Config

User Guide

Issue 01

Date 2025-02-27

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

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

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

Contents

1 Resource List

1.1 Viewing Resources

1.1.1 Querying All Resources

Scenarios

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

NOTICE

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 the resource recorder is enabled, Config will update resource changes within 24 hours.

To use the resource list, you must enable the resource recorder. If no resources are displayed on the resource list page, check if the resource recorder is enabled, if the resource type is within the configured monitoring scope, or if the service or resource is supported by Config. For details about how to configure the resource recorder, see **Configuring the Resource Recorder**.

If you need to view resources before the resource recorder is enabled, go to **My Resources**.

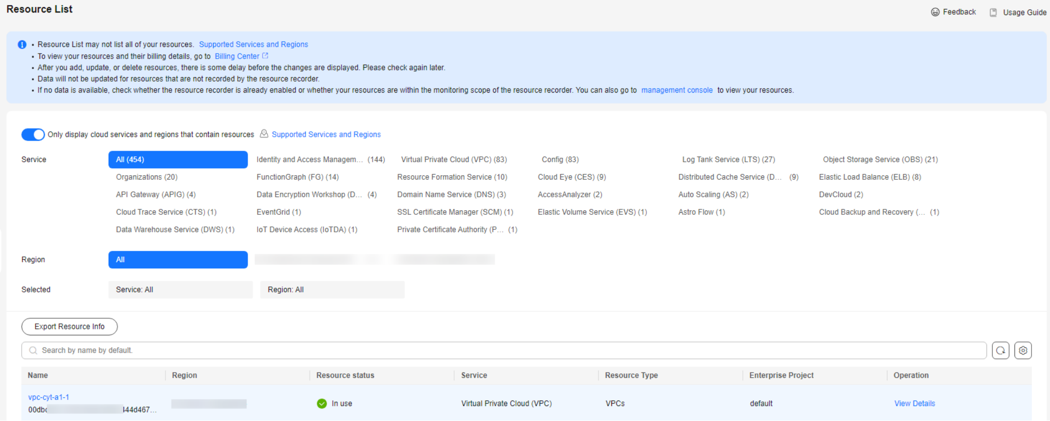
Procedure

Step 1 Log in to the management console.

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

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

Figure 1-1 Resource List



Resource List

- Resource List may not list all of your resources. Supported Services and Regions
- To view your resources and their billing details, go to Billing Center
- After you add, update, or delete resources, there is some delay before the changes are displayed. Please check again later.
- Data will not be updated for resources that are not recorded by the resource recorder.
- If no data is available, check whether the resource recorder is already enabled or whether your resources are within the monitoring scope of the resource recorder. You can also go to management console to view your resources.

Only display cloud services and regions that contain resources Supported Services and Regions

Service: All (454) | Identity and Access Managem... (144) | Virtual Private Cloud (VPC) (83) | Config (83) | Log Tank Service (LTS) (27) | Object Storage Service (OBS) (21) | Organizations (20) | FunctionGraph (FG) (14) | Resource Formation Service (10) | Cloud Eye (CES) (9) | Distributed Cache Service (D... (9) | Elastic Load Balance (ELB) (8) | API Gateway (APIG) (4) | Data Encryption Workshop (D... (4) | Domain Name Service (DNS) (3) | AccessAnalyzer (2) | Auto Scaling (AS) (2) | DevCloud (2) | Cloud Trace Service (CTS) (1) | EventGrid (1) | SSL Certificate Manager (SCM) (1) | Elastic Volume Service (EVS) (1) | Astro Flow (1) | Cloud Backup and Recovery (... (1) | Data Warehouse Service (DWS) (1) | IoT Device Access (IoTDA) (1) | Private Certificate Authority (P... (1)

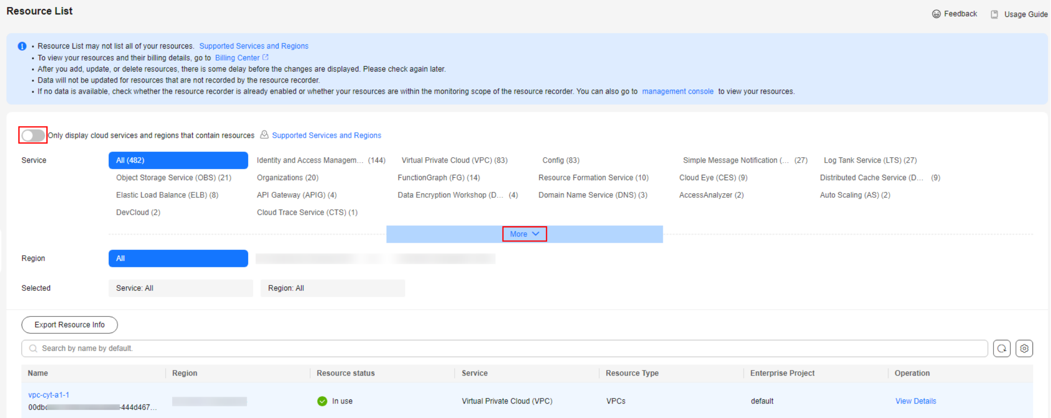
Region: All [redacted]

Selected: Service: All | Region: All

Name	Region	Resource status	Service	Resource Type	Enterprise Project	Operation
vpc-cyt-a1-1 00db[redacted]44d467...	[redacted]	In use	Virtual Private Cloud (VPC)	VPCs	default	View Details

Step 3 Disable **Only display cloud services and regions that contain resources** and then click **More** to view all services that are supported by Config.

Figure 1-2 Viewing all services supported by Config



Resource List

- Resource List may not list all of your resources. Supported Services and Regions
- To view your resources and their billing details, go to Billing Center
- After you add, update, or delete resources, there is some delay before the changes are displayed. Please check again later.
- Data will not be updated for resources that are not recorded by the resource recorder.
- If no data is available, check whether the resource recorder is already enabled or whether your resources are within the monitoring scope of the resource recorder. You can also go to management console to view your resources.

Only display cloud services and regions that contain resources Supported Services and Regions

Service: All (482) | Identity and Access Managem... (144) | Virtual Private Cloud (VPC) (83) | Config (83) | Simple Message Notification (... (27) | Log Tank Service (LTS) (27) | Object Storage Service (OBS) (21) | Organizations (20) | FunctionGraph (FG) (14) | Resource Formation Service (10) | Cloud Eye (CES) (9) | Distributed Cache Service (D... (9) | Elastic Load Balance (ELB) (8) | API Gateway (APIG) (4) | Data Encryption Workshop (D... (4) | Domain Name Service (DNS) (3) | AccessAnalyzer (2) | Auto Scaling (AS) (2) | DevCloud (2) | Cloud Trace Service (CTS) (1)

Region: All [redacted]

Selected: Service: All | Region: All

Name	Region	Resource status	Service	Resource Type	Enterprise Project	Operation
vpc-cyt-a1-1 00db[redacted]444d467...	[redacted]	In use	Virtual Private Cloud (VPC)	VPCs	default	View Details

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 some resource attributes. You can perform the following procedure to view more resource details.

Procedure

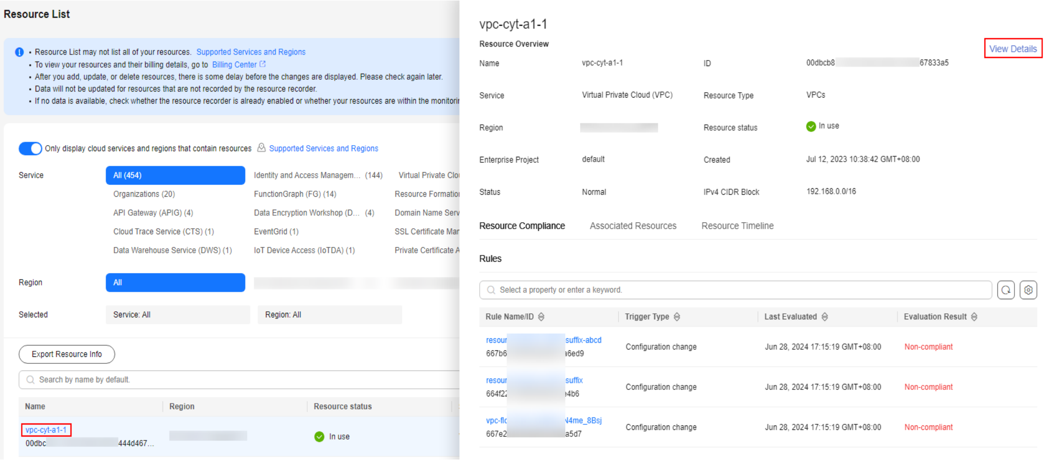
Step 1 Log in to the management console.

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 1-3 Resource overview and details



Resource List

- Resource List may not list all of your resources. Supported Services and Regions
- To view your resources and their billing details, go to Billing Center
- After you add, update, or delete resources, there is some delay before the changes are displayed. Please check again later.
- Data will not be updated for resources that are not recorded by the resource recorder.
- If no data is available, check whether the resource recorder is already enabled or whether your resources are within the monitori

Only display cloud services and regions that contain resources Supported Services and Regions

Service: All (454), Identity and Access Managem... (144), Virtual Private Clo, Organizations (20), FunctionGraph (FG) (14), Resource Formatio, API Gateway (APIG) (4), Data Encryption Workshop (D... (4), Domain Name Serv, Cloud Trace Service (CTS) (1), EventGrid (1), SSL Certificate Mar, Data Warehouse Service (DWS) (1), IoT Device Access (IoTDA) (1), Private Certificate A

Region: All [redacted]

Selected: Service: All, Region: All

Name	Region	Resource status
vpc-cyt-a1-1 00dbc[redacted]444d467...	[redacted]	In use

vpc-cyt-a1-1

Resource Overview

Name	vpc-cyt-a1-1	ID	00dbcb8[redacted]67833a5
Service	Virtual Private Cloud (VPC)	Resource Type	VPCs
Region	[redacted]	Resource status	In use
Enterprise Project	default	Created	Jul 12, 2023 10:38:42 GMT+08:00
Status	Normal	IPv4 CIDR Block	192.168.0.0/16

Rules

Rule Name/ID	Trigger Type	Last Evaluated	Evaluation Result
resour[redacted]suffix-abcd 667b6[redacted]a6ed9	Configuration change	Jun 28, 2024 17:15:19 GMT+08:00	Non-compliant
resour[redacted]suffix 664f2[redacted]4b6	Configuration change	Jun 28, 2024 17:15:19 GMT+08:00	Non-compliant
vpc-flo[redacted]N4me_8Bsj 667e2[redacted]a5d7	Configuration change	Jun 28, 2024 17:15:19 GMT+08:00	Non-compliant

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, and region on the Resource List page. In the search box in the middle of the page, you can also 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	Resource name. Fuzzy search is supported. The resource name is case-insensitive.
Resource ID	Resource ID. Fuzzy search is supported. The resource ID is case-sensitive.
Resource Status	Resource status. A resource can be in either of the following states: ● **In use**: A resource is being used. ● **Deleted**: A resource has been deleted.

Filter Criteria	Description
Tags	You can select a tag key and one or all values of this key to filter resources.
Enterprise Project	The enterprise project which resources belong to. If you select an enterprise project, resources in this enterprise project will be displayed. **NOTE** To filter resources by enterprise project, you need to **enable Enterprise Center** first. Filtering resources by enterprise project is only available to some users.

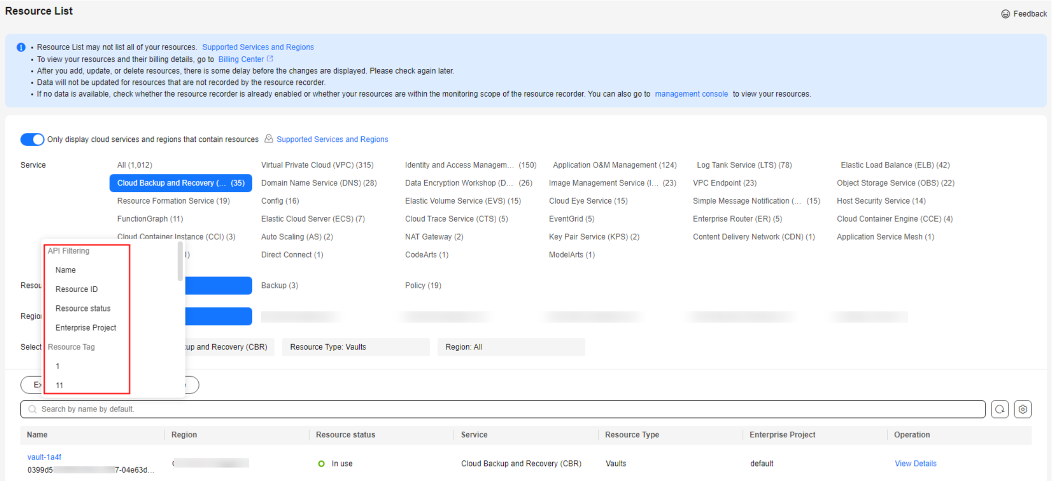
Procedure

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 by enterprise project, resource name, resource ID, resource status, enterprise project, or resource tag.

Figure 1-4 Filtering resources



Resource List

- Resource List may not list all of your resources. Supported Services and Regions
- To view your resources and their billing details, go to Billing Center
- After you add, update, or delete resources, there is some delay before the changes are displayed. Please check again later.
- Data will not be updated for resources that are not recorded by the resource recorder.
- If no data is available, check whether the resource recorder is already enabled or whether your resources are within the monitoring scope of the resource recorder. You can also go to management console to view your resources.

Only display cloud services and regions that contain resources

Resource Type: Vaults

Region: All

Name	Region	Resource status	Service	Resource Type	Enterprise Project	Operation
vault-1a4f 0399d5[redacted]7-04e63d...	[redacted]	○ In use	Cloud Backup and Recovery (CBR)	Vaults	default	View Details

Feedback
Supported Services and Regions
Service
All (1,012)
Virtual Private Cloud (VPC) (315)
Identity and Access Managem... (150)
Application O&M Management (124)
Log Tank Service (LTS) (78)
Elastic Load Balance (ELB) (42)
Cloud Backup and Recovery (... (35)
Domain Name Service (DNS) (28)
Data Encryption Workshop (D... (26)
Image Management Service (I... (23)
VPC Endpoint (23)
Object Storage Service (OBS) (22)
Resource Formation Service (19)
Config (16)
Elastic Volume Service (EVS) (15)
Cloud Eye Service (15)
Simple Message Notification (... (15)
Host Security Service (14)
FunctionGraph (11)
Elastic Cloud Server (ECS) (7)
Cloud Trace Service (CTS) (5)
EventGrid (5)
Enterprise Router (ER) (5)
Cloud Container Engine (CCE) (4)
Cloud Container Instance (CCI) (3)
Auto Scaling (AS) (2)
NAT Gateway (2)
Key Pair Service (KPS) (2)
Content Delivery Network (CDN) (1)
Application Service Mesh (1)
Direct Connect (1)
CodeArts (1)
ModelArts (1)
Resou
Backup (3)
Policy (19)
Regio
Select
up and Recovery (CBR)
API Filtering
Name
Resource ID
Resource status
Enterprise Project
Resource Tag
1
11
Ex
Search by name by default.

----End

1.1.4 Exporting the Resource List

Scenarios

On the Resource List page, you can export resource information.

Procedure

Step 1 Log in to the management console.

