you can centrally view or search for these resource data.

You can only view aggregated resources and their compliance data instead of modifying resource data. For example, you cannot use a resource aggregator to deploy rules or access snapshot files from a source account.

An aggregator can only record data from source accounts whose resource recorders has been enabled.

- If the resource recorder in a source account has not been enabled, resource data from this source account will not be aggregated.
- If you have configured a monitoring scope when enabling the resource recorder, only the resources within the specified scope are aggregated.
- If you enable the resource recorder and then disable it after a period of time, an aggregator only aggregate resource data during the period when the resource recorder is enabled.

Setting Up An Aggregator

To collect resource data from source accounts, perform the following operations:

1. Create an aggregator. For more details, see **Creating a Resource Aggregator**.
2. Enable the resource recorder from every source account. For more details, see **Configuring the Resource Recorder**.
3. Authorize the aggregator account to collect resource configurations and compliance data from source accounts. For more details, see **Authorizing an Aggregator Account**.
4. View resource configurations and compliance data from source accounts. For more details, see **Viewing Aggregated Rules** and **Viewing Aggregated Resources**.

Basic Concepts

Source Account

A source account is an account from which Config aggregates resource configurations and compliance data. A source account can be a Huawei Cloud account or an organization.

Aggregator

An aggregator is a kind of Config resource allowing you to collect resource configuration and compliance data from multiple resource accounts.

Aggregator Account

An aggregator account is an account used to create an aggregator.

Authorization

Authorization refers to the permissions that an aggregator account needs to obtain from a source account to collect resource configuration and compliance data from the source account. Authorization is not required for an organization specific aggregator.

6.2 Restrictions

To create a resource aggregator, you must have the **rms:aggregators:create** permissions.

- Up to 30 account specific aggregators can be created in an account.
- An aggregator can aggregate data from up to 30 source accounts.
- An account specific aggregator can add, update, and delete up to 1,000 source accounts within 7 days.
- Up to 1 organization specific aggregator can be created in an account.
- You cannot create organization aggregators multiple times a day. For example, if you create and then delete an organization aggregator on the same day, creating another organization aggregator on the same day is not support.
- Resource changes from source accounts will be synchronized to the aggregator where source account data is collected.
- The Organizations service is in open beta test (OBT). To use organization sepcific aggregators, apply for OBT.

NOTE

You can only use aggregators to query or view resource data from source accounts. If you need to modify or delete resources, go to related service consoles.

6.3 Creating a Resource Aggregator

Scenarios

You can create an account specific or organization specific aggregator.

To aggregate resource data from a source account to an aggregator account, authorization from the source account is required. For details, see **Authorizing a Resource Aggregator Account**.

Procedure

Step 1 Sign in to the Config console.

Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

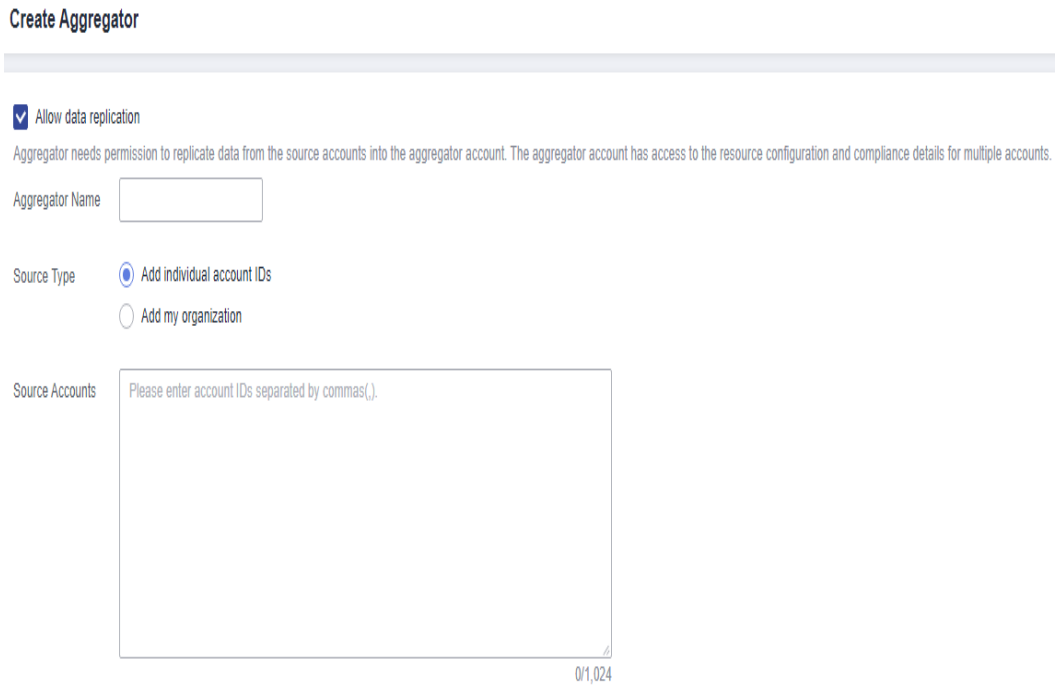
Step 3 In the left navigation, choose **Resource Aggregation** > **Aggregators**.

Step 4 In the upper right corner, click **Create Aggregator**.

Step 5 On the **Create Aggregator** page, select **Allow data replication** and configure the aggregator name and source accounts.

If you select **Add individual account IDs** for **Source Type**, enter Huawei Cloud account IDs and separate them with commas (,). If you select **Add my organization**, the resource aggregator aggregates data of all member accounts in the organization.

Figure 6-1 Create Aggregator



NOTE

- An account specific aggregator can only aggregate resource data from the Huawei Cloud accounts. For details about how to obtain account IDs, see **Obtaining Account ID**.
- If you need to create an organization aggregator, you must use an organization management account or a delegated administrator account of Config and the Organizations service must be enabled. For details, see **Specifying, Viewing, or Removing a Delegated Administrator**. If an organization management account is used to create organization aggregators, Config will enable the integration with Organizations by using the **enableTrustedService** API. If a delegated administrator account of Config is used, Config will call the **DelegatedAdministrators** API to check whether the account used is valid.

Step 6 Click **OK**.

----End

6.4 Viewing Resource Aggregators

Scenarios

You can view and search for all created resource aggregators and their details in the resource aggregator list.

Procedure

Step 1 Sign in to the Config console.

Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

Step 3 In the left navigation, choose **Resource Aggregation** > **Aggregators**.

Step 4 On the **Aggregators** page, view all resource aggregators created.

You can use the filter in the upper right corner of the list to search for the resource aggregator you want to view. Exact search by complete aggregator name is supported.

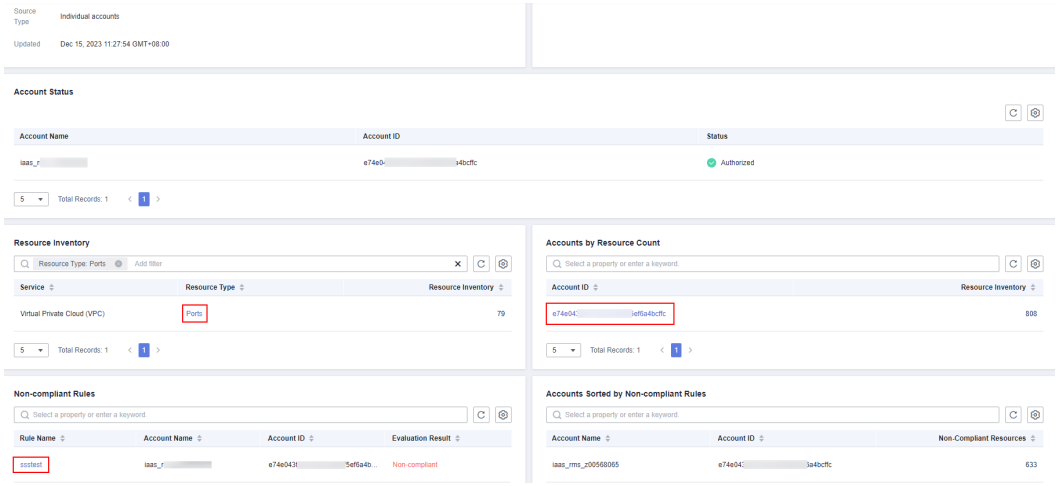
Step 5 Locate the aggregator you want to view and click its name.

Click a target resource type in the **Resource Inventory** area to view all aggregated resources of this resource type.

Click a target account ID in the **Accounts by Resource Count** area to view all aggregated resources from this account.

On the details page, click a rule name in the **Rule That Have Found Non-compliant** area.

Figure 6-2 Resource aggregator details page



----End

6.5 Editing an Aggregator

Scenarios

You can follow the following procedure to modify source accounts in an aggregator.

You cannot edit organization aggregators.

Procedure

Step 1 Sign in to the Config console.

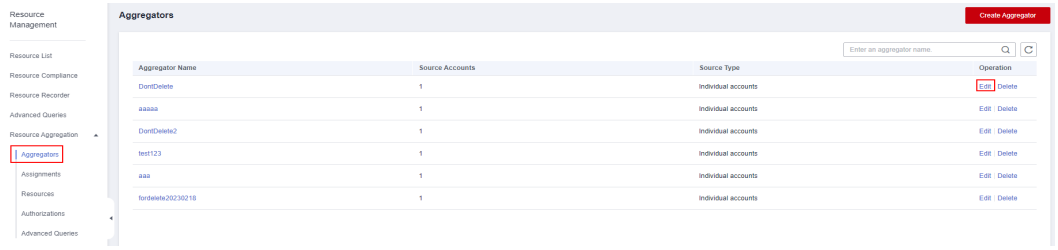
Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

Step 3 In the left navigation, choose **Resource Aggregation** > **Aggregators**.

Step 4 Locate the aggregator to be edited and click **Edit** in the **Operation** column.

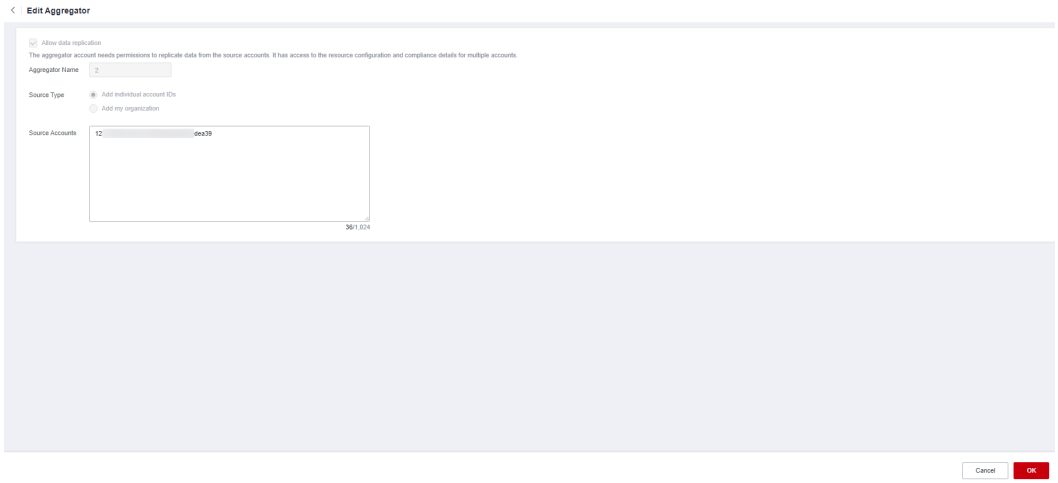
Alternatively, in the upper right corner of the resource aggregator details page, click **Edit** to go to the **Edit Aggregator** page.