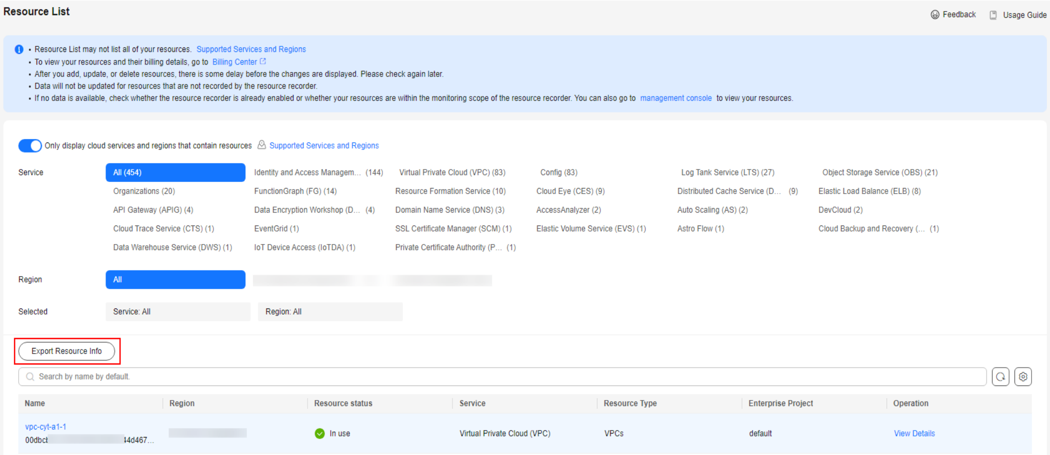
Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

Step 3 Set search options to filter resources and click **Export Resource Info** above the list.

Only information that you can see in the list will be exported.

- If you do not set any search options, all your resources that are supported by Config will be exported.
- If you set search options to filter resources, only the search results will be exported. For details about how to filter resources, see **Filtering Resources**.

Figure 1-5 Exporting resource information



Resource List

- Resource List may not list all of your resources. Supported Services and Regions
- To view your resources and their billing details, go to Billing Center
- After you add, update, or delete resources, there is some delay before the changes are displayed. Please check again later.
- Data will not be updated for resources that are not recorded by the resource recorder.
- If no data is available, check whether the resource recorder is already enabled or whether your resources are within the monitoring scope of the resource recorder. You can also go to management console to view your resources.

Only display cloud services and regions that contain resources Supported Services and Regions

Service: All (454), Identity and Access Managem... (144), Virtual Private Cloud (VPC) (83), Config (83), Log Tank Service (LTS) (27), Object Storage Service (OBS) (21), Organizations (20), FunctionGraph (FG) (14), Resource Formation Service (10), Cloud Eye (CES) (9), Distributed Cache Service (D... (9), Elastic Load Balance (ELB) (8), API Gateway (APIG) (4), Data Encryption Workshop (D... (4), Domain Name Service (DNS) (3), AccessAnalyzer (2), Auto Scaling (AS) (2), DevCloud (2), Cloud Trace Service (CTS) (1), EventGrid (1), SSL Certificate Manager (SCM) (1), Elastic Volume Service (EVS) (1), Astro Flow (1), Cloud Backup and Recovery (... (1), Data Warehouse Service (DWS) (1), IoT Device Access (IoTDA) (1), Private Certificate Authority (P... (1)

Region: All [redacted]

Selected: Service: All Region: All

Name	Region	Resource status	Service	Resource Type	Enterprise Project	Operation
vpc-cyt-a1-1 00dbc[redacted]4d467...	[redacted]	In use	Virtual Private Cloud (VPC)	VPCs	default	View Details

----End

NOTE

Information of all resources will be exported to an Excel file, containing all attributes that are reported to Config.

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**.

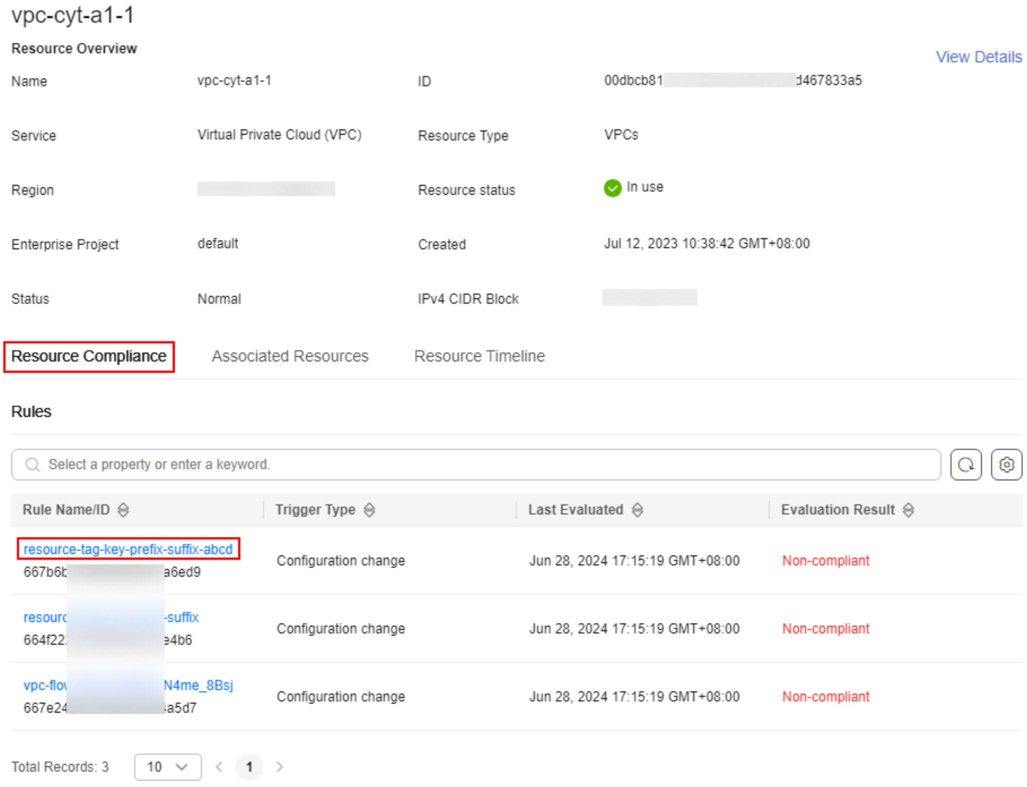
Step 3 On the **Resource List** page, click the name of a target resource.

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.

In the search box above the list, enter a rule name, a rule ID, the trigger type, the time of the latest evaluation, or the evaluation result to filter rules.

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

Figure 1-6 Viewing resource compliance data



vpc-cyt-a1-1

Resource Overview

View Details

Name	vpc-cyt-a1-1	ID	00dbcb81[redacted]d467833a5
Service	Virtual Private Cloud (VPC)	Resource Type	VPCs
Region	[redacted]	Resource status	✓ In use
Enterprise Project	default	Created	Jul 12, 2023 10:38:42 GMT+08:00
Status	Normal	IPv4 CIDR Block	[redacted]

Rules

Rule Name/ID	Trigger Type	Last Evaluated	Evaluation Result
resource-tag-key-prefix-suffix-abcd 667b6[redacted]a6ed9	Configuration change	Jun 28, 2024 17:15:19 GMT+08:00	Non-compliant
resourc[redacted]-suffix 664f22[redacted]e4b6	Configuration change	Jun 28, 2024 17:15:19 GMT+08:00	Non-compliant
vpc-flo[redacted]N4me_8Bsj 667e24[redacted]a5d7	Configuration change	Jun 28, 2024 17:15:19 GMT+08:00	Non-compliant

Total Records: 3 10 < 1 >

----End

1.3 Viewing Resource Relationships

Scenarios

Config allows you to view resource relationships. A resource relationship may be described as that an EVS disk is attached to an ECS or an ECS is deployed in a VPC. Through resource relationships, you can gain insights into the structures and dependencies of your resources. Config only provides relationships of supported resources. For more 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**.

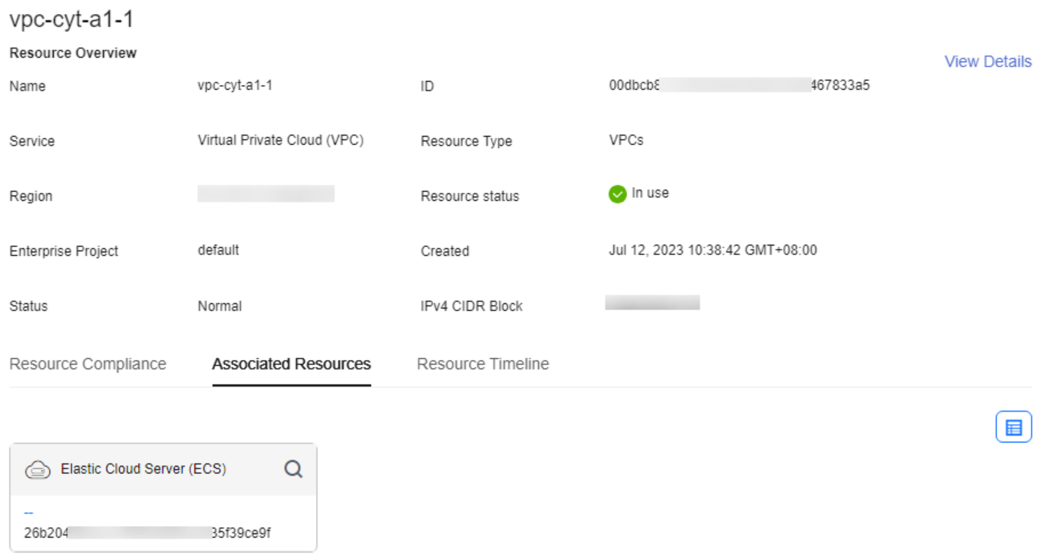
Step 3 On the **Resource List** page, click the name of a target resource.

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

Hover over the name of an associated resource to view resource information and resource relationships.

For each service, you can filter resources by resource ID or resource name.

Figure 1-7 Associated Resources



vpc-cyt-a1-1

Resource Overview

View Details

Name	vpc-cyt-a1-1	ID	00dbcb8[redacted]467833a5
Service	Virtual Private Cloud (VPC)	Resource Type	VPCs
Region	[redacted]	Resource status	✓ In use
Enterprise Project	default	Created	Jul 12, 2023 10:38:42 GMT+08:00
Status	Normal	IPv4 CIDR Block	[redacted]

----End

NOTE

On the **Associated Resources** tab, you can click the name of an associated resource to view related information of this resource.

1.4 Viewing Resource Changes

Prerequisites

Resource changes that are reported to Config 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. A record will be added to the resource timeline when the related service reports a resource attribute or relationship change to Config and the record will be retained for seven years by default.

NOTE

A maximum of 1,000 resource relationships can be displayed in the **Resource Timeline** tab.

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.

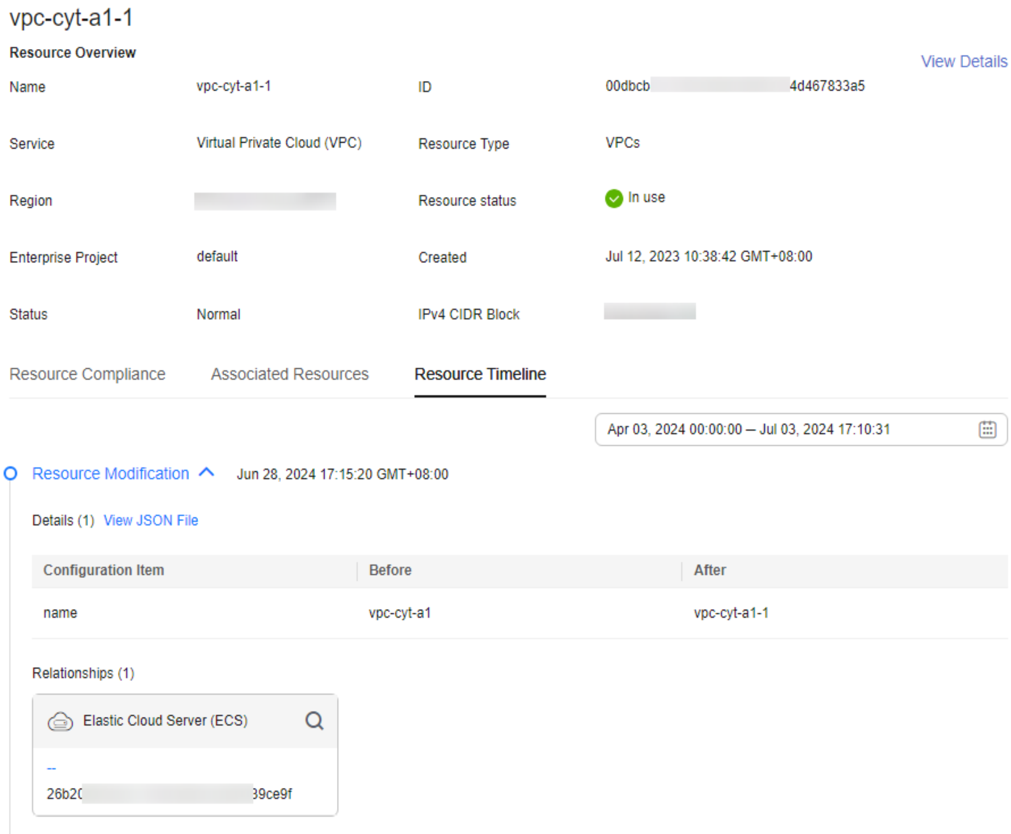
Step 4 Choose the **Resource Timeline** tab to view the resource changes.

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 also click **View JSON File** to view the resource attributes reported to Config.

Figure 1-8 Resource timeline



vpc-cyt-a1-1

Resource Overview

View Details

Name	vpc-cyt-a1-1	ID	00dbcb[redacted]4d467833a5
Service	Virtual Private Cloud (VPC)	Resource Type	VPCs
Region	[redacted]	Resource status	✓ In use
Enterprise Project	default	Created	Jul 12, 2023 10:38:42 GMT+08:00
Status	Normal	IPv4 CIDR Block	[redacted]

Apr 03, 2024 00:00:00 – Jul 03, 2024 17:10:31

○ Resource Modification ^ Jun 28, 2024 17:15:20 GMT+08:00

Details (1) View JSON File

Configuration Item	Before	After
name	vpc-cyt-a1	vpc-cyt-a1-1

Relationships (1)

Elastic Cloud Server (ECS)

--

26b2[redacted]39ce9f

----End

2 Resource Recorder

2.1 Overview

Introduction

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

To be specific, the resource recorder:

- Notifies you using the specified SMN topic if your resources are created, modified, or deleted.
- Notifies you using the specified SMN topic if there is a change to your resource relationships.
- Stores your resource change notifications every 6 hours if you have configured an OBS bucket and an SMN topic.
- Stores resource snapshots every 24 hours if you have configured an OBS bucket.

For details about resources supported by the resource recorder, see **Services and Regions Supported by Config**.

Notes and Constraints

- When enabling and configuring the resource recorder, you must configure **Topic** or **Resource Dump**. To enable the resource recorder, you must configure either an SMN topic or an OBS bucket.
- To receive notifications of resource changes with the configured SMN topic, you not only have to create the topic, but also add subscription endpoints and request subscription confirmations for the topic. For details, see **Creating a Topic**, **Adding a Subscription**, and **Requesting Subscription Confirmation**.
- The resource recorder only updates data for the resources within the monitoring scope.
- By default, the resource configuration information is stored for seven years (2,557 days).

- You can enable or modify the resource recorder for up to 10 times per day. The number of times will be reset at 00:00 every day.
- There is a delay in synchronizing resource data to Config. The delay varies depending on services. If the resource recorder is enabled, Config will update related data for resources that are included in the monitoring scope within 24 hours. If the resource recorder is disabled, Config will not update resource data.

NOTICE

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

2.2 Configuring the Resource Recorder

Scenarios

You must enable the resource recorder for Config to track changes to your resource configurations.

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

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

This section includes the following content:

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

Enabling the Resource Recorder

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

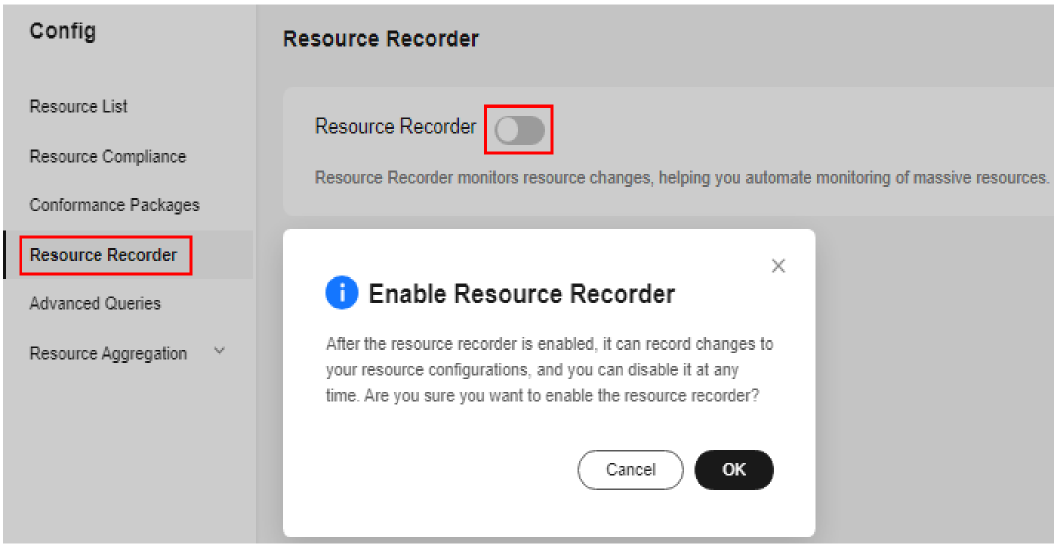
Step 1 Log in to the management console.

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

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

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

Figure 2-1 Enabling the resource recorder



Resource Recorder monitors resource changes, helping you automate monitoring of massive resources.

Enable Resource Recorder

After the resource recorder is enabled, it can record changes to your resource configurations, and you can disable it at any time. Are you sure you want to enable the resource recorder?

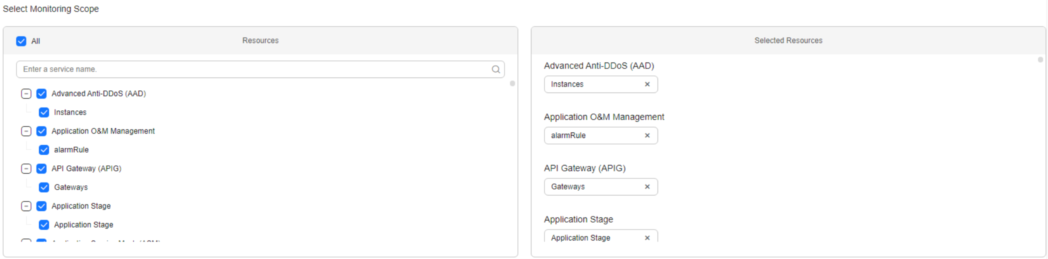
Step 5 Select the monitoring scope.

By default, all resources supported by Config will be recorded by the resource recorder. You can also specify a resource scope for the resource recorder.

NOTE

By default, the resource recorder records all resources of Config, and these resources cannot be deselected.

Figure 2-2 Specifying the monitoring scope


Select Monitoring Scope

☑ All Resources

Enter a service name.

☑ Advanced Anti-DDoS (AAD)
☑ Instances
☑ Application O&M Management
☑ alarmRule
☑ API Gateway (APIG)
☑ Gateways
☑ Application Stage
☑ Application Stage

Selected Resources

Advanced Anti-DDoS (AAD)
Instances ×
Application O&M Management
alarmRule ×
API Gateway (APIG)
Gateways ×
Application Stage
Application Stage ×

Step 6 Specify an OBS bucket.

Specify an OBS bucket to store notifications of resource changes and resource snapshots.

To enable the resource recorder, you must configure either an SMN topic or an OBS bucket.

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

  Select **Your bucket** and then select a bucket from the drop-down list to store resource change notifications and resource snapshots. If you need to store the notifications and snapshots to a specific folder in the OBS bucket, enter the folder name after you select a bucket. If there are no OBS buckets in the current account, create one first. For details, see **Creating a Bucket**.

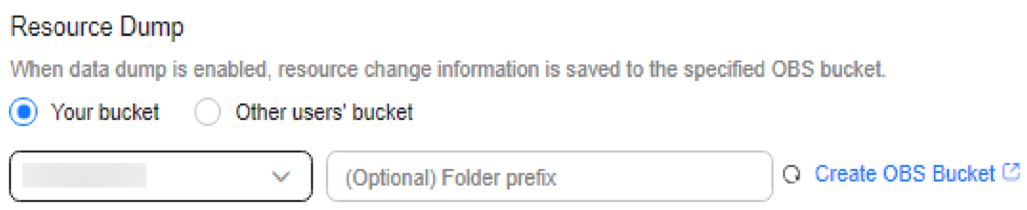
- **Select an OBS bucket from another account**:

  Select **Other users' bucket** and then configure **Region ID** and **Bucket Name**. If you need to store the notifications and snapshots to a specific folder in the OBS bucket, enter the folder name after you select a bucket. 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 specify an OBS bucket from the current or another account, Config will write an empty file named **ConfigWritabilityCheckFile** to the OBS bucket to verify whether resources can be written to the OBS bucket. If an error is reported, you can address the error based on **Why Is an Error Reported When Data Is Dumped to the OBS Bucket After the Resource Recorder Is Enabled?**

Figure 2-3 Specifying an OBS bucket



Resource Dump

When data dump is enabled, resource change information is saved to the specified OBS bucket.

● Your bucket ○ Other users' bucket

[redacted] | (Optional) Folder prefix | Create OBS Bucket

Step 7 Specify a data retention period.

Select **Seven years (2,557 days)** or select **A custom period** and enter a retention period from 30 days to 2,557 days.

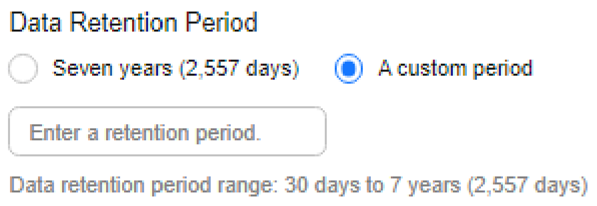
NOTE

The data retention period only applies to resource configurations and snapshots reserved by Config. It will not affect your data storage with SMN or OBS.

After a retention period is configured, Config will delete data older than the retention period.

If you modify the data retention period, the change is only applied to newly recorded data. Existing data is not affected. For example, if you modify the data retention period from 100 days to 30 days, data recorded after the modification will only be retained for 30 days by Config, and data recorded before the modification will still be retained for 100 days.

Figure 2-4 Specifying a data retention period



Data Retention Period

○ Seven years (2,557 days) ● A custom period

Enter a retention period.

Data retention period range: 30 days to 7 years (2,557 days)

Step 8 (Optional) Configure an SMN topic.

Toggle on **Topic**, then select a region and an SMN topic for receiving notifications of resource changes.

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

  Select **Your topic**, then select a region and an SMN topic. If there are no SMN topics available, create one first. For details, see **Creating a Topic**.

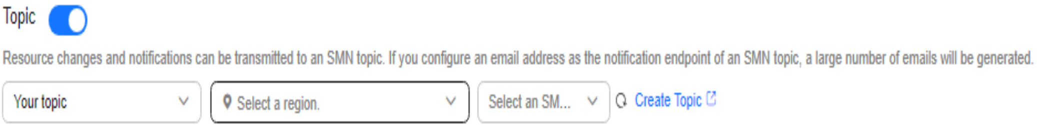
- **Select a topic from another account**:

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

NOTE

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

Figure 2-5 Selecting an SMN topic



Topic

Resource changes and notifications can be transmitted to an SMN topic. If you configure an email address as the notification endpoint of an SMN topic, a large number of emails will be generated.

Your topic | Select a region. | Select an SM... | Create Topic

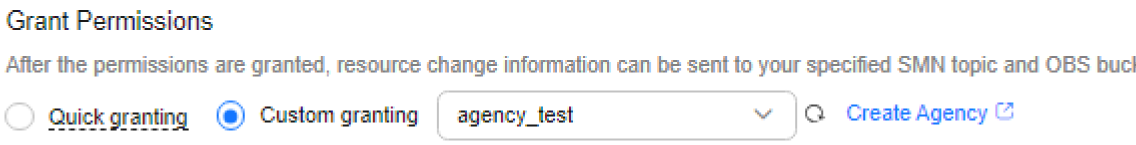
Step 9 Grant permissions.

- **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 contains permissions, including the **SMN Administrator** for sending notifications and the **OBS OperateAccess** permission for writing data into an OBS bucket. The agency created by **quick granting** does not contain KMS permissions, so the resource recorder is unable to store resource change notifications and snapshots to an OBS bucket that is encrypted using KMS. If you need to use an encrypted bucket, you can add required **KMS Administrator** permissions to the agency or use custom authorization. For details, see **Storing Resource Change Notifications and Resource Snapshots to an Encrypted OBS Bucket**.

  For details about how to add permissions in an agency, see **Deleting or Modifying Agencies**.

- **Custom granting**: You can create an agency using IAM to customize authorization for Config. The agency must include either the permissions for sending notifications using an SMN topic or the permissions for writing data into an OBS bucket. To store resource changes and snapshots to an OBS bucket that is encrypted using KMS, you need the required **KMS Administrator** permissions. For details, see **Storing Resource Change Notifications and Resource Snapshots to an Encrypted OBS Bucket**. For details about how to create an agency, see **Cloud Service Agency**.

Figure 2-6 Grant permissions



Grant Permissions

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

○ Quick granting ● Custom granting agency_test | Create Agency

Step 10 Click **Save**.

Step 11 In the displayed dialog box, click OK.

----End

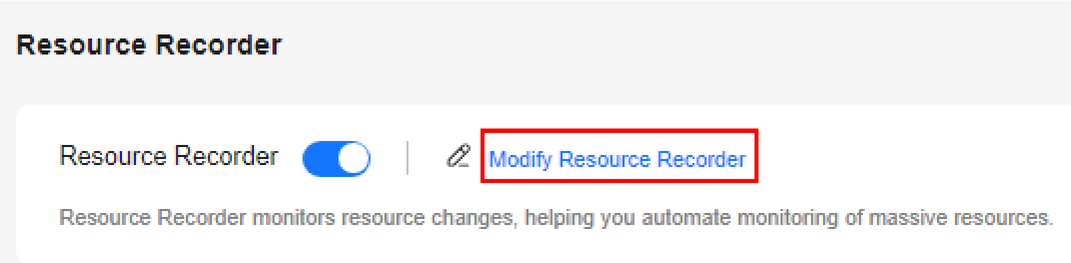
Modifying the Resource Recorder

You can modify the resource recorder at any time.

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

Step 2 Click **Modify Resource Recorder**.

Figure 2-7 Modifying the resource recorder



Resource Recorder

Resource Recorder monitors resource changes, helping you automate monitoring of massive resources.

Step 3 Modify configurations.

Step 4 Click **Save**.

Step 5 In the displayed dialog box, click OK.

----End

Disabling the Resource Recorder

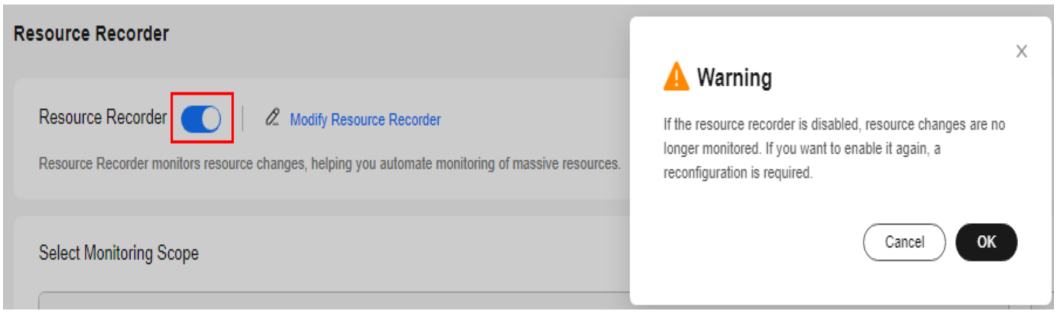
You can disable the resource recorder at any time.

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

Step 2 Toggle off the resource recorder.

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

Figure 2-8 Disabling the resource recorder



Resource Recorder

Resource Recorder monitors resource changes, helping you automate monitoring of massive resources.

Select Monitoring Scope

Warning

If the resource recorder is disabled, resource changes are no longer monitored. If you want to enable it again, a reconfiguration is required.

----End

Cross-Account Authorization

- **Granting SMN topic permissions to another account**
  a. Log in to the management console with the authorizing account and go to the SMN console.
  b. Attach related SMN permissions to target accounts based on **Configuring Topic Policies in Basic Mode**.

     If an account is not attached with related SMN permissions, the account cannot receive resource change notifications.
- **Granting OBS bucket permissions to another account**
  a. Log in to the management console with the authorizing account and go to the OBS console.
  b. Grant related OBS permissions to target accounts based on **Creating a Custom Bucket Policy (JSON View)**.

     The following is an example of a bucket policy. The policy allows the authorized account to store data into a specific object or folder in an OBS bucket. You need to configure the following parameters in a bucket policy:

     - ${account_id}: ID of the authorized account
     - ${agency_name}: Agency name. If you choose **Quick granting**, this parameter will be set to **rms_tracker_agency**.
     - ${bucket_name}: The name of an OBS bucket.
     - ${folder_name}: The name of a folder in an OBS bucket. If you do not need to specify a folder or object in an OBS bucket, you do not need to configure **/${folder_name}**.

```
{
  "Statement": [
    {
      "Sid": "org-bucket-policy",
      "Effect": "Allow",
      "Principal": {
        "ID": [
          "domain/${account_id}:agency/${agency_name}"
        ]
      },
      "Action": [
        "PutObject"
      ],
      "Resource": [
        "${bucket_name}/${folder_name}/RMSLogs/*/Snapshot/*",
        "${bucket_name}/${folder_name}/RMSLogs/*/Notification/*"
      ]
    }
  ]
}
```

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

- **Using an OBS bucket that is encrypted with SSE-OBS**

  If you need to store resource change notifications 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.

- **Using an OBS bucket that is encrypted with a default key of SSE-KMS**

  If you need to store resource change notifications 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.

- **Using an OBS bucket that is encrypted with a custom key of SSE-KMS**

  If you need to store resource change notifications and snapshots to an OBS bucket 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 notifications 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. Log in to the management console and go to the **Key Management Service** page on the Data Encryption Workshop (DEW) console.

  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 permissions for using the key based on **Creating a Grant**.

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

     - Select **Create Data Key**, **Describe Key**, and **Decrypt Data Key** for **Granted Operations**.

2.3 Batch Configuring the Resource Recorder

Scenario

To get full functionality of Config, you need to enable the resource recorder. If the resource recorder is disabled, you may have problems using other features of Config.