Figure 6-3 Editing a resource aggregator



Step 5 On the **Edit Aggregator** page, change IDs for **Source Accounts**.

Figure 6-4 Modifying source accounts



Step 6 Click **OK**.

----End

6.6 Deleting a Resource Aggregator

Scenarios

If a resource aggregator is no longer used, you can delete it.

Procedure

Step 1 Sign in to the Config console.

Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

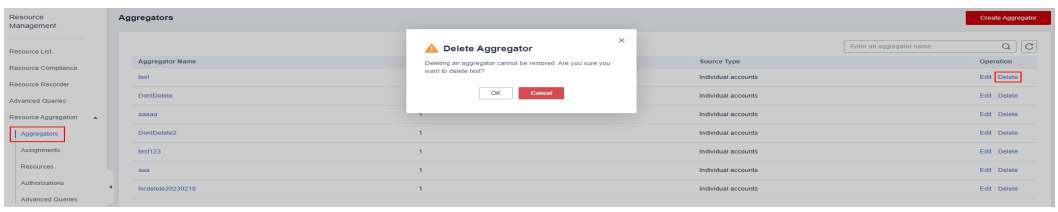
Step 3 In the left navigation, choose **Resource Aggregation** > **Aggregators**.

Step 4 In the resource aggregator list, locate the aggregator to be deleted and click **Delete** in the **Operation** column.

Alternatively, in the upper right corner of the resource aggregator details page, click **delete**.

Step 5 In the displayed dialog box, click **OK**.

Figure 6-5 Delete Aggregator



----End

6.7 Viewing Aggregated Rules

Scenarios

You can view and filter all compliance data aggregated by an aggregator. For example, you can filter rules by rule name, evaluation result, and account ID.

Procedure

Step 1 Sign in to the Config console.

Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

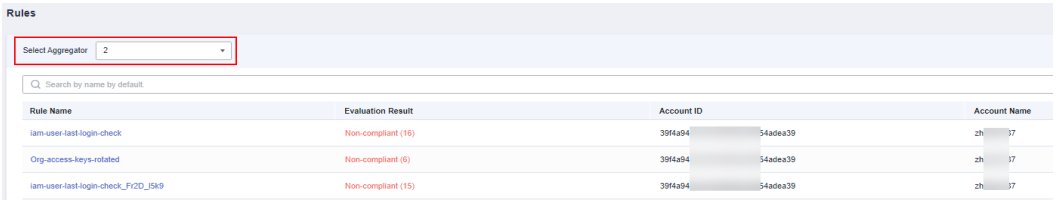
Step 3 On the left navigation, choose **Resource Aggregation** > **Rules**.

Step 4 In the upper right corner, select an aggregator from the drop-down list to view compliance data aggregated by this aggregator.

In the rule list, click a target rule name to view rule details.

In the search box above the list, enter a rule name, evaluation result, or account ID to filter compliance data.

Figure 6-6 Viewing aggregated rules



----End

6.8 Viewing Aggregated Resources

Scenarios

You can view all resources aggregated by an aggregator. You can filter resource data by aggregator, resource name, account ID, and resource type. You can also view details of each resource.

Procedure

Step 1 Sign in to the Config console.

Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

Step 3 In the navigation pane, choose **Resource Aggregation** > **Resources**.

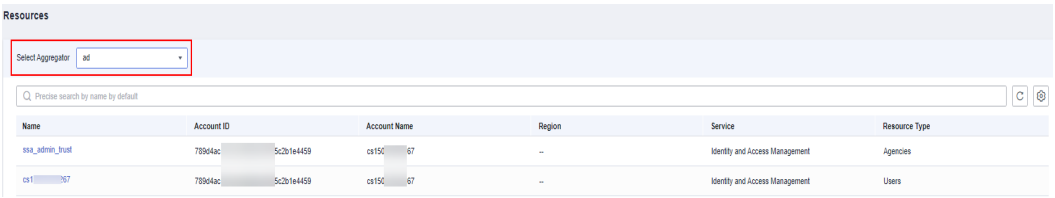
Step 4 In the upper left corner, select an aggregator.

All resources aggregated by the aggregator are displayed in a list.

In the search box above the list, enter a resource name, an account ID, or a resource type to filter resource data.

In the resource list, click a target resource name to view resource details.

Figure 6-7 Viewing aggregated resources



----End

6.9 Authorizing an Aggregator Account

Scenarios

Before an aggregator account initiates aggregation requests, source accounts must grant this account the permissions to collect resource configurations and compliance data. There are no requirements on the order of adding authorization and creating an aggregator.

An organization specific aggregator can collect resource data of all member accounts in an organization without source account authorization.

Helpful links:

- **Adding Authorization**
- **Accepting an Authorization**
- **Deleting an Authorization**

Adding an Authorization

You can use the **Add Authorization** function to authorize an aggregator account.

Step 1 Sign in to the Config console.

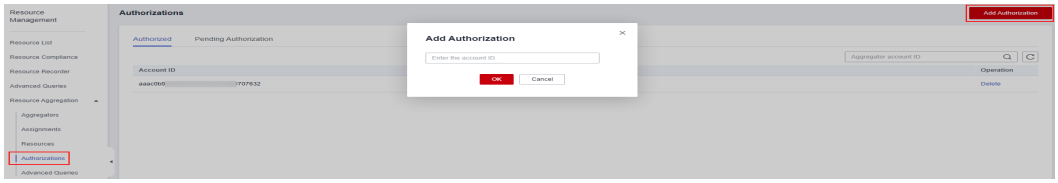
Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

Step 3 In the left navigation, choose **Resource Aggregation** > **Authorizations**.

Step 4 Click **Add Authorization** in the upper right corner of the page.

Step 5 In the **Add Authorization** dialog box, enter the ID of the aggregator account which you want to authorize.

Figure 6-8 Adding an authorization



Step 6 Click **OK**.

After the authorization is complete, the authorization record is displayed in the **Authorized** list.

----End

Accepting an Authorization

You can approve a pending authorization request to authorize an aggregator account.

Step 1 Sign in to the Config console.

Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

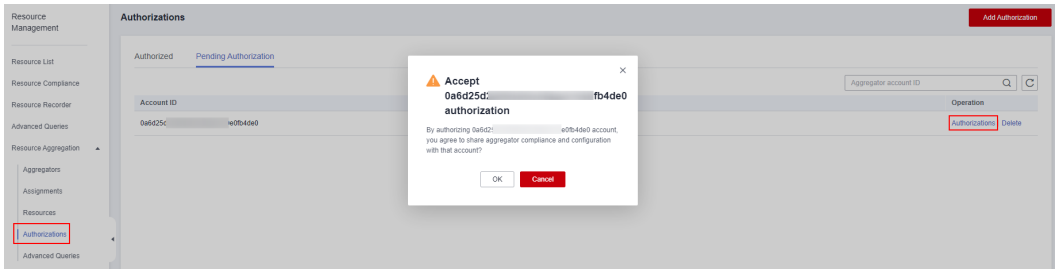
Step 3 In the left navigation, choose **Resource Aggregation** > **Authorizations**.

Step 4 Click the **Pending Authorization** tab, locate the account ID that sends an authorization request to be processed in the list, and click **Authorize** in the **Operation** column.

Step 5 In the displayed dialog box, click **OK**.

After the authorization request is accepted, the authorization record is displayed in the **Authorized** list.

Figure 6-9 Accepting an authorization



----End

Deleting an Authorization

You can revoke authorization from an aggregator account.

Step 1 Sign in to the Config console.

Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

Step 3 In the left navigation, choose **Resource Aggregation** > **Authorizations**.

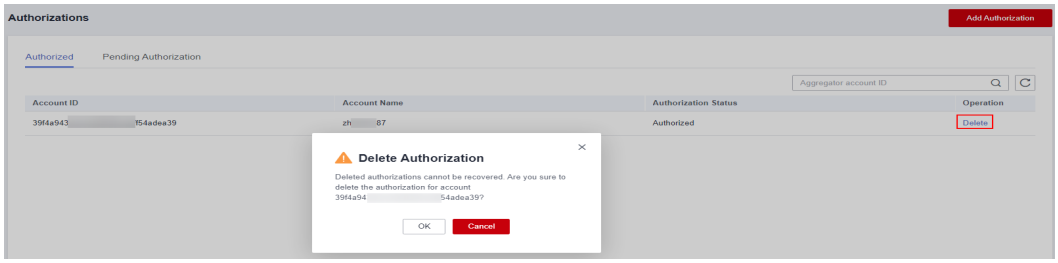
Step 4 Locate the authorization to be deleted in the list, and click **Delete** in the **Operation** column.

Step 5 In the displayed dialog box, click **OK**.

The authorization record is moved to the **Pending Authorization** tab, and the authorization status changes to **Pending authorization**.

To authorize the aggregator account again, you can click **Authorize** in the **Operation** column in the **Pending Authorization** list.

Figure 6-10 Deleting an authorization



Step 6 In the **Pending Authorization** list, locate the authorization, and click **Delete** in the **Operation** column. In the displayed dialog box, click **OK** to delete the authorization record completely.

NOTE

You can authorize an aggregator account again after revoking the authorization from this account.

----End

6.10 Advanced Queries

Overview

Resource aggregation supports advanced queries. You can use ResourceQL to query configuration states of one or multiple aggregator account.

You can create custom queries using **Query Editor**.

You can use the query statements preset by Config or customize query statements based on resource configuration attributes to query specific cloud resource configurations.

ResourceQL is a subset of structured query language (SQL) SELECT syntax to help you perform property-based queries and aggregations. The query complexity varies. You can query resources by tag or resource identifier, or by using complex SQL statements. For example, you can query an ECS with a specified OS version.

Limitations

To use advanced queries, you must have the **rms:aggregatorResources:runQuery** permission and enable the resource recorder.

To prevent a single user from occupying resources for queries for a long time, note the following restrictions:

- If the execution duration of a query statement exceeds15 seconds, a timeout error will be returned.
- If a query generates a large amount of data and an error is returned, you need to simplify the query statement.
- Only the first 4,000 records are returned for a single query.
- A single query statement can be used to perform a maximum of two join queries for tables.
- A maximum of 200 advanced queries can be created for each account.

NOTE

You can only use advanced queries to query, view, or export cloud resources. If you need to modify or delete resources, go to related service consoles.

Creating a Query

Step 1 Log in to the management console.

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

Step 3 In the left navigation, choose **Resource Aggregation** > **Advanced Queries**.

Step 4 Choose the **Custom Queries** tab and click **New Query** in the upper right corner.

Step 5 On the **Query Range** area on the right, select the aggregator whose resource configuration needs to be queried. In the text box below, enter the query statement.

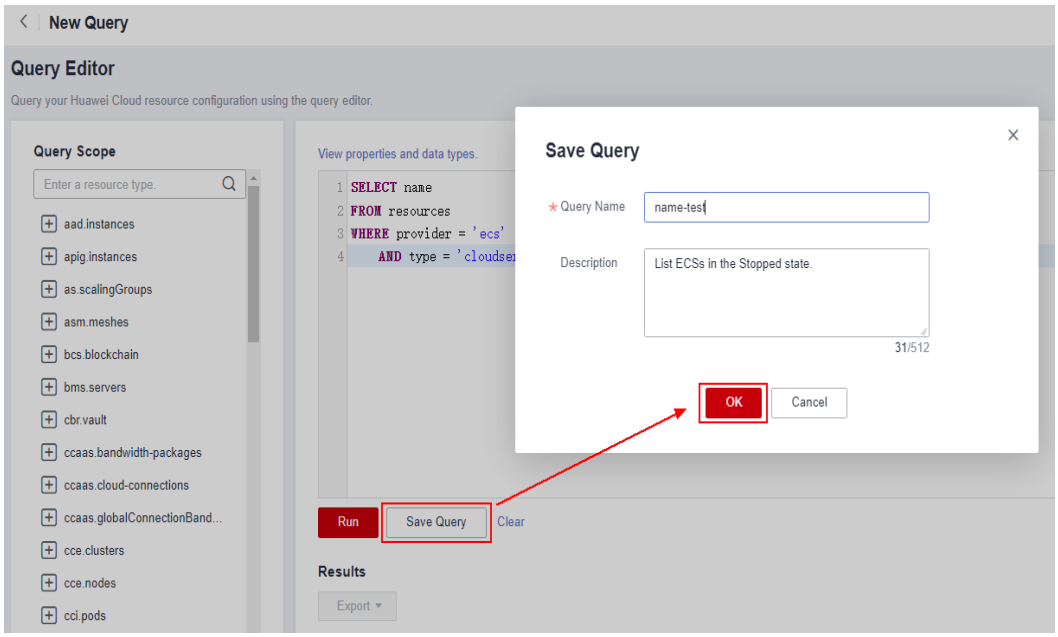
The Schema information used for advanced query is displayed on the left of the page. The properties parameter included in a request should be set to the Schema information which shows the detailed attributes of a cloud service resource. For details about the configuration example of the query statement, see **Configuration Examples of Advanced Queries**.

Step 6 Click **Save Query** and enter the query name and description.

The query name can contain only digits, letters, underscores (_), and hyphens (-).

Step 7 Click **OK**.

Figure 6-11 Save Query



NOTE

If the number of customized queries reaches the upper limit, you cannot click **Save Query**. In addition, the message "**The number of customized queries has reached the upper limit. Please delete unnecessary queries.**" is displayed.

When the maximum number of custom queries has been reached, you can run the queries and export the query results.

Step 8 Click **Run** and then view the query results. Only the first 4000 query results can be displayed and saved.

Step 9 Click **Export** and select the format of the file to be exported (CSV or JSON).

----End

Other Operations

- You can modify the name, description, and query statement of a default query or an existing custom query. After you click **Save As**, a new query is generated. For details, see **Other Operations**.
- To view the name, description, and query statements of a query, see **Viewing a Query**.
- To modify the query statement of a custom query, see **Modifying a Query**.
- To delete a custom query, see **Deleting a Query**. Default queries cannot be deleted.

NOTE

To run an advanced query for an aggregator, you must specify this aggregator first.

Configuration Examples of Advanced Queries

ResourceQL uses a subset of the SQL SELECT syntax to query how your Huawei Cloud resources are configured and how they are related to one another. You do

not need to call specific APIs for the query or use multiple APIs to download full data and manually analyze the data. ResourceQL can only query data from the **aggregator_resources** table.

Table 6-1 aggregator_resources

Parameter	Type	Description
domain_id	String	Account ID
id	String	Resource ID
name	String	Resource name.
provider	String	Cloud service name
type	String	Resource type
region_id	String	Region ID
project_id	String	Project ID
ep_id	String	Enterprise project ID
checksum	String	Resource checksum
created	Date	The time when the resource was created
updated	Date	The time when the resource was updated
provisioning_state	String	The result of an operation on resources.
tag	Array(Map<String,String>)	Resource tag
properties	Map<String,Object>	Resource attributes

Example quires are as follows:

- Example 1: Querying the names of stopped ECSs in a resource aggregator

```
SELECT domainId, name
FROM aggregator_resources
WHERE provider = 'ecs'
    AND type = 'cloudservers'
    AND properties.status = 'SHUTOFF'
```

- Example 2: Querying EVS disks of specified specifications in a resource aggregator

```
SELECT *
FROM aggregator_resources
WHERE provider = 'evs'
    AND type = 'volumes'
    AND properties.size = 100
```

- Example 3: Fuzzily querying OBS buckets in the resource aggregator

```
SELECT *
FROM aggregator_resources
```



```
WHERE provider = 'obs'
   AND 'type' = 'buckets'
   AND name LIKE '%figure%'
```

- Example 4: Querying the types of resources whose count is greater than 100 under each source account

```
WITH counts AS (
    SELECT region_id, provider, type, count(*) AS number
    FROM aggregator_resources
    GROUP BY domain_id, provider, type
)
SELECT *
FROM counts
WHERE number > 100
```

For details about query statements, see **ResourceQL Syntax**.

7 Cloud Trace Service

7.1 Supported CTS Operations

Scenarios

Cloud Trace Service (CTS) records operations on Config for your later query, audit, and backtrack.

Prerequisites

You have enabled CTS.

Key Operations Recorded by CTS

Table 7-1 Config operations recorded by CTS

Operation	Resource Type	Event Name
Adding a rule	policy	createPolicyAssignments
Deleting a rule	policy	deletePolicyAssignment
Modifying a rule	policy	updatePolicyAssignment
Triggering a resource evaluation	policy	runEvaluation
Disabling a rule	policy	disablePolicyAssignment
Enabling a rule	policy	enablePolicyAssignment
Creating or modifying resource recorder configuration	trackerConfig	createOrUpdateTracker-Config
Deleting the resource recorder configuration	trackerConfig	deleteTrackerConfig

Operation	Resource Type	Event Name
Creating an advanced query	storedQuery	createStoredQuery
Updating an advanced query	storedQuery	updateStoredQuery
Deleting an advanced query	storedQuery	deleteStoredQuery
Updating a compliance evaluation result	policyState	updatePolicyState
Creating or updating an organization rule	organizationPolicyAssignments	createOrganizationPolicyAssignment
Deleting an organization rule	organizationPolicyAssignments	deleteOrganizationPolicyAssignment
Creating authorization	authorization	createAggregationAuthorization
Deleting authorization	authorization	deleteAggregationAuthorization
Creating an aggregator	aggregator	createConfigurationAggregator
Deleting an aggregator	aggregator	deleteConfigurationAggregator
Updating an aggregator	aggregator	updateConfigurationAggregator
Deleting a pending authorization request	aggregationRequests	deletePendingAggregationRequest
Creating a conformance package	conformancePacks	createConformancePack
Deleting a conformance package	conformancePacks	deleteConformancePack

7.2 Querying Real-Time Traces

Scenarios

After you enable CTS and the management tracker is created, CTS starts recording operations on cloud resources. After a data tracker is created, the system starts recording operations on data in OBS buckets. CTS stores operation records generated in the last seven days.

This section describes how to query and export operation records of the last seven days on the CTS console.

- **Viewing Real-Time Traces in the Trace List of the New Edition**
- **Viewing Real-Time Traces in the Trace List of the Old Edition**

Constraints

- Traces of a single account can be viewed on the CTS console. Multi-account traces can be viewed only on the **Trace List** page of each account, or in the OBS bucket or the **CTS/system** log stream configured for the management tracker with the organization function enabled.
- You can only query operation records of the last seven days on the CTS console. To store operation records for more than seven days, you must configure an OBS bucket to transfer records to it. Otherwise, you cannot query the operation records generated seven days ago.
- After performing operations on the cloud, you can query management traces on the CTS console 1 minute later and query data traces on the CTS console 5 minutes later.

Viewing Real-Time Traces in the Trace List of the New Edition

1. Log in to the management console.
2. Click  in the upper left corner and choose **Management & Governance** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. On the **Trace List** page, use advanced search to query traces. You can combine one or more filters.
   - **Trace Name**: Enter a trace name.
   - **Trace ID**: Enter a trace ID.
   - **Resource Name**: Enter a resource name. If the cloud resource involved in the trace does not have a resource name or the corresponding API operation does not involve the resource name parameter, leave this field empty.
   - **Resource ID**: Enter a resource ID. Leave this field empty if the resource has no resource ID or if resource creation failed.
   - **Trace Source**: Select a cloud service name from the drop-down list.
   - **Resource Type**: Select a resource type from the drop-down list.
   - **Operator**: Select one or more operators from the drop-down list.
   - **Trace Status**: Select **normal**, **warning**, or **incident**.
     - **normal**: The operation succeeded.
     - **warning**: The operation failed.
     - **incident**: The operation caused a fault that is more serious than the operation failure, for example, causing other faults.
   - Time range: Select **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range.
5. On the **Trace List** page, you can also export and refresh the trace list, and customize the list display settings.

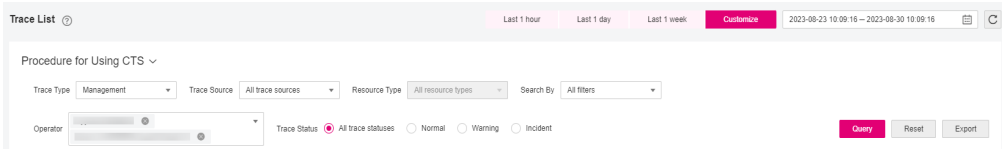
- Enter any keyword in the search box and click to filter desired traces.
- Click **Export** to export all traces in the query result as an .xlsx file. The file can contain up to 5000 records.
- Click to view the latest information about traces.
- Click to customize the information to be displayed in the trace list. If **Auto wrapping** is enabled ( ), excess text will move down to the next line; otherwise, the text will be truncated. By default, this function is disabled.

6. For details about key fields in the trace structure, see **Trace Structure** and **Example Traces**.
7. (Optional) On the **Trace List** page of the new edition, click **Go to Old Edition** in the upper right corner to switch to the **Trace List** page of the old edition.