If you are an organization administrator, you can batch enable and configure the resource recorder for organization members using Terraform templates and RFS stacks. This effectively improves configuration efficiency by eliminating the need to confiture the resource recorder for each member account.

This section describes how to batch enable and configure the resource recorder across an organization.

Procedure Overview

Step	Description
Enabling RFS as a Trusted Service	Enabling Resource Formulation Stack Set Service (RF) as a trusted service using the service Organizations

Step	Description
Configuring an OBS Bucket Policy	Configuring a bucket policy allowing organization members to dump their resource data into the specified OBS bucket
Configure an SMN Topic Policy	Configuring an access policy allowing organization members to send notifications with the specified SMN topic
Creating an RFS Resource Stack Set	Creating an RFS stack set with a Terraform template and deploying stack instances to organization members

Restrictions and Limitations

- Currently, an RFS stack set can be used to enable the resource recorders for up to 100 organization members.
- Only an organization administrator is allowed to created RFS stack sets.
- The resource stack set deploys resource stacks to organization members, but not the organization administrator.
- If an organization member has already enabled and configured the resource recorder, the configurations delivered through the stack set will not overwrite the current configurations of the resource recorder in the member account.

Enabling RFS as a Trusted Service

The following procedure shows how to enable RFS as a trusted service:

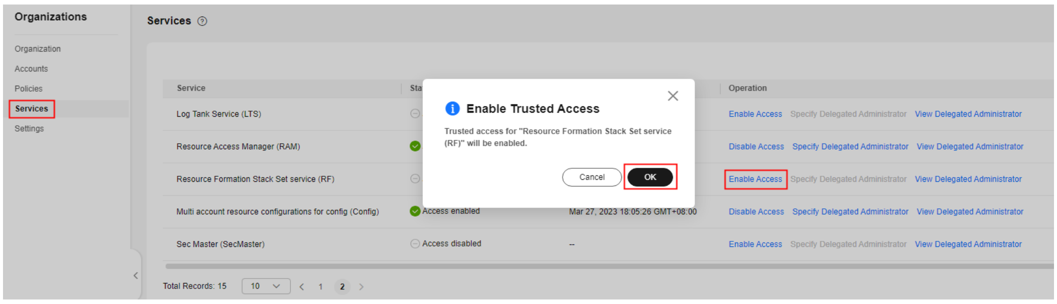
Step 1 Log in to the management console as an organization administrator and go to the Organizations console.

Step 2 In the navigation pane on the left, choose **Services**.

Step 3 In the row that contains **Resource Formation Stack Set service (RF)**, click **Enable Access** in the **Operation** column.

Step 4 In the displayed dialog box, click **OK**.

Figure 2-9 Enabling RFS as a trusted service



Enable Trusted Access

Trusted access for "Resource Formation Stack Set service (RF)" will be enabled.

Service	Sta		Operation
Log Tank Service (LTS)			Enable Access Specify Delegated Administrator View Delegated Administrator
Resource Access Manager (RAM)			Disable Access Specify Delegated Administrator View Delegated Administrator
Resource Formation Stack Set service (RF)			Enable Access Specify Delegated Administrator View Delegated Administrator
Multi account resource configurations for config (Config)	Access enabled	Mar 27, 2023 18:05:26 GMT+08:00	Disable Access Specify Delegated Administrator View Delegated Administrator
Sec Master (SecMaster)	Access disabled	--	Enable Access Specify Delegated Administrator View Delegated Administrator

----End

Configuring an OBS Bucket Policy

NOTE

If you use a **Public Read and Write** bucket policy, any user can read, write, and delete objects in the OBS bucket, and you can skip this step.

To store resource change notifications and resource snapshots in an OBS bucket, you need to configure one when configuring the resource recorder. If no OBS bucket is available, **create one** first.

In this scenario, you need to set a bucket policy allowing organization members to dump their resource data into the specified OBS bucket. The following procedure shows how to configure such a bucket policy:

Step 1 Log in to the management console with the authorizing account and go to the OBS console.

The authorizing account is the account to which the OBS bucket belongs.

Step 2 Grant member accounts related OBS permissions based on **Creating a Custom Bucket Policy (JSON View)**.

An example bucket policy is provided here to show how to allow member accounts to store data into a specific object or folder in an OBS bucket. You need to configure the following parameters in a bucket policy:

- **${account_id}**: member account IDs (domain_id). Use commas (,) to separate multiple domain IDs.
- **${agency_name}**: the name of the custom IAM agency For details about how to create an IAM agency, see **Cloud Service Agency**. Set the authorization object to Config in the agency.
- **${bucket_name}**: the name of an OBS bucket
- **${folder_name}**: the name of a folder in the OBS bucket If you do not need to specify a folder or object in an OBS bucket, you do not need to configure this parameter.

```
{
  "Statement": [
    {
      "Sid": "org-bucket-policy",
      "Effect": "Allow",
      "Principal": {
        "ID": [
          "domain/${account_id}:agency/${agency_name}"
        ]
      },
      "Action": [
        "PutObject"
      ],
      "Resource": [
        "${bucket_name}/${folder_name}/RMSLogs/*/Snapshot/*",
        "${bucket_name}/${folder_name}/RMSLogs/*/Notification/*"
      ]
    }
  ]
}
```

NOTE

If you need to store resource change notifications and snapshots in an OBS bucket encrypted with KMS, you need to set permissions for the KMS key to be used across member accounts. For details, see **Storing Resource Change Notifications and Resource Snapshots to an Encrypted OBS Bucket**. Specify IDs of member accounts (domain_id) as the pending authorization accounts

----End

Configure an SMN Topic Policy

To send resource change notifications, you need to configure an SMN topic when configuring the resource recorder. If no SMN topic is available, **create one** first. After you create a topic, you must **add subscriptions** and **request subscription confirmation**.

In this scenario, you need to set a topic access policy allowing organization members to send notifications using this topic.

Step 1 Log in to the management console with the authorizing account and go to the SMN console.

The authorizing account is the account to which the SMN topic belongs.

Step 2 Grant member accounts topic permissions based on **Configuring Topic Policies**.

Select **Specific user accounts** for **Users who can publish messages to this topic** and enter member account IDs.

If an organization member is not granted the required permissions, they cannot receive resource change notifications sent by Config.

----End

Creating an RFS Resource Stack Set

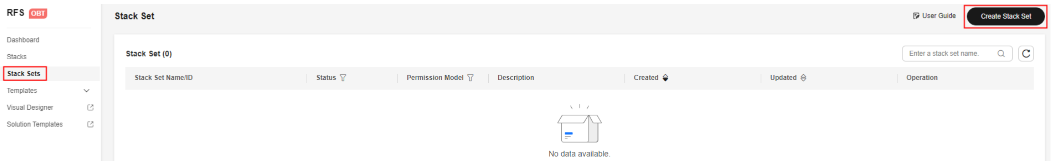
Step 1 Log in to the management console as an organization administrator.

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

Step 3 In the navigation pane on the left, choose **Stack Sets**.

Step 4 In the upper right corner, click **Create Stack Set**.

Figure 2-10 Creating a stack set



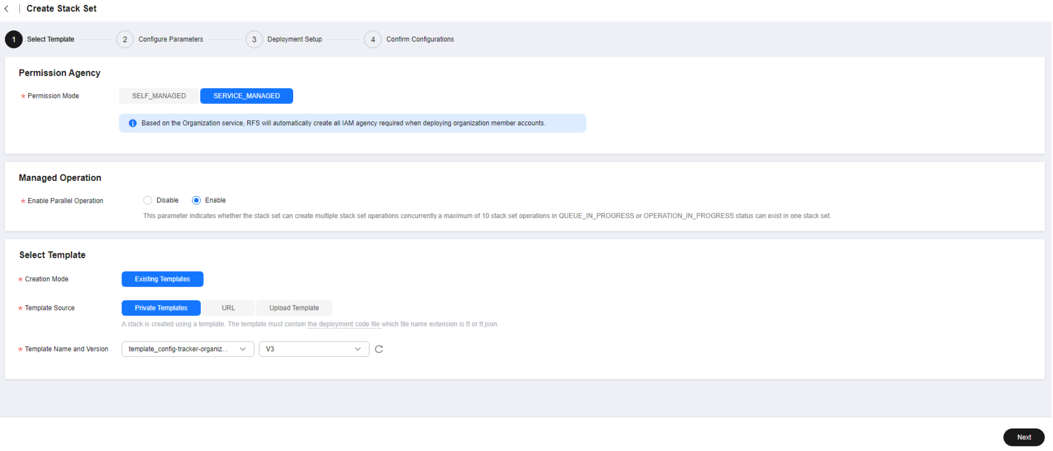
Stack Set Name/ID	Status	Permission Model	Description	Created	Updated	Operation

No data available.

Step 5 On the **Select Template** page, configure required parameters and click **Next**.

- Select **SERVICE_MANAGED** for **Permission Mode**.
- Select **Enable** or **Disable** for **Enable Parallel Operation**. You are advised to enable parallel operations for faster stack running.
- Select a template source as needed. For details about template content, see **Example Terraform Template**

Figure 2-11 Select Template



Permission Agency

* Permission Mode: SELF_MANAGED [✓ SERVICE_MANAGED]

Based on the Organization service, RFS will automatically create all IAM agency required when deploying organization member accounts.

Managed Operation

* Enable Parallel Operation: ○ Disable ● Enable

This parameter indicates whether the stack set can create multiple stack set operations concurrently.a maximum of 10 stack set operations in QUEUE_IN_PROGRESS or OPERATION_IN_PROGRESS status can exist in one stack set.

Select Template

* Creation Mode: [✓ Existing Templates]

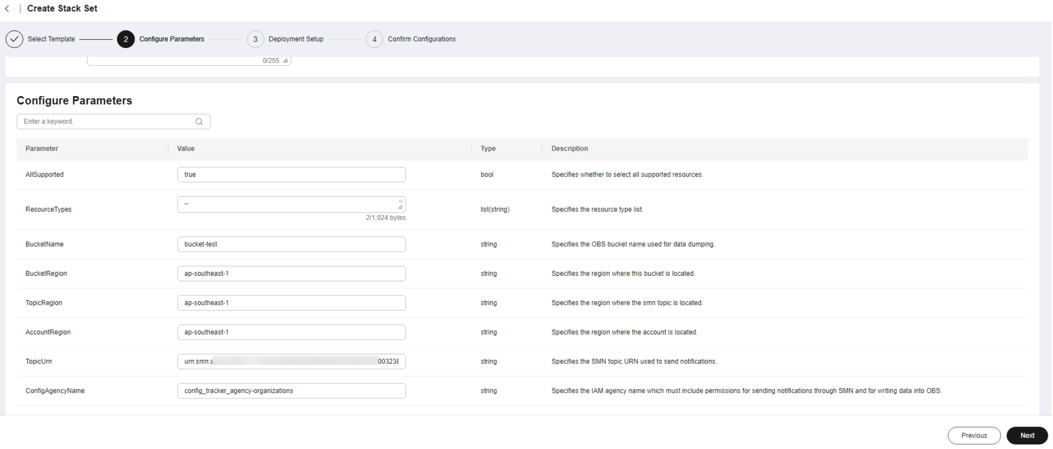
* Template Source: [✓ Private Templates] URL Upload Template

A stack is created using a template. The template must contain the deployment code file which file name extension is tf or tf.json.

* Template Name and Version: template_config-tracker-organiz... V3

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

Figure 2-12 Configure Parameters



Configure Parameters

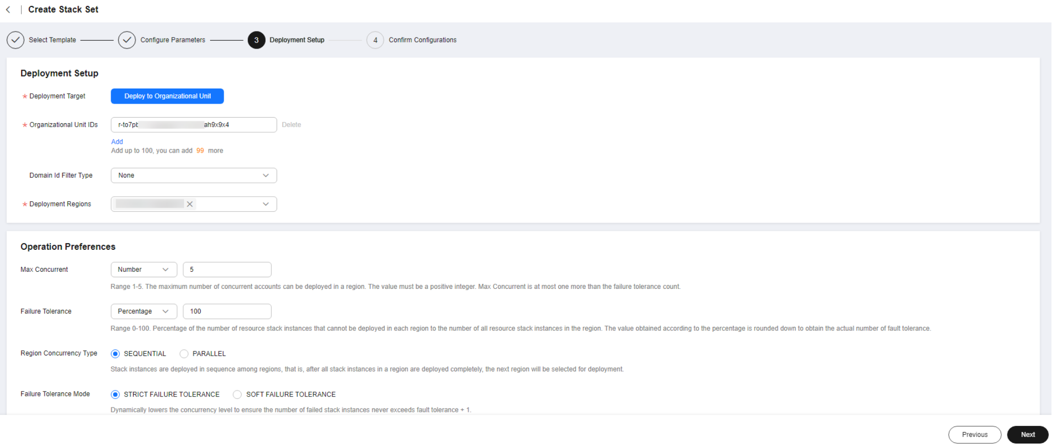
Parameter	Value	Type	Description
AllSupported	true	bool	Specifies whether to select all supported resources.
ResourceTypes	--	list(string)	Specifies the resource type list.
BucketName	bucket-test	string	Specifies the OBS bucket name used for data dumping.
BucketRegion	ap-southeast-1	string	Specifies the region where this bucket is located.
TopicRegion	ap-southeast-1	string	Specifies the region where the smn topic is located.
AccountRegion	ap-southeast-1	string	Specifies the region where the account is located.
TopicUrn	urn:smn:a [redacted] 003238	string	Specifies the SMN topic URN used to send notifications.
ConfigAgencyName	config_tracker_agency-organizations	string	Specifies the IAM agency name which must include permissions for sending notifications through SMN and for writing data into OBS.

- **Stack Set Name**: You can use a default or custom stack set name. Stack set names must be unique.

- **Configure Parameters**
  - **AllSupported**: whether to record all resource types supported by Config. Possible values are true or false. This parameter is mandatory.
  - **ResourceTypes**: list of resource types. This parameter is optional. If **AllSupported** is set to false, you need to specify specific resource types, for example, **vpc.vpcs** and **rds.instances**.
  - **BucketName**: the name of the specified OBS bucket. This parameter is mandatory. The value must be of string type.
  - **BucketRegion**: the region where the specified OBS bucket is deployed. This parameter is mandatory. The value must be of string type.
  - **AccountRegion**: the subsidiary website of Huawei Cloud where member accounts are registered. Possible values include **cn-north-4** (Chinese mainland website) and **ap-southeast-1** (international website).
  - **TopicUrn**: SMN topic URN. This parameter is mandatory. The value must be of string type.
  - **TopicRegion**: the region where the specified SMN topic is deployed. This parameter is mandatory. The value must be of string type.
  - **ConfigAgencyName**: IAM agency name. This parameter is mandatory. The value must be of string type. The agency must contain permissions for the resource recorder to call SMN to send notifications and write data into an OBS bucket.

Step 7 On the **Deployment Setup** page, configure required parameters based on the following picture and click **Next**.

Figure 2-13 Deployment Setup



Create Stack Set

Select Template — Configure Parameters — 3 Deployment Setup — 4 Confirm Configurations

Deployment Setup

* Deployment Target: Deploy to Organizational Unit

* Organizational Unit IDs: r-to7pt[redacted]ah9x9x4 Delete

Add

Add up to 100, you can add 99 more

Domain Id Filter Type: None

* Deployment Regions: [redacted]

Operation Preferences

Max Concurrent: Number 5

Range 1-5. The maximum number of concurrent accounts can be deployed in a region. The value must be a positive integer. Max Concurrent is at most one more than the failure tolerance count.