Viewing Real-Time Traces in the Trace List of the Old Edition

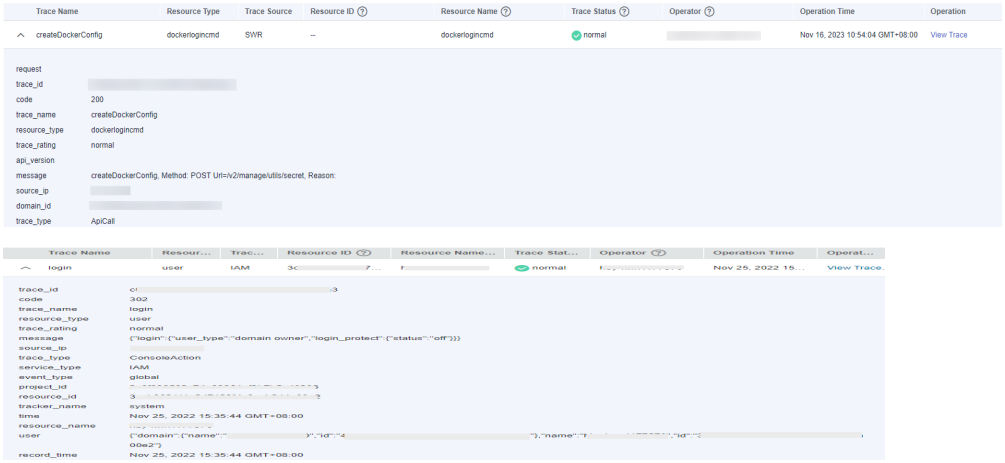
1. Log in to the management console.
2. Click in the upper left corner and choose **Management & GovernanceManagement & Deployment** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. Each time you log in to the CTS console, the new edition is displayed by default. Click **Go to Old Edition** in the upper right corner to switch to the trace list of the old edition.
5. Set filters to search for your desired traces, as shown in **Figure 7-1**. The following filters are available:

Figure 7-1 Filters

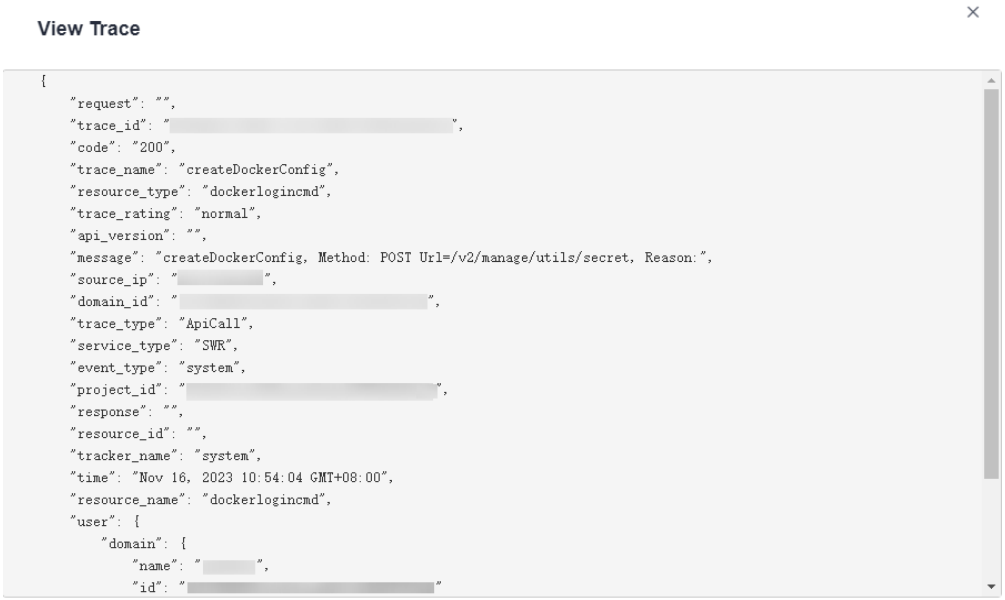


- **Trace Type**, **Trace Source**, **Resource Type**, and **Search By**: Select a filter from the drop-down list.
  - If you select **Resource ID** for **Search By**, specify a resource ID.
  - If you select **Trace name** for **Search By**, specify a trace name.
  - If you select **Resource name** for **Search By**, specify a resource name.
- **Operator**: Select a user.
- **Trace Status**: Select **All trace statuses**, **Normal**, **Warning**, or **Incident**.
- Time range: You can query traces generated during any time range in the last seven days.
- Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5000 records.

6. Click **Query**.
7. On the **Trace List** page, you can also export and refresh the trace list.
   - Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5000 records.
   - Click to view the latest information about traces.
8. Click on the left of a trace to expand its details.



9. Click **View Trace** in the **Operation** column. The trace details are displayed.



10. For details about key fields in the trace structure, see **Trace Structure**section "Trace References" > "Trace Structure" and **Example Traces**section "Trace References" > "Example Traces".
11. (Optional) On the **Trace List** page of the old edition, click **New Edition** in the upper right corner to switch to the **Trace List** page of the new edition.

8 Appendix

8.1 Supported Services and Regions

For services and regions supported by Config, see **Supported Services and Regions**.

8.2 Relationships with Supported Resources

Table 8-1 Relationships with supported resources

Service	Resource Type	Relationship	Related Service	Related Resource Type
ECS	Cloud server	isContainedIn	VPC	VPC
			MRS	MRS
		isAttachedTo	VPC	Elastic IP
			EVS	Volume
		isAssociatedWith	VPC	Security group
			IMS	Image
BMS	Cloud server	isContainedIn	VPC	VPC
		isAttachedTo	EVS	Volume
		isAssociatedWith	VPC	Security group
			IMS	Image

Service	Resource Type	Relationship	Related Service	Related Resource Type
HECS	Hyper Elastic Cloud Server (HECS)	isContainedIn	VPC	VPC
		contains	VPC	Elastic IP
		isAttachedTo	EVS	volumes
		isAssociatedWith	VPC	Security group
			IMS	Image
AS	AS group	isContainedIn	VPC	VPC
		isAssociatedWith	VPC	Security group
DCS	Memcached instance	isContainedIn	VPC	VPC
		isAssociatedWith	VPC	Security group
	Node	isContainedIn	DCS	Redis instance
	Redis instance	isContainedIn	VPC	VPC
		contains	DCS	Node
		isAssociatedWith	VPC	Security group
ELB	Load balancer	contains	ELB	Listener
		isAttachedTo	VPC	Elastic IP
			ELB	Server group
			ELB	Server group
	Listener	Is contained in	ELB	Load balancer
		Is attached to	ELB	Server group
			ELB	Server group
	Server group	Contains	ELB	Server
		Is attached to	ELB	Load balancer

Service	Resource Type	Relationship	Related Service	Related Resource Type
			ELB	Listener
	Server group	Contains	ELB	Server
		Is attached to	ELB	Load balancer
			ELB	Listener
	Server	Is contained in	ELB	Server group
			ELB	Server group
VPC	VPC	contains	ECS	Cloud server
			BMS	Cloud server
			HECS	HECS
			AS	AS group
			DCS	Memcached instance
			DCS	Redis instance
			MRS	MRS
	Security group	isAssociatedWith	ECS	Cloud server
			BMS	Cloud server
			HECS	HECS
			AS	AS group
			DCS	Memcached instance
			MRS	mrs
			DCS	Redis instance
	Bandwidth	contains	VPC	publicips
	Elastic IP	isContainedIn	VPC	Bandwidth

Service	Resource Type	Relationship	Related Service	Related Resource Type
		isAttachedTo	ECS	Cloud server
			ELB	Load balancer
			MRS	MRS
			NAT Gateway	Public NAT gateway
EVS	Volume	isAttachedTo	ECS	Cloud server
			BMS	Cloud server
			HECS	HECS
IMS	Image	isAssociatedWith	ECS	Cloud server
			BMS	Cloud server
			HECS	HECS
NAT Gateway	Public NAT gateway	isAttachedTo	VPC	Elastic IP
GaussDB NoSQL	Instance	contains	GaussDB NoSQL	Node
	Node	isContainedIn	GaussDB NoSQL	Instance
GaussDB	Instance	contains	GaussDB	Node
	Node	isContainedIn	GaussDB	Instance
MRS	MRS	isContainedIn	VPC	VPC
		isAttachedTo	VPC	Elastic IP
		isAssociatedWith	VPC	Security group
		contains	ECS	Cloud server
CCE	Cluster	contains	CCE	Node
	Node	isContainedIn	CCE	Cluster

Service	Resource Type	Relationship	Related Service	Related Resource Type
Enterprise Router	Connection	isContainedIn	Enterprise Router	Instance
	Instance	contains	Enterprise Router	Connection
IAM	User group	contains	IAM	User
	User	isContainedIn	IAM	User group
RDS	Instance	contains	RDS	Node
	Node	isContainedIn	RDS	Instance
Config	Conformance package	Contains	Config	Rule
	Rule	Is contained in	Config	Conformance package

8.3 Message Notification Models

Config uses SMN to send notifications of:

- Resource changes (creation, modification, and deletion)
- Resource relationship changes
- Resource change notification storage completed
- Resource snapshot storage completed

Notification Model of Resource Changes

Table 8-2 Parameter description

Parameter	Type	Description
notification_type	String	Specifies the message notification type.
notification_creation_time	String	Specifies the time when the message was sent. The time is a UTC time in a fixed format complying with ISO-8601 (for example, **2018-11-14T08:59:14Z**).
domain_id	String	Account ID
detail	Object	Specifies the message details.

Table 8-3 detail parameters

Parameter	Type	Description
resource_id	String	Specifies the resource ID.
resource_type	String	Specifies the resource type.
event_type	Enum	Specifies the event type. The value can be **CREATE**, **UPDATE**, or **DELETE**.
capture_time	String	Specifies the time when the event was captured. The time is a UTC time in a fixed format complying with ISO-8601 (for example, **2018-11-14T08:59:14Z**).
resource	Object	Specifies the resource details.

Table 8-4 resource parameters

Parameter	Type	Description
id	String	Specifies the resource ID.
name	String	Specifies the resource name.
provider	String	Specifies the cloud service name.
type	String	Specifies the cloud resource type.
region_id	String	Specifies the ID of the region where the resource is located.
project_id	String	Specifies the IAM project ID.
project_name	String	Specifies the IAM project name.
ep_id	String	Specifies the enterprise project ID.
ep_name	String	Specifies the enterprise project name.
checksum	String	Specifies the checksum.
created	String	Specifies the time when the cloud resource was created. The time is a UTC time in a fixed format complying with ISO-8601 (for example, **2018-11-14T08:59:14Z**).

Parameter	Type	Description
updated	String	Specifies the last time when the cloud resource was updated. The time is a UTC time in a fixed format complying with ISO-8601 (for example, **2018-11-14T08:59:14Z**).
provisioning_state	String	Specifies the status of the operation that causes the resource change.
tags	Map	Specifies the cloud resource tag.
properties	Map	Specifies the cloud resource attribute.

Notification Example of Resource Changes


```
{
  "detail": {
    "resource": {
      "id": "3e62c0e6-e779-469e-b0f2-35743f6229d1",
      "name": "ecs-51c8",
      "provider": "evs",
      "type": "volumes",
      "checksum": "b3bcc019cecbb701e324e0dcf2f283236685885236b49f5ba5ea2f5f788170a1",
      "created": "2020-08-12T07:14:41.638Z",
      "updated": "2020-08-12T07:14:44.423Z",
      "tags": {},
      "properties": {
        "shareable": false,
        "volumeType": "SATA",
        "metadata": {},
        "attachments": [],
        "replicationStatus": "disabled",
        "availabilityZone": "regionid1a",
        "bootable": "true",
        "userId": "059b5c937d80d3e41ff3c00a3c883d16",
        "volTenantAttrTenantId": "059b5e0a2500d5552fa1c00adada8c06",
        "size": "40",
        "encrypted": false,
        "volumeImageMetadata": {
          "virtualEnvType": "FusionCompute",
          "isregistered": "true",
          "imageSourceType": "uds",
          "minDisk": "40",
          "platform": "CentOS",
          "size": 0,
          "osVersion": "CentOS 7.5 64bit",
          "minRam": "0",
          "name": "CentOS 7.5 64bit",
          "checksum": "d41d8cd98f00b204e9800998ecf8427e",
          "osBit": "64",
          "osType": "Linux",
          "containerFormat": "bare",
          "supportXen": "true",
          "id": "e0adce3a-a4d2-4207-9018-69ce64b4426a",
          "supportKvm": "true",
          "diskFormat": "zvhd2",
          "imageType": "gold"
        },
```



```
      "links": [
        {
          "rel": "self",
          "href": "https://evs.regionid1.xxxxxx.com/v2/059b5e0a2500d5552fa1c00adada8c06/os-vendor-volumes/3e62c0e6-e779-469e-b0f2-35743f6229d1"
        },
        {
          "rel": "bookmark",
          "href": "https://evs."regionid1.xxxxxx.com/059b5e0a2500d5552fa1c00adada8c06/os-vendor-volumes/3e62c0e6-e779-469e-b0f2-35743f6229d1"
        }
      ],
      "volHostAttrHost": ""regionid1a-pod01."regionid1#0",
      "multiattach": false,
      "status": "available"
    },
    "region_id": ""regionid1",
    "project_id": "059b5e0a2500d5552fa1c00adada8c06",
    "project_name": ""regionid1",
    "ep_id": "0",
    "ep_name": "default",
    "provisioning_state": "Succeeded"
  },
  "resource_id": "3e62c0e6-e779-469e-b0f2-35743f6229d1",
  "resource_type": "evs.volumes",
  "event_type": "CREATE",
  "capture_time": "2020-08-12T07:15:15.116Z"
 },
 "notification_type": "ResourceChanged",
 "notification_creation_time": "2020-08-12T07:14:47.192Z",
 "domain_id": "059b5c937100d3e40ff0c00a7675a0a0"
}
```


Notification Model of Resource Relationship Changes

Table 8-5 Parameter description

Parameter	Type	Description
notification_type	String	Specifies the message notification type.
notification_creation_time	String	Specifies the time when the message was sent. The time is a UTC time in a fixed format complying with ISO-8601 (for example, **2018-11-14T08:59:14Z**).
domain_id	String	Account ID
detail	Object	Specifies the message details.

Table 8-6 detail parameters

Parameter	Type	Description
resource_id	String	Specifies the resource ID.

Parameter	Type	Description
resource_type	String	Specifies the resource type.
event_type	Enum	Specifies the event type (**CHANGE**).
capture_time	String	Specifies the time when the event was captured. The time is a UTC time in a fixed format complying with ISO-8601 (for example, **2018-11-14T08:59:14Z**).

Notification Example of Resource Relationship Changes

```
{
  "detail": {
    "resource_id": "f65b06d1-d63b-438a-93cc-bdd55b304f0a",
    "resource_type": "ecs.cloudservers",
    "event_type": "CHANGE",
    "capture_time": "2020-08-12T07:15:14.257Z"
  },
  "notification_type": "ResourceRelationChanged",
  "notification_creation_time": "2020-08-12T07:14:56.296Z",
  "domain_id": "059b5c937100d3e40ff0c00a7675a0a0"
}
```

Notification Model of Resource Snapshot Storage Completed

Table 8-7 Parameter description

Parameter	Type	Description
notification_type	String	Specifies the message notification type.
notification_creation_time	String	Specifies the time when the message was sent. The time is a UTC time in a fixed format complying with ISO-8601 (for example, **2018-11-14T08:59:14Z**).
domain_id	String	Specifies the tenant ID.
detail	Object	Specifies the message details.

Table 8-8 detail parameters

Parameter	Type	Description
snapshot_id	String	Specifies the resource snapshot ID.
region_id	String	Specifies the ID of the region where the resource snapshot is located.
bucket_name	String	Specifies the name of the OBS bucket where the resource snapshot is stored.
object_keys	Array of String	Specifies the resource snapshot path list.

Notification Example of Resource Snapshot Storage Completed

```
{
  "detail": {
    "snapshot_id": "474f85e6-72cd-442b-af4e-517120a5c669",
    "region_id": ""regionid1",
    "bucket_name": "test",
    "object_keys": [
      "RMSLogs/059b5c937100d3e40ff0c00a7675a0a0/Snapshot/
2020/8/11/059b5c937100d3e40ff0c00a7675a0a0_Snapshot_"regionid1_ResourceSnapshot_2020-08-10T170901_474f85e6-72cd-442b-af4e-517120a5c669_part-1.json.gz"
    ]
  },
  "notification_type": "SnapshotArchiveCompleted",
  "notification_creation_time": "2020-08-10T17:09:27.314Z",
  "domain_id": "059b5c937100d3e40ff0c00a7675a0a0"
}
```

Notification Model of Resource Change Notification Storage Completed

Table 8-9 Parameter description

Parameter	Type	Description
notification_type	String	Specifies the message notification type.
notification_creation_time	String	Specifies the time when the message was sent. The time is a UTC time in a fixed format complying with ISO-8601 (for example, **2018-11-14T08:59:14Z**).
domain_id	String	Account ID
detail	Object	Specifies the message details.

Table 8-10 detail parameters

Parameter	Type	Description
region_id	String	Specifies the ID of the region where the resource snapshot is located.
bucket_name	String	Specifies the name of the OBS bucket where the resource snapshot is stored.
object_key	String	Specifies the resource snapshot path.

Notification Example of Resource Change Notification Storage Completed

```
{
    "detail": {
        "region_id": ""regionid1",
        "bucket_name": "test",
        "object_key": "RMSLogs/059b5c937100d3e40ff0c00a7675a0a0/Notification/2020/12/10/
NotificationChunk/
059b5c937100d3e40ff0c00a7675a0a0_Notification_"regionid2_NotificationChunk_VPC_VPCS_2020-12-10T02
4612Z_2020-12-10T050621Z.json.gz"
    },
    "notification_type": "NotificationArchiveCompleted",
    "notification_creation_time": "2020-12-10T05:09:28.002Z",
    "domain_id": "059b5c937100d3e40ff0c00a7675a0a0"
}
```

8.4 Resource Storage Models

Table 8-11 Parameter description

Parameter	Type	Description
snapshot_id	String	Specifies the resource snapshot ID.
items	Array of Object	Specifies the list of the resource snapshot items.
snapshot_time	String	Specifies the time when the resource snapshot was stored. **snapshot_time** is a UTC time in a fixed format complying with ISO-8601 (for example, **2018-11-14T08:59:14Z**).

Table 8-12 Resource snapshot items

Parameter	Type	Description
resource	Object	Specifies the resource.
relations	Array of Object	Specifies the item list of the resource relationship.

Table 8-13 resource parameters

Parameter	Type	Description
id	String	Specifies the resource ID.
name	String	Specifies the resource name.
provider	String	Specifies the cloud service name.
type	String	Specifies the cloud resource type.
region_id	String	Specifies the ID of the region where the resource is located.
project_id	String	Specifies the IAM project ID.
project_name	String	Specifies the IAM project name.
ep_id	String	Specifies the enterprise project ID.
ep_name	String	Specifies the enterprise project name.
checksum	String	Specifies the checksum.
created	String	Specifies the time when the cloud resource was created. **created** is a UTC time in a fixed format complying with ISO-8601 (for example, **2018-11-14T08:59:14Z**).
updated	String	Specifies the last time when the cloud resource was updated. **updated** is a UTC time in a fixed format complying with ISO-8601 (for example, **2018-11-14T08:59:14Z**).

Parameter	Type	Description
provisioning_state	String	Specifies the result of an operation on resources. The value can be: • Succeeded: The operation is successful. • Failed: The operation fails. • Canceled: The operation is canceled. • Processing: The operation is in progress.
tags	Map	Specifies the cloud resource tag.
properties	Map	Specifies the cloud resource attribute.

Table 8-14 Resource relationship items

Parameter	Type	Description
from_resource_id	String	Specifies the ID of the source resource.
to_resource_id	String	Specifies the ID of the associated resource.
from_resource_type	String	Specifies the type of the source resource.
to_resource_type	String	Specifies the type of the associated resource.
relation_type	String	Specifies the resource relationship type.

Resource Storage Example


```
{
  "items": [
    {
      "resource": {
        "id": "c25ee8b3-c907-4cd4-9869-6c4b07c61a0b",
        "name": "rse-cdk-07-cdk-3sbz",
        "provider": "vpc",
        "type": "securityGroups",
        "region_id": ""regionid1",
        "project_id": "fc6d40abe7e54492b7c7aa5a29d6cbab",
        "project_name": "demo_project",
        "ep_id": "0",
        "ep_name": "default",
        "checksum": "4098715092c762b3eafe25be8eeda33a10b547033f9d59b6e18f5a960a1f805d",
        "updated": "2020-05-25T10:27:17.000Z",
```



```
      "created": "2020-05-25T10:27:17.000Z",
      "provisioning_state": "Succeeded",
      "tags": {},
      "properties": {}
    },
    "relations": [
      {
        "from_resource_id": "c25ee8b3-c907-4cd4-9869-6c4b07c61a0b",
        "to_resource_id": "0088a276-162b-4f07-aa40-f6ed8b801ca1",
        "from_resource_type": "vpc.securityGroups",
        "to_resource_type": "ecs.cloudservers",
        "relation_type": "isAssociatedWith"
      }
    ]
  }
 ],
 "snapshot_id": "6e40483d-5499-4440-a369-284e528f3d85",
 "snapshot_time": "2020-06-30T06:56:00.018Z"
}
```


8.5 Models of Resource Change Notification Storage

Table 8-15 Parameter description

Parameter	Type	Description
notification_items	Array of Object	Specifies the list of resource change notifications.