Failure Tolerance: Percentage 100

Range 0-100. Percentage of the number of resource stack instances that cannot be deployed in each region to the number of all resource stack instances in the region. The value obtained according to the percentage is rounded down to obtain the actual number of fault tolerance.

Region Concurrency Type: ● SEQUENTIAL ○ PARALLEL

Stack instances are deployed in sequence among regions, that is, after all stack instances in a region are deployed completely, the next region will be selected for deployment.

Failure Tolerance Mode: ● STRICT FAILURE TOLERANCE ○ SOFT FAILURE TOLERANCE

Dynamically lowers the concurrency level to ensure the number of failed stack instances never exceeds fault tolerance + 1.

- **Deployment Setup**
  - **Organizational Unit IDs**: organization unit IDs. If the root unit ID is specified, the stack set is deployed in the entire organization.
  - **Domain Id Filter Type**: criterion for filtering accounts
  - **Deployment Regions**: The region where the resource stack set is deployed.
- **Operation Preferences**
  - **Max Concurrent**: You are advised to select **Number** and set the value to 5.

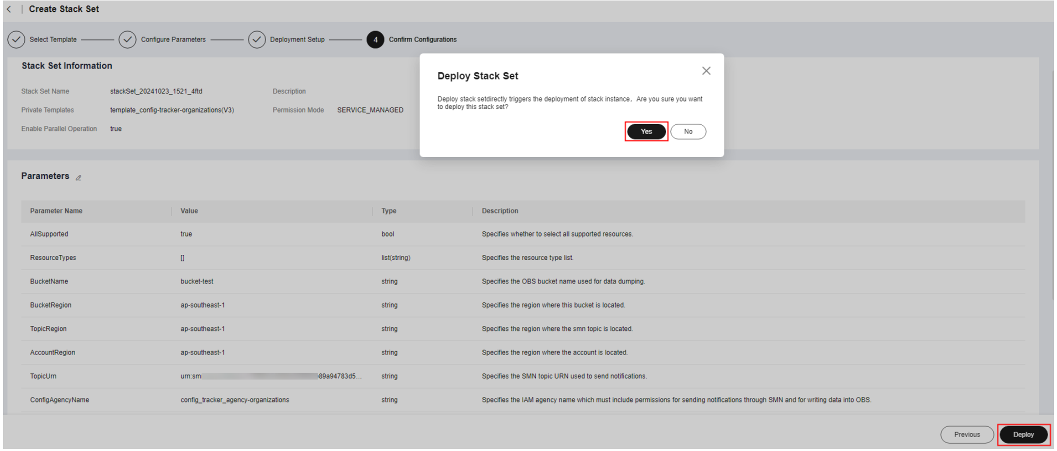
- **Fault Tolerance**: You are advised to select **Percentage** and set the value to **100**.
- **Region Concurrency Type** and **Failure Tolerance Mode**: Configure them as prompted.

Step 8 On the **Confirm Configurations** page, confirm the configurations and click **Deploy**.

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

The stack set will deploy a stack instance to each specified member account, and the resource recorder in each member account will be enabled and configured based on the Terraform template.

Figure 2-14 Deploying a resource stack set



Stack Set Information

Stack Set Name stackSet_20241023_1521_4ftd
Description
Private Templates template_config-tracker-organizations(V3)
Permission Mode SERVICE_MANAGED
Enable Parallel Operation true

Deploy Stack Set

Deploy stack setdirectly triggers the deployment of stack instance。Are you sure you want to deploy this stack set?

Parameters

Parameter Name	Value	Type	Description
AllSupported	true	bool	Specifies whether to select all supported resources.
ResourceTypes	[]	list(string)	Specifies the resource type list.
BucketName	bucket-test	string	Specifies the OBS bucket name used for data dumping.
BucketRegion	ap-southeast-1	string	Specifies the region where this bucket is located.
TopicRegion	ap-southeast-1	string	Specifies the region where the smn topic is located.
AccountRegion	ap-southeast-1	string	Specifies the region where the account is located.
TopicUrn	urn:sm[redacted]89a94783d5...	string	Specifies the SMN topic URN used to send notifications.
ConfigAgencyName	config_tracker_agency-organizations	string	Specifies the IAM agency name which must include permissions for sending notifications through SMN and for writing data into OBS.

NOTE

Organization members can disable and modify their resource recorders at any time. An organization administrator can also **modify** or **delete** a resource stack set at any time. After a stack set is deleted, the resource recorder in the deployed member account will be disabled.

----End

Example Terraform Template

You can create a private RFS template based on the following example or save this example template as a local .tf file and update this file to create a resource stack set as needed.

```
terraform {
  required_providers {
    huaweicloud = {
      source  = "huawei.com/provider/huaweicloud"
      version = ">=1.49.0"
    }
  }
}

provider "huaweicloud" {
}

variable "AllSupported" {
  description = "Specifies whether to select all supported resources."
  type        = bool
  default     = true

  validation {
    condition     = can(regex("^(true|false)$", var.AllSupported))
    error_message = "Must be true or false."
  }
}

variable "ResourceTypes" {
  description = "Specifies the resource type list. "
  type        = list(string)
  default     = []
}

variable "BucketName" {
  description = "Specifies the OBS bucket name used for data dumping."
  type        = string
}

variable "BucketRegion" {
  description = "Specifies the region where this bucket is located."
  type        = string
}

variable "TopicRegion" {
  description = "Specifies the region where the smn topic is located."
  type        = string
}

variable "AccountRegion" {
  description = "Specifies the region where the account is located."
  type        = string
}


variable "TopicUrn" {
  description = "Specifies the SMN topic URN used to send notifications."
  type        = string
}

variable "ConfigAgencyName" {
  description = "Specifies the IAM agency name which must include permissions for sending notifications
through SMN and for writing data into OBS."
  type        = string
}

data "huaweicloud_identity_projects" "CurrentAccountProject" {
  name = var.AccountRegion
}

resource "huaweicloud_identity_agency" "identity_agency" {
  name                  = var.ConfigAgencyName
  delegated_service_name = "op_svc_eps"
  all_resources_roles = ["SMN Administrator", "OBS Administrator", "KMS Administrator"]
}

resource "huaweicloud_rms_resource_recorder" "ConfigRecorder" {
  agency_name = var.ConfigAgencyName

  selector {
    all_supported  = var.AllSupported
    resource_types = var.ResourceTypes
  }

  obs_channel {
    bucket = var.BucketName
    region = var.BucketRegion
  }

  smn_channel {
    region = var.TopicRegion
    topic_urn = var.TopicUrn
    project_id = data.huaweicloud_identity_projects.CurrentAccountProject.projects[0].id
  }
  depends_on = [huaweicloud_identity_agency.identity_agency]
}
```

2.4 Notifications

Notifications of your resource changes will be sent to the SMN topic subscribers 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, see **Simple Message Notification User Guide**.

Config sends notifications when:

- Resources are created, modified, or deleted.
- Resource relationships change.
- Resource change notifications are saved.
- Resource snapshots are saved.

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

2.5 Storing Resource Snapshots

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

The path of in an OBS bucket where the resource recorder stores your data takes the form of **${bucket_name}/${bucket_prefix}/RMSLogs/${account_id}/Snapshot/${year}/${month}/*** The fields before each slash in the path indicate different layers of folders, and ***** indicates the name of a file. You can go to the **Objects** page on the OBS console and find your resource snapshots based on the paths.

The name of a resource snapshot file consists of the account ID, storage file type, ID of the region where the OBS bucket resides, storage time, randomly generated character string, and sequence number of the file. Each snapshot file can contain information of up to 2,000 resources. If you have more than 2,000 resources, there will be more than one files, and the name of each file will contain a sequence number (such as part-1). If you have less than 2,000 resources, there will be no sequence number in the file name. **.json.gz** indicates that the file is stored as a JSON package.

The following shows an example file name:
0926901ef980f2150fbdc001fdd23e80_Snapshot_me-east-1_ResourceSnapshot_2024-07-22T221441Z_90decead-b69b-4522-a090-657d8c299d40_part-1.json.gz.

For more details, see **Listing Objects**.

NOTE

A resource is in either of the two states: **In use** and **Deleted**. The snapshots of resources that are in the **Deleted** state will not be stored.

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

2.6 Storing Resource Change Notifications

After you enable the resource recorder and specify an SMN topic and an OBS bucket, Config stores your resource change notifications to the OBS bucket every 6 hours. If no topics are available, you need to create a topic, add subscription endpoints, and request subscription confirmations for the topic.

The path of in an OBS bucket where the resource recorder stores your resource change notifications takes the form of **${bucket_name}/${bucket_prefix}/RMSLogs/${account_id}/Notification/${year}/${month}/*** The fields before each slash in the path indicate different layers of folders, and ***** indicates the name of a file. You can go to the **Objects** page on the OBS console and find your resource change notification files based on the paths.

The name of the file for storing your resource change notifications consists of the account ID, storage file type, ID of the region where the OBS bucket resides, service type, resource type, and storage duration. Each file contains change notifications of only one type of resource. **.json.gz** indicates that the file is stored as a JSON package.

The following shows an example name of a resource change notification file: 0926901ef980f2150fbdc001fdd23e80_Notification_me-east-1_NotificationChunk_OBS_BUCKETS_2024-07-24T214735Z_2024-07-24T214759Z.json.gz

For more details, see **Listing Objects**.

For details, see **Simple Message Notification User Guide**.

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

2.7 Resource Recorder Event Monitoring

Event monitoring integrates Cloud Eye capabilities to enable you to query events and receive alarms when there are unexpected events.

Event monitoring is enabled by default. For details about how to view event details or perform other operations, see **Viewing Events** and **Creating an Alarm Rule to Monitor an Event**.

NOTE

Currently, Config only supports event monitoring in the **AP-Singapore** region.

The following table lists Config events supported by event monitoring.

Table 2-1 Supported Config events

Source	Event	Level	Description	Suggestion	Impact
SYS.RMS	Exporting resource snapshots failed	Major	Exporting resource snapshots to OBS failed.	You can check OBS bucket permissions.	Resource changes cannot be recorded.
SYS.RMS	Resource snapshots exported	Informational	Resource snapshots have been exported to OBS.	None	None
SYS.RMS	Exporting resource changes failed	Major	Exporting resource change records to OBS failed.	You can check OBS bucket permissions.	Resource changes cannot be recorded.
SYS.RMS	Resource changes exported	Informational	Resource change records have been exported to OBS.	None	None
SYS.RMS	Synchronizing resource changes failed	Major	Synchronizing resource change notifications to SMN failed.	You can check SMN topic permissions.	Customers will not be notified of resource relationship changes through SMN.
SYS.RMS	Resource change notifications synchronized	Informational	Resource change notifications have been synchronized to SMN.	None	None

Source	Event	Level	Description	Suggestion	Impact
SYS.RMS	Synchronizing notifications of resource relationship changes failed	Major	Synchronizing notifications of resource relationship changes to SMN failed.	You can check SMN topic permissions.	Customers will not be notified of resource relationship changes through SMN.
SYS.RMS	Notifications of resource relationship changes synchronized	Informational	Notifications of resource relationship changes have been synchronized to SMN.	None	None

For details about resource compliance events supported by event monitoring, see **Table 3-245**.

3 Resource Compliance

3.1 Overview

Overview

You can create a rule to evaluate your resource compliance. When creating a rule, you need to select **a built-in policy** or a custom policy, specify a monitoring scope, and specify the **trigger type**. Evaluation results are provided for you to check resource compliance.

If you are an organization administrator or a delegated administrator of Config, you can also add organization rules and deploy the rules to all member accounts (in the normal state) in your organization.

Config also allows you to remediate noncompliant resources with an RFS template or FunctionGraph function.

Restrictions and Limitations

- You can add up to 500 rules (including organization rules and rules included in conformance packages) with an account.
- The resource recorder must be enabled for adding, modifying, enabling, or triggering a rule. If the resource recorder is disabled, you can only view, disable, and delete rules.

  You cannot modify, disable, enable, or delete an individual organization rule that is deployed to your account or an individual rule of a conformance package. Only the organization administrator or delegated administrator of Config who creates the organization rule can modify or delete it. To modify or delete a rule of a conformance package, modify or delete the package. For details, see **Organization Rules** and **Conformance Packages**.
- The resource recorder must be enabled for adding, modifying, and triggering organization rules. If the resource recorder is disabled, you can only view and delete organization rules.
- The **Organization Rules** tab is inaccessible for an account that is not associated any organizations.

- To deploy an organization rule to a member, the member account must be in the normal state, and the resource recorder must be enabled for the member.
- Currently, you can only add remediation actions to non-organization rules that are not included in a conformance package.
- To create a remediation template with RFS, at least five stacks are required.
- You can only add one remediation action to each rule.
- To delete a rule, you need to delete the remediation action assigned and disable the rule.
- You can select up to 100 resources as remediation exceptions for each rule, however there is no limitation on how many resources the system will automatically add as remediation exceptions based on the remediation retry rules.

NOTICE

To evaluate resources with rules, you need to enable the resource recorder. Resource evaluation is subject to the following rules:

- If the resource recorder is disabled, no resources will be available for evaluation, but you can still view historical evaluation results.
- If the resource recorder is enabled and a monitoring scope is configured, only resources within the monitoring scope can be evaluated.

For details about how to enable and configure the resource recorder, see **Configuring the Resource Recorder**.

3.2 Rules

3.2.1 Adding a Rule with a Predefined Policy

Scenarios

This section describes how to add predefined rules.

Constraints and Limitations

- You can add up to 500 rules in an account.
- The resource recorder must be enabled for adding, modifying, enabling, or triggering a rule. If the resource recorder is disabled, you can only view, disable, and delete rules.

NOTICE

To evaluate resources with rules, you need to enable the resource recorder. Resource evaluation is subject to the following rules:

- If the resource recorder is disabled, no resources will be available for evaluation. You can still view historical evaluation results.
- If the resource recorder is enabled and a monitoring scope is configured, only resources within the monitoring scope can be evaluated.

For details about how to enable and configure the resource recorder, see **Configuring the Resource Recorder**.

Procedure

Step 1 Log in to the management console.

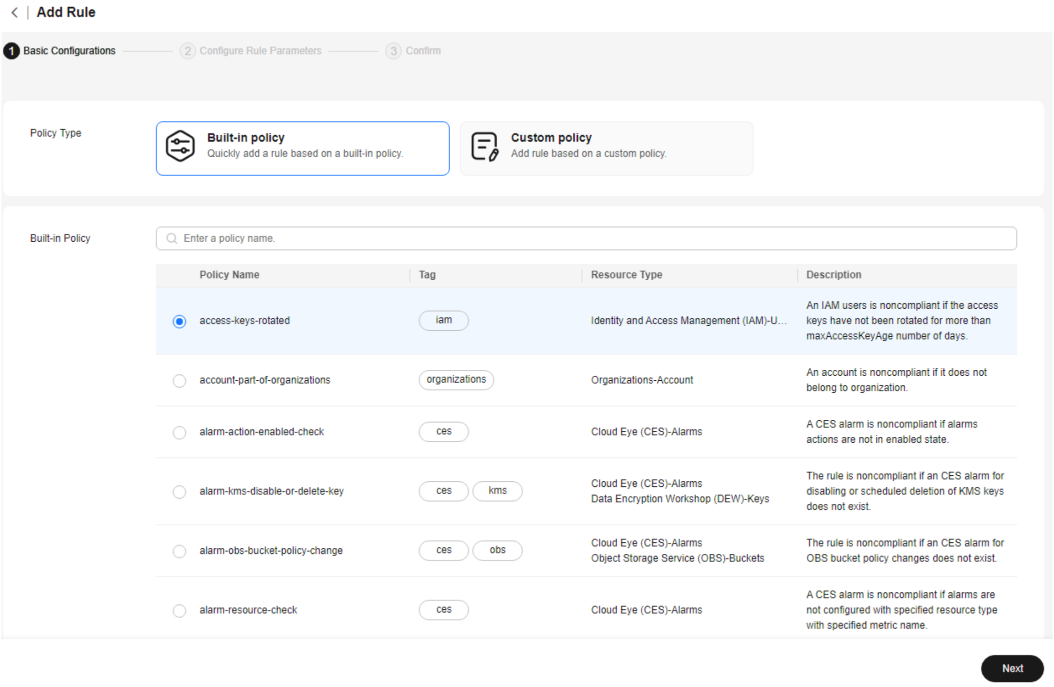
Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

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

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

Step 5 Configure basic details, and click **Next**.