Notification Model of Resource Changes

Table 8-16 Parameter description

Parameter	Type	Description
notification_type	String	Specifies the message notification type.
notification_creation_time	String	Specifies the time when the message was sent. The time is a UTC time in a fixed format complying with ISO-8601 (for example, **2018-11-14T08:59:14Z**).
domain_id	String	Account ID
detail	Object	Specifies the message details.

Table 8-17 detail parameters

Parameter	Type	Description
resource_id	String	Specifies the resource ID.
resource_type	String	Specifies the resource type.
event_type	Enum	Specifies the event type. The value can be **CREATE**, **UPDATE**, or **DELETE**.
capture_time	String	Specifies the time when the event was captured. The time is a UTC time in a fixed format complying with ISO-8601 (for example, **2018-11-14T08:59:14Z**).
resource	Object	Specifies the resource details.

Table 8-18 resource parameters

Parameter	Type	Description
id	String	Specifies the resource ID.
name	String	Specifies the resource name.
provider	String	Specifies the cloud service name.
type	String	Specifies the cloud resource type.
region_id	String	Specifies the ID of the region where the resource is located.
project_id	String	Specifies the IAM project ID.
project_name	String	Specifies the IAM project name.
ep_id	String	Specifies the enterprise project ID.
ep_name	String	Specifies the enterprise project name.
checksum	String	Specifies the checksum.
created	String	Specifies the time when the cloud resource was created. The time is a UTC time in a fixed format complying with ISO-8601 (for example, **2018-11-14T08:59:14Z**).

Parameter	Type	Description
updated	String	Specifies the last time when the cloud resource was updated. The time is a UTC time in a fixed format complying with ISO-8601 (for example, **2018-11-14T08:59:14Z**).
provisioning_state	String	Specifies the status of the operation that causes the resource change.
tags	Map	Specifies the cloud resource tag.
properties	Map	Specifies the cloud resource attribute.

Example of Resource Change Notification Storage

```
{
   "notification_items": [
      {
         "detail": {
            "resource": {
               "id": "ea05ef41-8bd6-4a9c-af39-244e1ec448eb",
               "name": "as-group-test",
               "provider": "as",
               "type": "scalingGroups",
               "checksum": "",
               "region_id": ""regionid1",
               "project_id": "068d54ceca00d5302f70c00aaf6a471c",
               "project_name": "test",
               "ep_id": "0",
               "ep_name": "default"
            },
            "resource_id": "ea05ef41-8bd6-4a9c-af39-244e1ec448eb",
            "resource_type": "as.scalingGroups",
            "event_type": "DELETE",
            "capture_time": "2020-12-08T09:30:27.158Z"
         },
         "notification_type": "ResourceChanged",
         "notification_creation_time": "2020-12-08T09:30:27.272Z",
         "domain_id": "059b5c937100d3e40ff0c00a7675a0a0"
      }
   ]
}
```

8.6 DSL Syntax

DSL consists of a logical operator shown as shown below. A Boolean value is returned.

```
{
  <logical operator>: <condition> | [<condition>, ..., <condition>]
}
```


8.6.1 Logical Operators

Supported logical operators are:

- "not": <condition>
- "allOf": [<condition>, ..., <condition>]
- "anyOf": [<condition>, ..., <condition>]

not inverts the result of the condition.

allOf evaluates true only if all included conditions are true, and evaluates false as long as one included condition is false.

anyOf evaluates true as long as one included condition is true, and evaluates false if all included conditions are false.

allOf and **anyOf** both implement short-circuit evaluation. They evaluate the conditions in the subsequent list in sequence.

If the return result of a condition is false, **allOf** returns false and the subsequent conditions are not calculated.

If the return result of a condition is true, **anyOf** returns true and the subsequent conditions are not calculated.

8.6.2 Conditions

A condition can be a single judgment statement or a nested logical operator.

The judgment statement is used to determine whether a specific value meets a specific requirement. It returns a Boolean value and its format is as follows:

```
{
  "value": "...",
  "comparator": "...",
  "pattern": "..."
}
```

NOTE

- **value** can be a constant or an expression. Its value type depends on the selected comparison operator. Example: **true**, **1**, **"hello"**, or **"$ {resource().properties.metadata}"**
- **comparator**: specifies the comparison operator.
- **pattern** can be a constant or an expression.

The following comparators are supported:

- **equals** compares whether **value** is equal to **pattern**. **value** can be a string, an integer, or a Boolean, so is **pattern**.
- **notEquals**: Its result is opposite to the **equals** result.
- **equalsIgnoreCase** compares whether **value** is equal to **pattern** in case-insensitive mode. **value** must be a string, so is **pattern**.
- **like** performs fuzzy match of **value** and **pattern**. You can add an asterisk (*) to **pattern** to match zero or multiple random characters, or add a question mark (?) to **pattern** to match any random character. **value** must be a string, so is **pattern**.

- **notLike**: Its result is opposite to the **like** result.
- **likeIgnoreCase** performs fuzzy match of **value** and **pattern** in case-insensitive mode. **value** must be a string, so is **pattern**.
- **contains** determines whether **pattern** is a substring of **value**. **value** must be a string, so is **pattern**.
- **notContains**: Its result is opposite to the **contains** result.
- **in** determines whether **value** is in **pattern**. **Pattern** must be an array. **value** can be a string or an integer.
- **notIn**: Its result is opposite to the **in** result.
- **containsKey** determines whether **value** contains the key-value pattern. **value** must be an object. **pattern** must be a string.
- **notContainsKey**: Its result is opposite to the **containsKey** result.
- **less** determines whether **value** is smaller than **pattern**. **value** can be a string or an integer, so is **pattern**.
- **lessOrEquals** determines whether **value** is smaller than or equal to **pattern**. **value** can be a string or an integer, so is **pattern**.
- **greater** determines whether **value** is greater than **pattern**. **value** can be a string or an integer, so is **pattern**.
- **greaterOrEquals** determines whether **value** is greater than or equal to **pattern**. **value** can be a string or an integer, so is **pattern**.

The following is an example of nested logical operators in a condition:

```
{
  "not": {
    "anyOf": [
      {
        "value": "${resource().properties.metadata}",
        "comparator": "notContainsKey",
        "pattern": "systemEncrypted"
      },
      {
        "value": "${resource().properties.metadata.systemEncrypted}",
        "comparator": "equals",
        "pattern": "0"
      }
    ]
  }
}
```

8.6.3 Expressions

value and **pattern** can be a constant or an expression. An expression is contained in ${}. You can use the following functions in the expression.

Table 8-19 String functions

Function	Parameter	Returned Value	Description
base64()	string	string	Encodes a specific string using Base64.
base64ToString()	string	string	Decodes a Base64-encoded string.

Function	Parameter	Returned Value	Description
concat()	string, string	string	Concatenates two strings.
contains()	string, string	bool	Determines whether parameter 2 is a substring of parameter 1.
empty()	string	bool	Determines whether a string is left blank.
endsWith()	string, string	bool	Determines whether parameter 1 ends with parameter 2.
indexOf()	string, string	int	Returns the position of parameter 2 when it appears for the first time in parameter 1. If parameter 2 does not appear, -1 is returned.
lastIndexOf()	string, string	int	Returns the position of parameter 2 when it appears for the last time in parameter 1. If parameter 2 does not appear, -1 is returned.
length()	string	int	Returns the length of a string.
replace()	string, string, string	string	Replaces parameter 2 in parameter 1 with parameter 3.
startsWith()	string, string	bool	Determines whether parameter 1 starts with parameter 2.
toLower()	string	string	Converts all letters in a string into lowercase letters.
toUpper()	string	string	Converts all letters in a string into uppercase letters.
equals()	string, string	bool	Checks whether two strings are the same.
greater()	string, string	bool	Determines whether parameter 1 is greater than parameter 2.
greaterOrEquals()	string, string	bool	Determines whether parameter 1 is greater than or equal to parameter 2.
less()	string, string	bool	Determines whether parameter 1 is smaller than parameter 2.
lessOrEquals()	string, string	bool	Determines whether parameter 1 is no more than parameter 2.

Function	Parameter	Returned Value	Description
split()	string, string	array	Returns the result of separating parameter 1 by parameter 2.
substring()	string, int, int	string	Obtains the substring of parameter 1. The start position of the substring is determined by parameter 2 and the length is determined by parameter 3.

Table 8-20 Numeric functions

Function	Parameter	Returned Value	Description
add()	int, int	int	Adds two integers.
max()	int, int	int	Uses the greater of the two integers.
min()	int, int	int	Uses the smaller of the two integers.
sub()	int, int	int	Calculates the result of parameter 1 minus parameter 2.
equals()	int, int	bool	Determines whether two integers are the same.
greater()	int, int	bool	Determines whether parameter 1 is greater than parameter 2.
greaterOrEquals()	int, int	bool	Determines whether parameter 1 is greater than or equal to parameter 2.
less()	int, int	bool	Determines whether parameter 1 is smaller than parameter 2.
lessOrEquals()	int, int	bool	Determines whether parameter 1 is no more than parameter 2.

Table 8-21 Array functions

Function	Parameter	Returned Value	Description
concat()	array, array	array	Concatenates two arrays.
contains()	array, any	bool	Determines whether parameter 2 is in array parameter 1.
empty()	array	bool	Determines whether the array is left blank.
first()	array	any	Returns the first element in the array.
last()	array	any	Returns the last element in the array.
length()	array	int	Returns the number of elements in the array.

Table 8-22 Object functions

Function	Parameter	Returned Value	Description
contains()	object, string	bool	Determines whether parameter 1 contains key-value parameter 2.
getValue()	object, string	any	Obtains the value corresponding to the key-value parameter 2 in parameter 1.
empty()	object	bool	Determines whether the object is left blank.

Function	Parameter	Returned Value	Description
length()	object	int	Returns the number of key-value pairs in the object.

Table 8-23 Logical functions

Function	Parameter	Returned Value	Description
if()	bool, any, any	any	Determines whether parameter 1 is true. If yes, parameter 2 is returned. If no, parameter 3 is returned.
and()	bool, bool	bool	Determines whether both parameter 1 and parameter 2 are true.
or()	bool, bool	bool	Determines whether at least one of parameter 1 and parameter 2 is true.
not()	bool	bool	Inverts the input Boolean value.

Table 8-24 Functions related to resource compliance

Function	Parameter	Returned Value	Description
resource()	None	object	Returns the structure of the current evaluated resource.
parameters()	string	any	Returns a parameter defined in the **parameters** section.

In addition to use function computing in expressions, you can use:

- a dot (.) to access a field in an object, for example, **resource().properties.metadata.systemEncrypted**.
- **CASE WHEN** statement


```
CASE WHEN condition1 THEN value1
    WHEN condition2 THEN value2
    ...
    ELSE defaultValue END
```

8.7 ResourceQL Syntax

8.7.1 Overview

ResourceQL provides SQL-like functions, allowing you to flexibly query your cloud resources.

```
SELECT name, created, updated FROM resources WHERE region_id = 'regionid1'
```

The statement is case insensitive. SELECT COUNT(*) and select CoUnT(*) are the same. Use single quotation marks to represent the literal of a string.

The following are data types supported by ResourceQL. For the array type, [] is used to index a position, and the number starts from 1.

Table 8-25 Supported data types

Type Name	Type
Integer	Int/Integer
Float	Float/Double
Boolean	Boolean
Array	Array
String	String
Dictionary	Object
Timestamp	Date

All your cloud resources are included in a table. The table name is fixed to **resources**. The resources under your aggregator account forms a table. The table name is fixed to **aggregator_resources**. Each row in the table records a piece of data. The conventions of each column are as follows.

Table 8-26 Parameter descriptions in table **resources**

Parameter	Type	Description
id	String	Specifies the resource ID.
name	String	Specifies the resource name.
provider	String	Specifies the cloud service name.

Parameter	Type	Description
type	String	Specifies the resource type.
region_id	String	Specifies the region ID.
project_id	String	Specifies the project ID.
ep_id	String	Specifies the enterprise project ID.
checksum	String	Specifies the resource checksum.
created	Date	Specifies the time when the resource was created.
updated	Date	Specifies the time when the resource was updated.
provisioning_state	String	Specifies the result of an operation on resources.
tag	Array(Map<String,String>)	Specifies the resource tag.
properties	Map<String,Object>	Specifies the resource attribute details.

aggregator_resources contains **domain_id** that indicates the account ID. The type of a domain ID is a string.

Different types of resources can be distinguished by **provider** and **type**, and the structures of their **properties** field are different. For example, **cloudservers** of an ECS has **properties** that contains 23 fields, and a VPC has **properties** that contains only three fields.

For details about the field types supported by the properties parameter, see **Creating a Query**. The field types supported by the properties parameter are also specified on the console when you create a new query.

For a specific resource type, you can use commas (.), a nesting method, to query the specific fields in **properties**. For example, if **properties** of an ECS contains the **status** and **addresses** fields, you can run the following statement to query the running ECS and its address:

```
SELECT name, created, updated, properties.addresses FROM resources
    WHERE provider = 'ecs' AND type = 'cloudservers' AND properties.status = 'ACTIVE'
```


8.7.2 Syntax

Symbol Conventions

In this section, the words that need to be typed in the original form are capitalized, and the characters that need to be typed in the original form are enclosed in single quotation marks (').

'[x]' indicates that statement 'x' can be used once or not even once.

'(x)' indicates that statement 'x' is a whole. '(x, ...)' indicates that statement 'x' can be used once or multiple times. If statement 'x' is used multiple times, use commas (,) to separate them.

'|' indicates all possible alternatives.

'expression' indicates any expression. Specially, 'bool_expression' indicates any Boolean expression.

'identifier' indicates a valid identifier. An identifier can contain letters, digits, and underscores (_), and cannot start with a digit.

'column_name' indicates a valid field name. It can be 'identifier' or multiple identifiers, for example,'A.id'.

'table_name' indicates a valid table name. In the ResourceQL syntax, 'table_name' must be 'resources'.

A unit enclosed in double quotation marks ("") is considered as a whole. For example, to indicate a column name containing special characters, add double quotation marks ("") before and after the column name.

Basic Query Syntax

```
[WITH (with_item, ...)]
SELECT [DISTINCT | ALL] (select_item, ...)
[FROM (from_item, ...)]
[WHERE bool_expression]
[GROUP BY [DISTINCT | ALL] (expression, ...)]
[HAVING booleanExpression]
[ORDER BY (expression [ASC | DESC] [NULLS (FIRST | LAST)], ...)]
[LIMIT number]
```

The field in 'select_item' can be renamed. Operation can be performed on the field values. 'select_item' supports the query of all fields in a table.

```
select_item = (expression [[AS] column_name_aias]) | *
```

'from_item' supports the join function and multiple subqueries, and the table name can be renamed.

```
from_item = table_name [[AS] table_name_aias]
        | (from_item join_type from_item [(ON bool_expression) | USING(column_name, ...)])
        | '(' query ')'
```

'with_item' is used to customize queries to facilitate subsequent invoking.

```
with_item = identifier AS '(' query ')'
```

For example, to list resources with a quantity greater than 100 in each region, run the following SQL statement:


```
WITH counts AS (
   SELECT region_id, provider, type, count(*) AS number FROM resources
   GROUP BY region_id, provider, type
) SELECT * FROM counts WHERE number > 100
```

Numeric Operation and Boolean Operation

ResourceQL supports binary mathematical operations on integers and floating digits. The following operators are supported: '+,-,*,/,%'

Values of the same type can be compared. The following comparison operators are supported: <, >, <=, >=, =, <>, !=. Both <> and != indicate not equal. Values are compared in size, and strings are compared in lexicographic order. Values and sets can also be compared. In this case, one from 'ALL | SOME | ANY' on the right of the comparison operator is used to specify the comparison range. 'All' indicates that all elements in the set must be met. 'SOME/ANY' indicates that at least one element must be met.

```
expression ('=' | '<>' | '!=' | '<' | '>' | '<=' | '>=')
expression
expression ('=' | '<>' | '!=' | '<' | '>' | '<=' | '>=')
[ALL | SOME | ANY] '(' query ')'
```

'bool_expression' indicates any Boolean expression. (**True** or **False** is returned after the operation.) 'bool_expression' includes the following syntax:

```
NOT bool_expression
bool_expression (AND | OR) bool_expression
expression [NOT] BETWEEN expression AND expression
expression [NOT] IN '(' query ')'
EXISTS '(' query ')'
expression [NOT] LIKE pattern [ESCAPE escape_characters]
expression IS [NOT] NULL
expression IS [NOT] DISTINCT FROM expression
```

In particular, operator '||' concatenates the left and right values and returns a new value. The left and right values are of the same type: array or string.

Timestamp

ResourceQL allows you to query fields of the time type. The query result is converted to the zero time zone and returned in ISO Date format. The result is saved in milliseconds.

Time types can be connected by comparison operators. If you want to use a literal to indicate time, use timestamps to write 'time'. 'time' can be in any ISO date format or a common time format. The following formats are allowed:

2019-06-17T12:55:42.233Z

2019-06-17T12:55:42Z

2019-06-17 12:55:42

2019-06-17T12:55:42.00 + 08:00

2019-06-17 05:55:40 - 06:00

2019-06-17

2019

If the time zone is not added, the zero time zone is used by default. If the 24-hour time is not added, 0:00 is used by default. If the month is not added, January 1 is used by default.

For example, to sort resources created since 12:55:00 on September 12, 2020 by update time in descending order, run the following statement:

```
select name, created, updated from resources
where created >= timestamp '2020-09-12T12:55:00Z'
order by updated DESC
```

Fuzzy Search

```
string LIKE pattern [ESCAPE escape_characters]
```

'LIKE' is used to determine whether a character string complies with a pattern. If you want to express the literal of '%' and '_' in the pattern, you can specify an escape character (for example, '#') after ESCAPE and write '# %' and '#_' in the pattern.

Wildcard '%' indicates that zero or multiple characters are matched.

Wildcard '_' indicates that one character is matched.

The fuzzy query of OBS buckets can be written in the following format:

```
SELECT name, id FROM resources
   WHERE provider = 'obs' AND type = 'buckets' AND name LIKE '%figure%'
```

or

```
SELECT name, id FROM resources
   WHERE provider = 'obs' AND type = 'buckets' AND name LIKE '%figure#_%' ESCAPE '#'
```

Condition Functions

The return value of CASE varies according to the actual situation. CASE can be used in either of the following ways:

- Calculate the value of a given expression and return the corresponding result based on the value.
- Calculate the value of each bool_expression in sequence, finds the first expression that meets the requirements, and returns the result.

```
CASE expression
   WHEN value1 THEN result1
   [WHEN value2 THEN result2]
   [...]
   [ELSE result]
END
CASE
   WHEN condition1 THEN result1
   WHEN condition2 THEN result2
   [...]
   [ELSE result]
END
```

IF can be used in either of the following ways:

- 'IF(bool_expression, value)': If the bool_expression value is true, 'value' is returned. Otherwise, NULL is returned.
- 'IF(bool_expression, value1, value2)': If the Boolean expression value is true, 'value1' is returned. Otherwise, 'value2' is returned.

Using Functions to Simplify Queries

ResourceQL provides a variety of functions to simplify queries. For details about the functions, see **Functions**.

ResourceQL supports lambda expressions. The arguments of some functions may be another function. In this case, it is convenient to use the lambda expression.

For example, to list the ECSs and the EVS disks attached to each ECS, run the following SQL statement:

```
SELECT ECS.id AS ecs_id, EVS.id AS evs_id FROM
   (SELECT id, transform(properties.ExtVolumesAttached, x -> x.id) AS evs_list
   FROM resources WHERE provider = 'ecs' AND type = 'cloudservers') ECS
   (SELECT id FROM resources WHERE provider = 'evs' AND type = 'volumes') EVS
   WHERE contains(ecs.evs_list, evs.id)
```

'contains(a, element) → boolean' determines whether an element appears in array a.

'transform(array(T), function(T, S)) → array(S) can convert an array of a certain type into an array of another type.

Join and Unnest

ResourceQL supports 'JOIN' and 'UNNEST'. 'JOIN' can be classified into the following types:

- [INNER] JOIN
- LEFT [OUTER] JOIN
- RIGHT [OUTER] JOIN
- FULL [OUTER] JOIN

'JOIN' must be followed by 'USING(...)' or 'ON <bool_expression>'.

'USING' is used to specify the names of columns to join.

'ON' accepts a Boolean expression and merges values of 'JOIN' if the Boolean expression value is true. To ensure performance, there must be at least one equation in a Boolean expression in the conjunctive normal form (CNF), and the operation content at the left and right ends of the equation is provided by the left and right tables separately.

You can add 'NATURAL' before 'JOIN' to indicate a connection. In this case, you do not need to add 'USING' or 'ON' after 'JOIN'.

'UNNEST' can unpack an array into a table. With 'WITH ORDINALITY', there is an auto-increment column. The format is as follows:

```
table_name CROSS JOIN UNNEST '(' (expression, ...) ')' [WITH ORDINALITY]
```

Note that 'CROSS JOIN' can only be used to connect to 'UNNEST'. ResourceQL does not support 'CROSS JOIN' in other formats.