Figure 3-1 Basic Configurations



< | Add Rule

1 Basic Configurations — 2 Configure Rule Parameters — 3 Confirm

Policy Type: ● Built-in policy — Quickly add a rule based on a built-in policy. ○ Custom policy — Add rule based on a custom policy.

Built-in Policy: Enter a policy name.

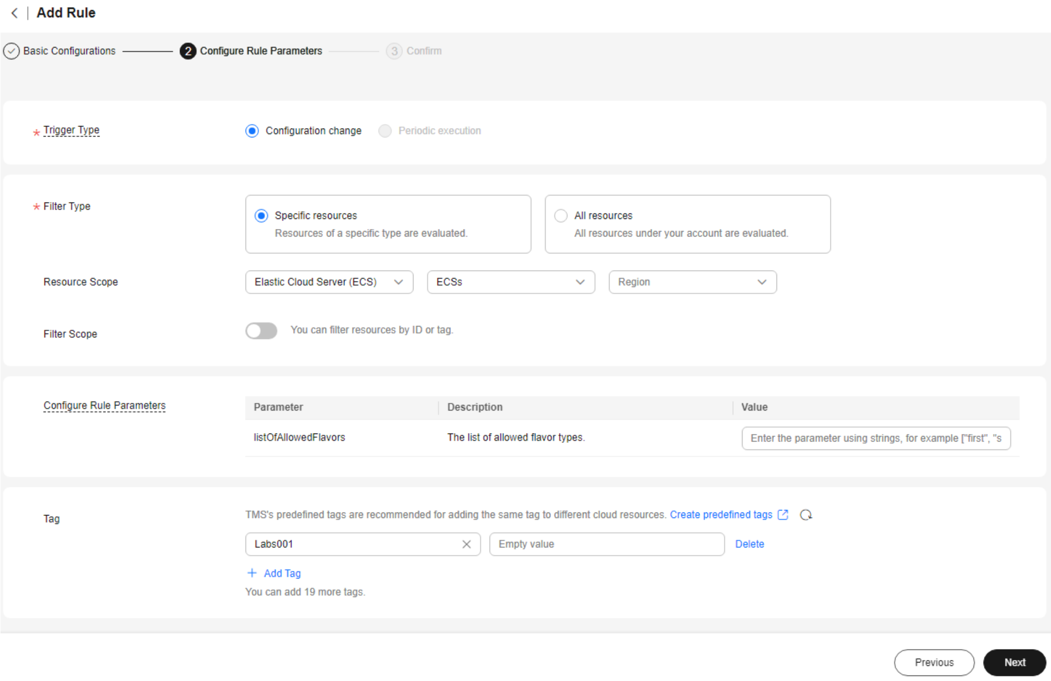
	Policy Name	Tag	Resource Type	Description
●	access-keys-rotated	iam	Identity and Access Management (IAM)-U...	An IAM users is noncompliant if the access keys have not been rotated for more than maxAccessKeyAge number of days.
○	account-part-of-organizations	organizations	Organizations-Account	An account is noncompliant if it does not belong to organization.
○	alarm-action-enabled-check	ces	Cloud Eye (CES)-Alarms	A CES alarm is noncompliant if alarms actions are not in enabled state.
○	alarm-kms-disable-or-delete-key	ces kms	Cloud Eye (CES)-Alarms Data Encryption Workshop (DEW)-Keys	The rule is noncompliant if an CES alarm for disabling or scheduled deletion of KMS keys does not exist.
○	alarm-obs-bucket-policy-change	ces obs	Cloud Eye (CES)-Alarms Object Storage Service (OBS)-Buckets	The rule is noncompliant if an CES alarm for OBS bucket policy changes does not exist.
○	alarm-resource-check	ces	Cloud Eye (CES)-Alarms	A CES alarm is noncompliant if alarms are not configured with specified resource type with specified metric name.

Table 3-1 Parameters of basic configurations

Parameter	Description
Policy Type	Select **Built-in policy**. Built-in policies are provided by Config. You can select a built-in policy to quickly add a rule. You can also search for a built-in policy by policy name or tag. For details, see **Built-In Policies**.
Rule Name	By default, the rule name is consistent with the predefined policy name. Rule names must be unique. A rule name can contain digits, letters, underscores (_), and hyphens (-) and cannot exceed 64 characters.
Description	By default, the rule description is the same as the selected predefined policy description. You can also customize the rule description. A rule description can contain any types of characters and cannot exceed 512 characters.

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

Figure 3-2 Configure Rule Parameters



Add Rule

Basic Configurations — 2 Configure Rule Parameters — 3 Confirm

* Trigger Type: ● Configuration change ○ Periodic execution

* Filter Type: ● Specific resources — Resources of a specific type are evaluated. ○ All resources — All resources under your account are evaluated.

Resource Scope: Elastic Cloud Server (ECS) | ECSs | Region

Filter Scope: You can filter resources by ID or tag.

Configure Rule Parameters

Parameter	Description	Value
listOfAllowedFlavors	The list of allowed flavor types.	Enter the parameter using strings, for example ["first", "s

Tag: TMS's predefined tags are recommended for adding the same tag to different cloud resources. Create predefined tags

Labs001 | Empty value | Delete

Add Tag

You can add 19 more tags.

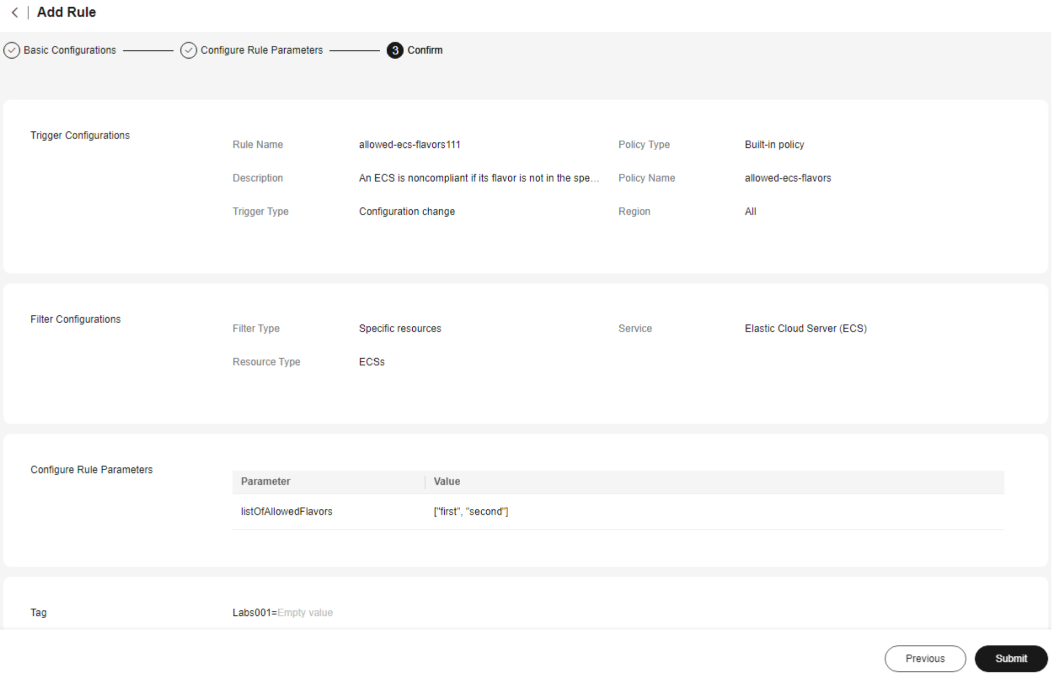
Table 3-2 Parameter descriptions

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. **NOTE** You cannot modify the **Trigger Type** of predefined policies. The **Trigger Type** varies depending on different predefined policies.
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**: The service that the resource belongs to. ● **Resource type**: The resource type ● **Region**: The region where the resource resides. **NOTE** ● You can specify a service and a resource type for **Resource Scope** only when **Trigger Type** is set to **Configuration change**. ● You can specify a region for **Resource Scope** when **Trigger Type** is set to **Periodic execution** and the resources are not of the account type. You can check more predefined policies on Config console or in **Predefined Policy List**.
(Optional) 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 optional for a rule whose trigger type is configuration change.
Execute Every	Indicates how often a rule is triggered. Available options: **1 hour**, **3 hours**, **6 hours**, **12 hours**, **24 hours**. This parameter is mandatory only when **Trigger Type** is set to **Periodic execution**.

Parameter	Description
Configure Rule Parameters	Parameters of a built-in policy. For example, if you select the **required-tag-check** policy, you need to specify a tag, so that resources that do not have the tag will be determined as noncompliant. Some default policies, such as **volumes-encrypted-check**, do not require **Configure Rule Parameters**.
Tag	Tag of the rule. To add a tag, click **Add Tag** and enter a tag key and a tag value. You can add up to 20 tags to a rule. ● A tag key cannot be empty. It can contain letters, digits, spaces, and special characters (_.:=+-@), but cannot start or end with a space or start with _sys_. A tag key can contain up to 128 characters. ● A tag value cannot be empty. It can contain letters, digits, spaces, and special characters (_.:=+-@), but cannot start or end with a space. A tag value can contain up to 255 characters.

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

Figure 3-3 Confirm



Trigger Configurations

Rule Name	allowed-ecs-flavors111	Policy Type	Built-in policy
Description	An ECS is noncompliant if its flavor is not in the spe...	Policy Name	allowed-ecs-flavors
Trigger Type	Configuration change	Region	All

Filter Configurations

Filter Type	Specific resources	Service	Elastic Cloud Server (ECS)
Resource Type	ECSs		

Configure Rule Parameters

Parameter	Value
listOfAllowedFlavors	["first", "second"]

Tag Labs001=Empty value

NOTE

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

----End

3.2.2 Adding a Custom Rule

Scenario

You can create custom rules with FunctionGraph if built-in policies cannot meet your resource audit requirements.

A custom policy is a function developed and published through **FunctionGraph**. Each custom rule is associated with a Function Graph function. Config reports events to the function. The function collects rule parameters and resource attributes from the events; evaluates whether your resources comply with the rule; and returns evaluation results using Open APIs of Config. Config sends events based on the trigger type (configuration changes or periodic) of a rule.

This section describes how to create a custom rule by performing the following two procedures:

1. **Creating a Function with FunctionGraph**
2. **Adding a Custom Rule**

Constraints and Limitations

- You can add up to 500 rules in an account.
- The resource recorder must be enabled for adding, modifying, enabling, or triggering a rule. If the resource recorder is disabled, you can only view, disable, and delete rules.

NOTICE

To evaluate resources with rules, you need to enable the resource recorder. Resource evaluation is subject to the following rules:

- If the resource recorder is disabled, no resources will be available for evaluation. You can still view historical evaluation results.
- If the resource recorder is enabled and a monitoring scope is configured, only resources within the monitoring scope can be evaluated.

For details about how to enable and configure the resource recorder, see **Configuring the Resource Recorder**.

Creating a Function with FunctionGraph

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page. In the service list that is displayed, under **Compute**, select **FunctionGraph**.

Step 3 In the navigation pane on the left, choose **Functions** > **Function List**.

Step 4 In the upper right corner, click **Create Function**. The **Create from scratch** tab is displayed by default.

Step 5 Set **Function Type** to **Event Function** and configure other parameters, including the function name and IAM agency.

The agency grants the function required permissions and must include the **rms:policyStates:update** permission.

Step 6 Click **Create Function**.

Step 7 In the code box, enter a function and click **Deploy**.

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

Step 8 Click **Configurations**, modify **Execution Timeout (s)** and **Memory (MB)** in the **Basic Settings** area as required. Configure **Concurrency**.

Step 9 Click **Save**.

For more 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**, complete related configurations and authorization, and click **Next**.

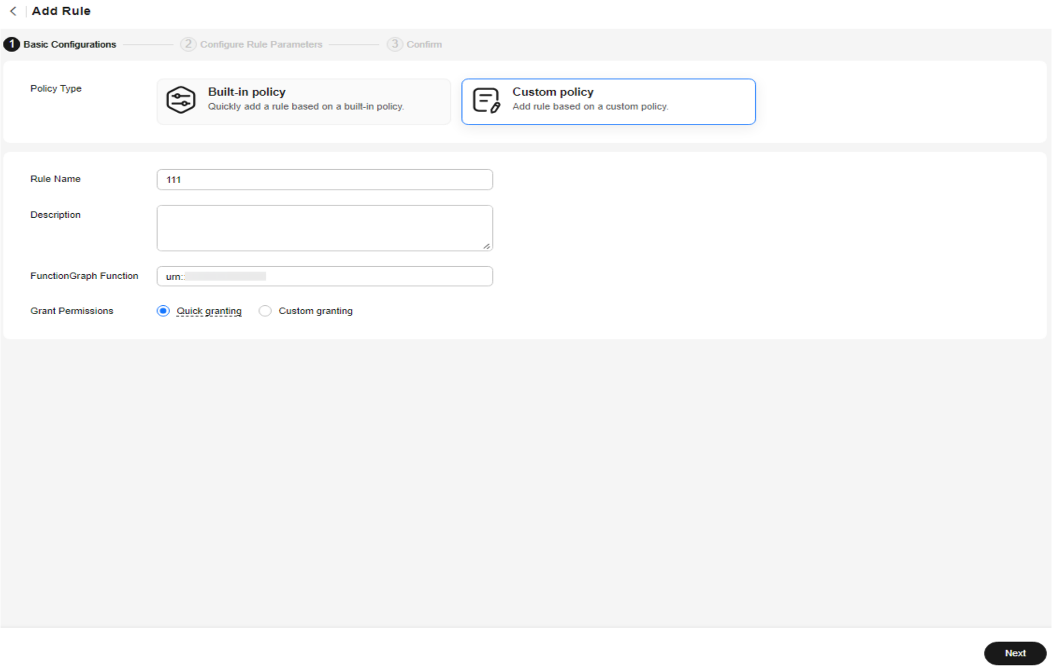
Table 3-3 Parameters of basic configurations

Parameter	Description
Policy Type	Select **Custom policy**. You can use custom policies to create rules.
Rule Name	The name of the rule. A rule name must be unique. A rule name can contain digits, letters, underscores (_), and hyphens (-) and cannot exceed 64 characters.
Description	A rule description can contain any types of characters and cannot exceed 512 characters.

Parameter	Description
FunctionGraph Function	The URN of the function. For details about how to create a FunctionGraph function, see **Creating a FunctionGraph Function for a Config Custom Policy**. **NOTE** You can use either of the following methods to obtain the URN of a function: - On the FunctionGraph console, choose **Functions** > **Function List** in the navigation pane on the left and click **Copy URN** in the **Operation** column for the target function. - Return to the FunctionGraph console, choose **Functions** > **Function List** in the navigation pane on the left, click the name of the target function, then obtain the function URN in the **Function Info** area.