The preceding example of querying the association between an ECS and an EVS disk can also be written in the following format:

```
SELECT ECS_EVS.id AS ecs_id, EVS.id AS evs_id FROM
   (SELECT id, evs_id FROM (SELECT id, transform(properties.ExtVolumesAttached, x ->x.id) AS evs_list
      FROM resources WHERE provider = 'ecs' AND type = 'cloudservers') ECS
```



```
CROSS JOIN UNNEST(evs_list) AS t (evs_id)) ECS_EVS,
(SELECT id FROM resources WHERE provider = 'evs' AND type = 'volumes') EVS
WHERE ECS_EVS.evs_id = EVS.id
```

8.7.3 Functions

ResourceQL supports the following functions.

Table 8-27 Mathematical operation functions

Function	Description
abs(x)	Returns the absolute value of x.
ceil/ceiling(x)	Returns *x* rounded up to the nearest integer.
floor(x)	Returns *x* rounded down to the nearest integer.
pow/power(x, p) → double	Returns *x* raised to the power of *p*.
round(x)	Returns *x* rounded to the nearest integer.
round(x, d)	Returns *x* rounded to *d* decimal places.
sign(x)	Returns the sign of *x*. • **1** if the argument is greater than 0 • **-1** if the argument is less than 0

Table 8-28 String functions

Function	Description
concat(str1, str2, ..., strn) → string	Returns the concatenation of *str1*, *str2*, ..., *strN*.
chr(n) → string	Returns the Unicode code point *n* as a single character string.
codepoint(str) → int	Returns the Unicode code point of the only character of *str*.
length(str) → int	Returns the length of *str* in characters.
lower/upper(str) → string	Converts *str* to lowercase or uppercase.
replace(str, sub) → string	Removes all substrings from strings.
replace(str, sub, replace) → string	Replaces all instances of *sub* with *replace* in *str*.
reverse(str) → string	Returns *str* with the characters in reverse order.

Function	Description
split(str, delimiter) → array	Splits *str* on *delimiter* and returns an array.
strpos(str, sub) → int	Returns the starting position of the first instance of *sub* in *str*. Positions start with **1**. If not found, **0** is returned.
strpos(str, sub, n) -> int	Returns the position of the N-th instance of *sub* in *str*. Positions start with **1**. If not found, **0** is returned.
strrpos(str, sub) → int	Returns the starting position of the last instance of *sub* in *str*. Positions start with **1**. If not found, **0** is returned.
strrpos(str, sub, n) -> int	Returns the position of the N-th instance of *sub* in *str* starting from the end of the string. Positions start with **1**. If not found, **0** is returned.
substr(str, start) → string	Returns the rest of *str* from the starting position *start*.
substr(str, start, length) → string	Returns a substring with a length from the start index.
trim/lstrim/rstrim(str)	Removes leading and trailing whitespace from a string.

Table 8-29 Array functions

Function	Description
all_match(array(T), function(T, boolean)) → boolean	Returns whether all elements of an array match the given predicate.
any_match(array(T), function(T, boolean)) → boolean	Returns whether any elements of an array match the given predicate.
array_average(a) → double	Returns the average of all non-null elements of *a*.
array_distinct(a) → array	Removes duplicate values from array *a*.
array_duplicates(a) → array	Returns a set of elements that occur more than once in array *a*.
array_frequency(a) → map	Returns a map: keys are the unique elements in *array*, values are how many times the key appears.

Function	Description
array_has_duplicates(a) → boolean	Returns a boolean: whether *a* has any elements that occur more than once.
array_intersect(a, b) → array	Returns an array of the elements in the intersection of *a* and *b*, without duplicates.
array_join(x, delimiter) → string	Concatenates the elements of the given array using the delimiter.
array_join(x, delimiter[, null_replacement]) → string	Concatenates the elements of the given array using the delimiter and an optional string to replace nulls.
array_max/array_min(a)	Returns the maximum or minimum value of input array *a*.
array_position(a, element) → int	Returns the position of the first occurrence of the *element* in array *a* (or 0 if not found).
array_position(a, element, instance) → int	Returns the position of the first occurrence of the *element* in array *a*. If no matching element instance is found, **0** is returned. If *instance* > 0, returns the position of the *instance*-th occurrence of the *element* in array *a*. If *instance* < 0, return the position of the *instance*-to-last occurrence of the *element* in array *a*.
array_remove(a, element) → array	Removes all elements that equal *element* from array *a*.
array_sort(a) → array	Sorts and returns array *a*.
array_sort(array(T), function(<T, T>, int)) → array	Sorts and returns the *array* based on the given comparator *function*. The comparator will take two nullable arguments representing two nullable elements of the *array*. It returns **-1**, **0**, or **1** as the first nullable element is less than, equal to, or greater than the second nullable element.
array_sum(a)	Returns the sum of all non-null elements of *a*.
array_overlap(a, b) → boolean	Tests if arrays *a* and *b* have any non-null elements in common.
array_union(a, b) → array	Returns an array of the elements in the union of *a* and *b*, without duplicates.

Function	Description
array_except(x, y) → array	Returns an array of elements in **x** but not in **y**.
cardinality(a) → int	Returns the cardinality (size) of array *a*.
concat(a1, a2, ...) → array	Concatenates the arrays *a1*, *a2*, ... This function provides the same functionality as the SQL-standard concatenation operator (||).
contains(a, element) → boolean	Returns true if the array *a* contains the *element*.
element_at(a, index)	Returns element of *a* at given *index*. If *index* < 0, element_at accesses elements from the last to the first.
filter(array(T), function(T, boolean)) → array(T)	Constructs an array from those elements of *array* for which *function* returns true.
none_match(array(T), function(T, boolean)) → boolean	Returns whether no elements of an array match the given predicate.
reverse(a) → array	Returns an array which has the reversed order of array *a*.
sequence(start, stop, step)	Generates a sequence of timestamps from *start* to *stop*, incrementing by *step*. It is similar to the range() function in Python, which returns a sequence of numbers, starting from 0 by default, and increments by 1 (by default), and stops before a specified number.
shuffle(a) → array	Generates a random permutation of given array *a*.
slice(a, start, length) → array	Subsets array *a* starting from index *start* (or starting from the end if *start* is negative) with a length of *length*.
transform(array(T), function(T, S)) → array(S)	Returns an array that is the result of applying *function* to each element of *array*.

Table 8-30 Aggregate functions

Function	Description
arbitrary(x)	Returns an arbitrary non-null value of *x*, if one exists.
array_agg(x) → array	Returns an array created from the input *x* elements.
avg(x) → double	Returns the average (arithmetic mean) of all input values.
bool_and/bool_or(x) → boolean	**bool_and** returns **TRUE** if every input value is **TRUE**, otherwise **FALSE**. **bool_or** returns **TRUE** if any input value is **TRUE**, otherwise **FALSE**.
coalesce(value1, value2, ...)	Returns the first non-null value in an argument list. Short-circuit evaluation will be used.
count(*)/count(x) → int	**count(*)** returns the number of input rows. **count(x)** returns the number of non-null input values.
greatest(value1, value2, ..., valueN)	Returns the largest of the provided values.
histogram(x) → map	Returns a map containing the count of the number of times each input value occurs.
least(value1, value2, ..., valueN)	Returns the smallest of the provided values.
max/min(x, n=1)	Returns *n* largest or smallest values of all input values of *x*.
max_by/min_by(x, y, n=1)	Returns *n* values of *x* associated with the *n* largest of all input values of *y* in descending order of *y*, or return *n* values of *x* associated with the *n* smallest of all input values of *y* in ascending order of *y*.
geometric_mean(x) → double	Returns the geometric mean of all input values.
set_agg(x) → array	Returns an array created from the distinct input *x* elements.
set_union(x) → array	Returns an array of all the distinct values contained in each array of the input.
sum(x)	Returns the sum of all input values.

Function	Description
multimap_agg(key, value)	Returns multiple mappings created from input key-value pairs.
map_agg(key, value)	Returns the mapping created from the input key-value pair.

Table 8-31 Time functions

Function	Description
now() → date	Returns the current time.
date_diff(unit, timestamp1, timestamp2) → int	Returns timestamp2-timestamp1 expressed in terms of unit. The option of unit can be millisecond, second, minute, hour, day, week, month, quarter, or year.
date_parse(string, format) → timestamp	Parses a string into a timestamp using **format**.

9 Change History

Released On	Description
2023-12-30	This issue is the seventeenth official release, which incorporates the following change: Optimized **Predefined Policies**.
2023-11-24	This issue is the sixteenth official release. which incorporates the following changes: • Added **Organization Conformance Packages**. • Added the content in **Cross-Account Authorization** to explain that an encrypted OBS bucket ban be specified when the resource recorder is configured.
2023-10-25	This issue is the fifteenth official release, Added the new feature **Conformance Packages**. A conformance package is a collection of rules. Config provides you with conformance packages to centrally create and manage rules, and query compliance data.
2023-10-11	This is the fourteenth official release. The following content is added: • **Viewing Resource Compliance Data** • **Viewing Noncompliant Resources**
2023-06-07	This issue is the thirteenth official release, which incorporates the following change: Changed the service name from Resource Management Service (RMS) to Config.

Released On	Description
2023-04-20	This issue is the twelfth official release, which incorporates the following changes: • Added **Organization Rules**. • Added **Viewing Aggregated Rules**. • Added **Advanced Queries**.
2023-03-30	This issue is the eleventh official release, which incorporates the following changes: • Added **Resource Aggregation**. • The **My Resources** feature is renamed **Resource List**.
2023-02-17	This issue is the tenth official release, which incorporates the following change: Added **Event Monitoring**.
2022-12-30	This issue is the ninth official release, which incorporates the following changes: • Added **Adding a Custom Rule**. • Added **Example Functions (Python)**. • Added **Events**.
2022-08-24	This issue is the eighth official release, which incorporates the following change: Added **Cross-account authorization**: Permissions on SMN topics and OBS buckets can be granted across accounts during resource recorder configuration.
2022-04-06	This issue is the seventh official release, which incorporates the following changes: • Added **Advanced Queries**. • Added **ResourceQL Syntax**.
2021-09-09	This issue is the sixth official release. Added **Why Can't I Delete Resources on the Resource List Page?**.
2021-07-16	This issue is the fifth official release, which incorporates the following change: Changed **Management & Deployment** to **Management & Governance** and **Computing** to **Compute** based on changes in the console product catalog.

Released On	Description
2020-12-28	This issue is the fourth official release, which added the following sections: • **Cloud Trace Service** • **Supported CTS Operations** • **Querying Real-Time Traces**
2020-12-16	This issue is the third official release. Added **FAQs**.
2020-12-14	This issue is the second official release, which added the following sections: • **Storing Resource Change Messages** • **Notification Model of Resource Change Notification Storage Completed** • **Models of Resource Change Notification Storage**
2020-11-30	This issue is the first official release. • **Resource List** : You can view, filter, and export resources. You can also view resource relationships and resource history. • **Resource Recorder**: You can enable, configure, and modify the resource recorder. • **Resource Compliance**: You can add, trigger, and modify rules.