Grant Permissions	This agency grants Config the read-only and call permissions of FunctionGraph. These permissions allow you to customize rules to query and send events to FunctionGraph functions.
	NOTE
	- **Quick granting**: Quickly grants you permissions of the **rms_custom_policy_agency** agency. The permissions ensure proper functioning of a custom rule and allow a custom rule to obtain and asynchronously execute a FunctionGraph function.
	- **Custom granting**: Allows you to create an agency using Identity and Access Management (IAM) and assign permissions. The agency must contain the permissions for calling and asynchronously executing FunctionGraph functions. The authorization object must be Config. The following shows an authorization example.
	`{`
	`    "Version": "1.1",`
	`    "Statement": [`
	`        {`
	`            "Effect": "Allow",`
	`            "Action": [`
	`                "functiongraph:function:invokeAsync",`
	`                "functiongraph:function:getConfig"`
	`            ]`
	`        }`
	`    ]`
	`}`
	For details about how to create an agency, see ***Identity and Access Management User Guide***.

Figure 3-4 Basic Configurations



< | Add Rule

1 Basic Configurations — 2 Configure Rule Parameters — 3 Confirm

Policy Type: Built-in policy (Quickly add a rule based on a built-in policy.) | Custom policy (Add rule based on a custom policy.)

Rule Name: 111

Description:

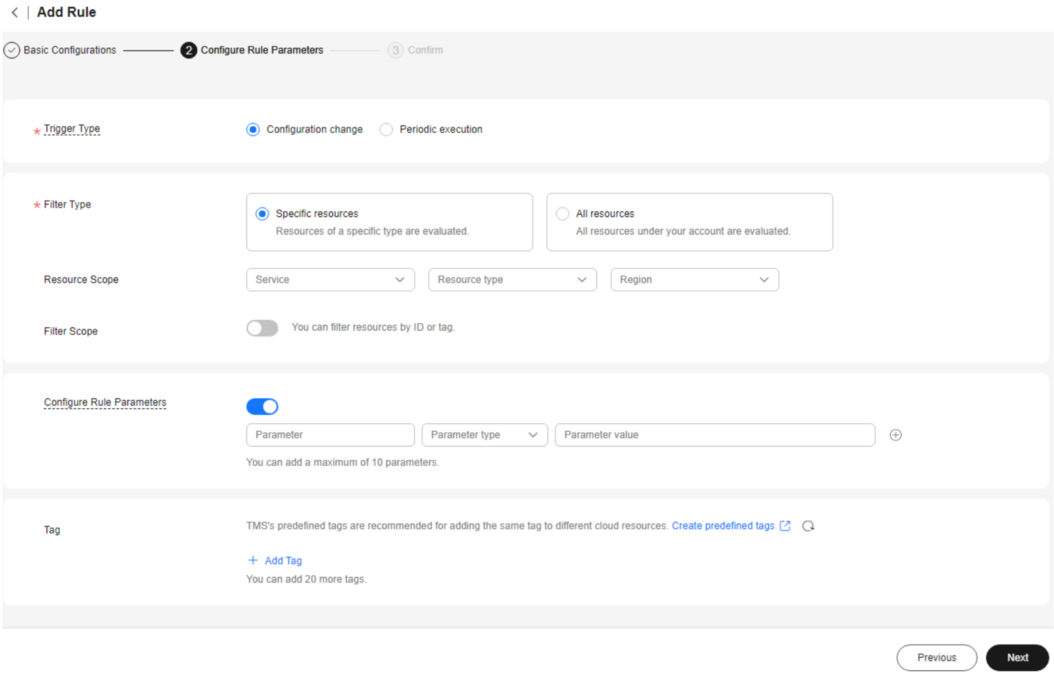
FunctionGraph Function: urn:

Grant Permissions: ● Quick granting ○ Custom granting

Next

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

Figure 3-5 Configure Rule Parameters



< | Add Rule

Basic Configurations — 2 Configure Rule Parameters — 3 Confirm

* Trigger Type: ● Configuration change ○ Periodic execution

* Filter Type: ● Specific resources (Resources of a specific type are evaluated.) ○ All resources (All resources under your account are evaluated.)

Resource Scope: Service | Resource type | Region

Filter Scope: You can filter resources by ID or tag.

Configure Rule Parameters: Parameter | Parameter type | Parameter value

You can add a maximum of 10 parameters.

Tag: TMS's predefined tags are recommended for adding the same tag to different cloud resources. Create predefined tags

+ Add Tag

You can add 20 more tags.

Previous Next

Table 3-4 Rule parameters

Parameter	Description
Trigger Type	The condition under which a rule will be triggered. Trigger types are as follows: ● **Configuration change**: A rule is triggered when there is a change in resource configurations. ● **Periodic execution**: A rule is triggered at a specific frequency.
Filter Type	The type of resources to be evaluated. Filter types are as follows: ● **Specific resources**: Resources of a specific type. ● **All resources**: All resources from your account. 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**: The service that the resource belongs to. ● **Resource type**: The resource type ● **Region**: The region where the resource resides. This parameter is mandatory only when **Trigger Type** is set to **Configuration change** and the **Filter Type** is set to **Specific resources**.
(Optional) 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 optional for a rule whose trigger type is configuration change.
Execute Every	How often a rule will be triggered. Available options: **1 hour**, **3 hours**, **6 hours**, **12 hours**, **24 hours**. This parameter is mandatory only when **Trigger Type** is set to **Periodic execution**.
Configure Rule Parameters	You can set up to 10 rule parameters for a custom rule.

Parameter	Description
Tag	Tag of the rule. To add a tag, click **Add Tag** and enter a tag key and a tag value. You can add up to 20 tags to a rule. ● A tag key cannot be empty. It can contain letters, digits, spaces, and special characters (_.:=+-@), but cannot start or end with a space or start with _sys_. Can contain a maximum of 128 characters. ● A tag value cannot be empty. It can contain letters, digits, spaces, and special characters (_.:=+-@), but cannot start or end with a space. A tag value can contain up to 255 characters.

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

NOTE

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

----End

3.2.3 Viewing a Rule

Scenario

After you add a rule, you can view all rules in the rule list and view evaluation results, tags, remediation, and configurations of a rule on the rule details page.

You can export all evaluation results. On the upper right corner of the rule details page, multiple buttons are provided for you to trigger, modify, enable, disable, or delete a rule. On the remediation tab, you can check remediation configurations. On the tag tab, you can edit rule tags.

NOTE

The resource recorder must be enabled for adding, modifying, enabling, or triggering a rule. If the resource recorder is disabled, you can only view, disable, and delete rules.

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.

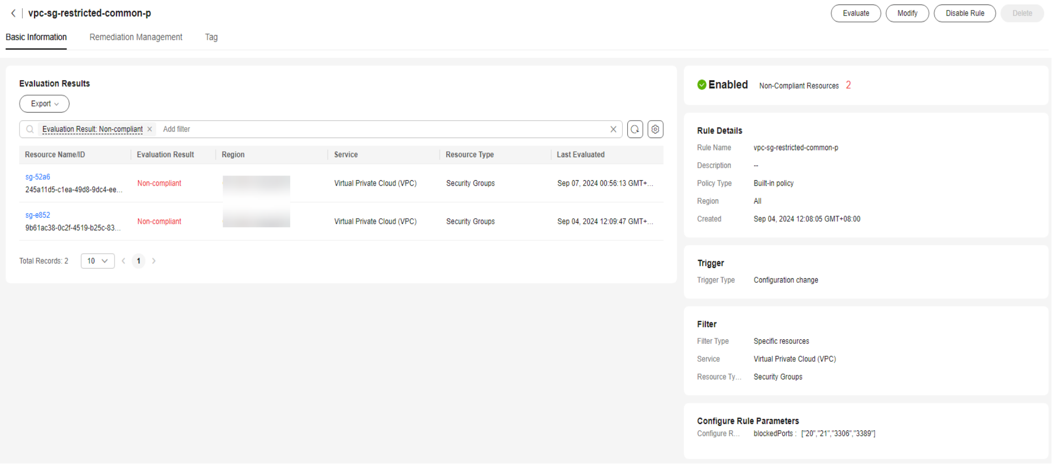
Step 5 Click the name of the target rule to go to the **Rule Details** page.

On the left of the **Basic Information** tab, evaluation results are displayed, and on the right, rule details are displayed. By default, noncompliant resources are displayed. Above the list, you can filter the resources by evaluation result, resource name, and resource ID. You can also export all evaluation results.

On the **Remediation Management** tab, you can view, edit, and delete remediation configurations and execute the remediation. You can also add and delete remediation exceptions.

On the tag tab, you can view and modify tags of a rule.

Figure 3-6 Rule details page



Resource Name/ID	Evaluation Result	Region	Service	Resource Type	Last Evaluated
sg-52a6 245a11d5-c1ea-49d8-9dc4-ee...	Non-compliant	[redacted]	Virtual Private Cloud (VPC)	Security Groups	Sep 07, 2024 00:56:13 GMT+...
sg-e852 9b61ac38-0c2f-4519-b25c-83...	Non-compliant	[redacted]	Virtual Private Cloud (VPC)	Security Groups	Sep 04, 2024 12:09:47 GMT+...

Total Records: 2 10 1

Enabled Non-Compliant Resources 2

Rule Details

Rule Name vpc-sg-restricted-common-p

Description --

Policy Type Built-in policy

Region All

Created Sep 04, 2024 12:08:05 GMT+08:00

Trigger

Trigger Type Configuration change

Filter

Filter Type Specific resources

Service Virtual Private Cloud (VPC)

Resource Ty... Security Groups

Configure Rule Parameters

Configure R... blockedPorts : ["20","21","3306","3389"]

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

3.2.4 Triggering a Rule

Scenarios

Rules can be triggered automatically or manually.

- **Automatic**
  - A rule will be automatically triggered after it is created.
  - A rule will be automatically triggered after it is updated.
  - A rule will be automatically triggered after it is enabled.
  - If the **Trigger type** is set to **Configuration change** for a rule, the rule will be automatically triggered when there is a change to the resources within the monitoring scope.

  - If the **Trigger Type** to **Periodic execution** for a rule, the rule will be automatically triggered at the configured frequency.
- **Manual**

  You can manually initiate rule evaluation at any time. For details, see **Procedure**.

Constraints and Limitations

- You can add up to 500 rules in an account.
- The resource recorder must be enabled for adding, modifying, enabling, or triggering a rule. If the resource recorder is disabled, you can only view, disable, and delete rules.

NOTICE

To evaluate resources with rules, you need to enable the resource recorder. Resource evaluation is subject to the following rules:

- If the resource recorder is disabled, no resources will be available for evaluation. You can still view historical evaluation results.
- If the resource recorder is enabled and a monitoring scope is configured, only resources within the monitoring scope can be evaluated.

For details about how to enable and configure the resource recorder, see **Configuring the Resource Recorder**.

Procedure

Step 1 Log in to the management console.

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

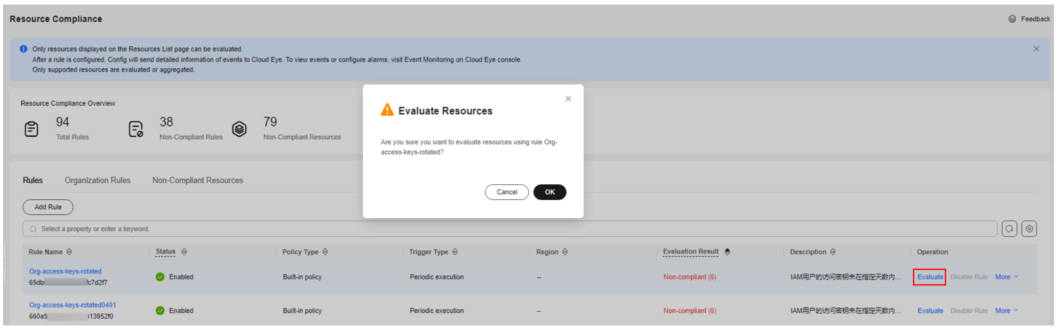
Step 3 In the navigation pane on the left, choose **Resource Compliance**.

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

Alternatively, you can click **Evaluate** in the upper right corner of the rule details page.

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

Figure 3-7 Manually triggering a rule



Only resources displayed on the Resources List page can be evaluated.
After a rule is configured, Config will send detailed information of events to Cloud Eye. To view events or configure alarms, visit Event Monitoring on Cloud Eye console.
Only supported resources are evaluated or aggregated.

Are you sure you want to evaluate resources using rule Org-access-keys-rotated?

Rule Name	Status	Policy Type	Trigger Type	Region	Evaluation Result	Description	Operation
Org-access-keys-rotated 65db[redacted]c7d2f7	Enabled	Built-in policy	Periodic execution	--	Non-compliant (6)	IAM用户的访问密钥未在指定天数内...	Evaluate Disable Rule More
Org-access-keys-rotated0401 660a5[redacted]13952f0	Enabled	Built-in policy	Periodic execution	--	Non-compliant (6)	IAM用户的访问密钥未在指定天数内...	Evaluate Disable Rule More

----End

3.2.5 Editing 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 through the rule list.

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

NOTE

- The resource recorder must be enabled for adding, modifying, enabling, or triggering a rule. If the resource recorder is disabled, you can only view, disable, and delete rules.
- You cannot modify, disable, enable, or delete an individual organization rule that is deployed to your account or an individual rule of a conformance package. Only the organization administrator or delegated administrator of Config who creates the organization rule can modify or delete it. To modify or delete a rule of a conformance package, modify or delete the package. For details, see **Organization Rules** and **Conformance Packages**.

Disabling a Rule

Step 1 Log in to the management console.

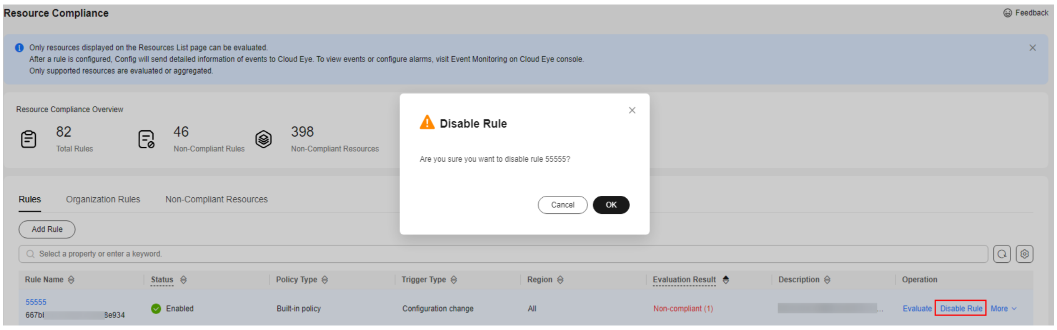
Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

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



Resource Compliance

Feedback

Only resources displayed on the Resources List page can be evaluated.
After a rule is configured, Config will send detailed information of events to Cloud Eye. To view events or configure alarms, visit Event Monitoring on Cloud Eye console.
Only supported resources are evaluated or aggregated.

Resource Compliance Overview

82 Total Rules

46 Non-Compliant Rules

398 Non-Compliant Resources

Disable Rule

Are you sure you want to disable rule 55555?

Cancel | OK

Rules | Organization Rules | Non-Compliant Resources

Add Rule

Select a property or enter a keyword.

Rule Name	Status	Policy Type	Trigger Type	Region	Evaluation Result	Description	Operation
55555 667bl[redacted]8e934	Enabled	Built-in policy	Configuration change	All	Non-compliant (1)	[redacted]...	Evaluate Disable Rule More

----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**.

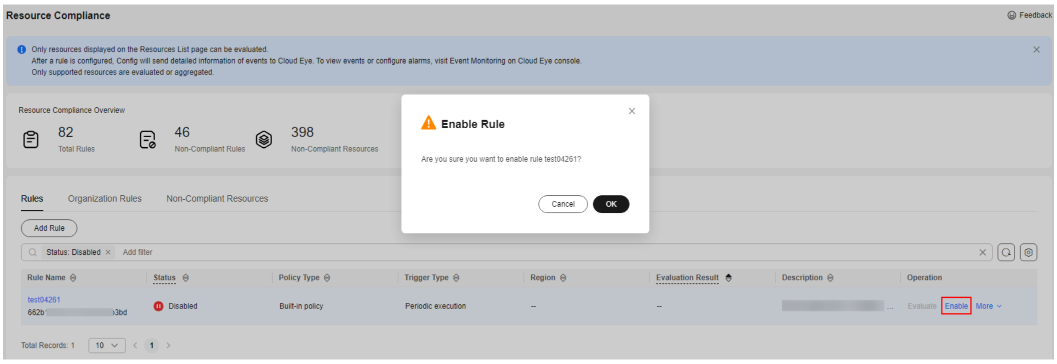
Step 4 On the **Rules** tab, locate a target rule and click **Enable** in the **Operation** column.

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

NOTE

After a rule is enabled, it will be automatically triggered immediately.

Figure 3-9 Enabling a rule



Resource Compliance

Feedback

Only resources displayed on the Resources List page can be evaluated.
After a rule is configured, Config will send detailed information of events to Cloud Eye. To view events or configure alarms, visit Event Monitoring on Cloud Eye console.
Only supported resources are evaluated or aggregated.

Resource Compliance Overview

82 Total Rules

46 Non-Compliant Rules

398 Non-Compliant Resources

Enable Rule

Are you sure you want to enable rule test04261?

Cancel | OK

Rules | Organization Rules | Non-Compliant Resources

Add Rule

Status: Disabled × Add filter

Rule Name	Status	Policy Type	Trigger Type	Region	Evaluation Result	Description	Operation
test04261 662b[redacted]3bd	Disabled	Built-in policy	Periodic execution	--	--	[redacted]...	Evaluate Enable More

Total Records: 1 10 < 1 >

----End

Modifying a Rule

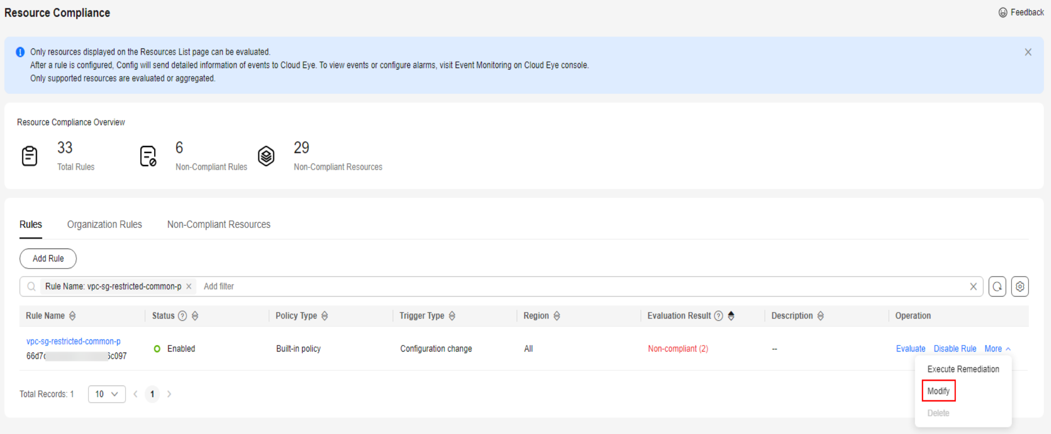
Step 1 Log in to the management console.

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



Resource Compliance

Only resources displayed on the Resources List page can be evaluated.
After a rule is configured, Config will send detailed information of events to Cloud Eye. To view events or configure alarms, visit Event Monitoring on Cloud Eye console.
Only supported resources are evaluated or aggregated.

Resource Compliance Overview

33 Total Rules
6 Non-Compliant Rules
29 Non-Compliant Resources

Rule Name: vpc-sg-restricted-common-p

Rule Name	Status	Policy Type	Trigger Type	Region	Evaluation Result	Description	Operation
vpc-sg-restricted-common-p 66d7[redacted]c097	Enabled	Built-in policy	Configuration change	All	Non-compliant (2)	--	Evaluate Disable Rule More

Total Records: 1

Step 5 On **Basic Configurations** page, modify the rule description and name and click **Next**.

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

The configuration items that you can modify vary for different policies.

- **Filter Type**: Can be modified when **Trigger Type** is set to **Configuration change**
- **Resource Scope**: Can be modified when **Trigger Type** is set to **Configuration change**
- **Filter Scope**: Can be modified when **Trigger Type** is set to **Configuration change**.
- **Execute Every**: Can be modified when **Trigger Type** is set to **Periodic execution**.
- **Configure Rule Parameters**: For a rule created with a predefined policy, you can only modify the values of parameters for **Configure Rule Parameters**. For a custom rule, you can add, delete, and modify related parameters.

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

NOTE

After a rule is modified, it will be automatically triggered.

----End

Deleting a Rule

To delete a rule, you need to disable the rule first. If a rule has remediation configured, you also need to delete the remediation.

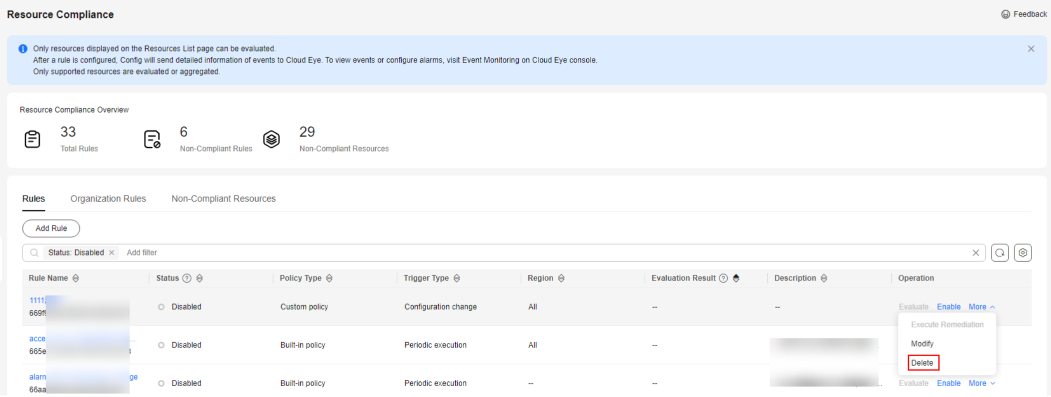
Step 1 Log in to the management console.

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



Resource Compliance

Feedback

Only resources displayed on the Resources List page can be evaluated.
After a rule is configured, Config will send detailed information of events to Cloud Eye. To view events or configure alarms, visit Event Monitoring on Cloud Eye console.
Only supported resources are evaluated or aggregated.

Resource Compliance Overview

33 Total Rules

6 Non-Compliant Rules

29 Non-Compliant Resources

Rules | Organization Rules | Non-Compliant Resources

Add Rule

Status: Disabled × Add filter

Rule Name	Status	Policy Type	Trigger Type	Region	Evaluation Result	Description	Operation
1111[redacted] 669f[redacted]	○ Disabled	Custom policy	Configuration change	All	--	--	Evaluate Enable More
acce[redacted] 665e[redacted]	○ Disabled	Built-in policy	Periodic execution	All	--	[redacted]	
alarn[redacted]ge 66aa[redacted]	○ Disabled	Built-in policy	Periodic execution	--	--	[redacted]	Evaluate Enable More

Step 5 Click **OK**.

----End

3.2.6 Example Custom Rules

3.2.6.1 Example Functions (Python)

Example Function of 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 time
import http.client
from huaweicloudsdkcore.auth.credentials import GlobalCredentials
from huaweicloudsdkcore.exceptions.exceptions import ConnectionException
from huaweicloudsdkcore.exceptions.exceptions import RequestTimeoutException
from huaweicloudsdkcore.exceptions.exceptions import ServiceResponseException
from huaweicloudsdkconfig.v1.region.config_region import ConfigRegion
from huaweicloudsdkconfig.v1.config_client import ConfigClient
from huaweicloudsdkconfig.v1 import PolicyResource, PolicyStateRequestBody
from huaweicloudsdkconfig.v1 import UpdatePolicyStateRequest

'''
The evaluation result of a rule will be either Compliant or NonCompliant.
In this example, if the vpcId of an ECS 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").get("value") else "NonCompliant"


def update_policy_state(context, domain_id, evaluation):
    auth = GlobalCredentials(
        ak=context.getSecurityAccessKey(),
        sk=context.getSecuritySecretKey(),
        domain_id=domain_id
    ).with_security_token(context.getSecurityToken())
    client = ConfigClient.new_builder() \
        .with_credentials(credentials=auth) \
        .with_region(region=ConfigRegion.value_of(region_id="cn-north-4")) \
        .build()

    try:
        response = client.update_policy_state(evaluation)
        return 200
    except ConnectionException as e:
        print("A connect timeout exception occurs while the Config performs some operations, exception: ",
e.error_msg)
        return e.status_code
    except RequestTimeoutException as e:
        print("A request timeout exception occurs while the Config performs some operations, exception: ",
e.error_msg)
        return e.status_code
    except ServiceResponseException as e:
        print("There is service error, exception: ", e.status_code, e.error_msg)
        return e.status_code


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

    request_body = UpdatePolicyStateRequest(PolicyStateRequestBody(
        policy_resource = PolicyResource(
            resource_id = resource.get("id"),
            resource_name = resource.get("name"),
            resource_provider = resource.get("provider"),
            resource_type = resource.get("type"),
            region_id = resource.get("region_id"),
            domain_id = domain_id
        ),
        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"),
        evaluation_time = event.get("evaluation_time"),
        evaluation_hash = event.get("evaluation_hash")
    ))

    for retry in range(5):
        status_code = update_policy_state(context, domain_id, request_body)
        if status_code == http.client.TOO_MANY_REQUESTS:
            print("TOO_MANY_REQUESTS: retry again")
            time.sleep(1)
        elif status_code == http.client.OK:
            print("Update policyState successfully.")
            break
        else:
            print("Failed to update policyState.")
            break
```

Example Function of Evaluations Triggered by Periodic Execution

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

```
import time
import http.client
from huaweicloudsdkcore.auth.credentials import GlobalCredentials
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkcore.exceptions.exceptions import ConnectionException
from huaweicloudsdkcore.exceptions.exceptions import RequestTimeoutException
from huaweicloudsdkcore.exceptions.exceptions import ServiceResponseException
from huaweicloudsdkconfig.v1.region.config_region import ConfigRegion
from huaweicloudsdkconfig.v1.config_client import ConfigClient
from huaweicloudsdkconfig.v1 import PolicyResource, PolicyStateRequestBody
from huaweicloudsdkconfig.v1 import UpdatePolicyStateRequest
from huaweicloudsdkiam.v3.region.iam_region import IamRegion
from huaweicloudsdkiam.v3 import IamClient, ShowDomainLoginPolicyRequest

"""
The evaluation result will be either 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 method is to call the API, ShowDomainLoginPolicy, of IAM.
In this case, you may need to set a timeout and memory limit for the function.
"""
def evaluate_compliance(context, domain_id):
    credentials = GlobalCredentials(
        ak=context.getSecurityAccessKey(),
        sk=context.getSecuritySecretKey(),
        domain_id=domain_id
    ).with_security_token(context.getSecurityToken())
    client = IamClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(IamRegion.value_of("cn-north-4")) \
        .build()

    try:
        request = ShowDomainLoginPolicyRequest()
        request.domain_id = domain_id
        response = client.show_domain_login_policy(request)
        session_timeout = response.login_policy.session_timeout
        print("session_timeout", session_timeout)
        if not session_timeout:
            return "NonCompliant"
        return "NonCompliant" if session_timeout > 30 else "Compliant"
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)


def update_policy_state(context, domain_id, evaluation):
    auth = GlobalCredentials(ak=context.getAccessKey(), sk=context.getSecretKey(), domain_id=domain_id)
    client = ConfigClient.new_builder() \
        .with_credentials(credentials=auth) \
        .with_region(region=ConfigRegion.value_of(region_id="cn-north-4")) \
        .build()
    try:
        response = client.update_policy_state(evaluation)
        return 200
    except ConnectionException as e:
        print("A connect timeout exception occurs while the Config performs some operations, exception: ",
e.error_msg)
        return e.status_code
    except RequestTimeoutException as e:
        print("A request timeout exception occurs while the Config performs some operations, exception: ",
e.error_msg)
        return e.status_code
    except ServiceResponseException as e:
        print("There is service error, exception: ", e.status_code, e.error_msg)
        return e.status_code

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

```
request_body = UpdatePolicyStateRequest(PolicyStateRequestBody(
    policy_resource = PolicyResource(
        resource_id = resource.get("id"),
        resource_name = resource.get("name"),
        resource_provider = resource.get("provider"),
        resource_type = resource.get("type"),
        region_id = resource.get("region_id"),
        domain_id = domain_id
    ),
    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"),
    evaluation_time = event.get("evaluation_time"),
    evaluation_hash = event.get("evaluation_hash")
))

for retry in range(5):
    status_code = update_policy_state(context, domain_id, request_body)
    if status_code == http.client.TOO_MANY_REQUESTS:
        print("TOO_MANY_REQUESTS: retry again")
        time.sleep(1)
    elif status_code == http.client.OK:
        print("Update policyState successfully.")
        break
    else:
        print("Failed to update policyState.")
        break
```

Dependency Package

If dependency packages are missing, you need to manually import them. For details, see **Configuring Dependency Packages**. In the preceding example, the dependency packages are **huaweicloudsdkiam** and **huaweicloudsdkconfig**.

3.2.6.2 Events

Example Event for Evaluations Triggered by Configuration Changes

When a custom rule is triggered, Config will send an event to invoke the FunctionGraph function associated with the rule.

The following example shows an event sent by Config when 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 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 an event sent by Config when 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
  }
}
```

3.3 Organization Rules

3.3.1 Adding a Predefined Organization Rule

Scenarios

If you are an organization administrator or a delegated administrator of Config, you can add organization rules and deploy the rules to member accounts that are in the normal state in your organization.

A deployed organization rule will be displayed in the rule list of each member in the organization. An organization rule can only be modified or deleted with the account that was used to create it. 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

- You can add up to 500 rules in an account.
- The resource recorder must be enabled for adding, modifying, and triggering organization rules. If the resource recorder is disabled, you can only view and delete organization rules.
- The **Organization Rules** tab is inaccessible for an account that is not associated any organizations.
- To deploy an organization rule to a member, the member account must be in the normal state, and the resource recorder must be enabled for the member.

NOTICE

To evaluate resources with rules, you need to enable the resource recorder. Resource evaluation is subject to the following rules:

- If the resource recorder is disabled, no resources will be available for evaluation. You can still view historical evaluation results.
- If the resource recorder is enabled and a monitoring scope is configured, only resources within the monitoring scope can be evaluated.

For details about how to enable and configure the resource recorder, see **Configuring the Resource Recorder**.

Procedure

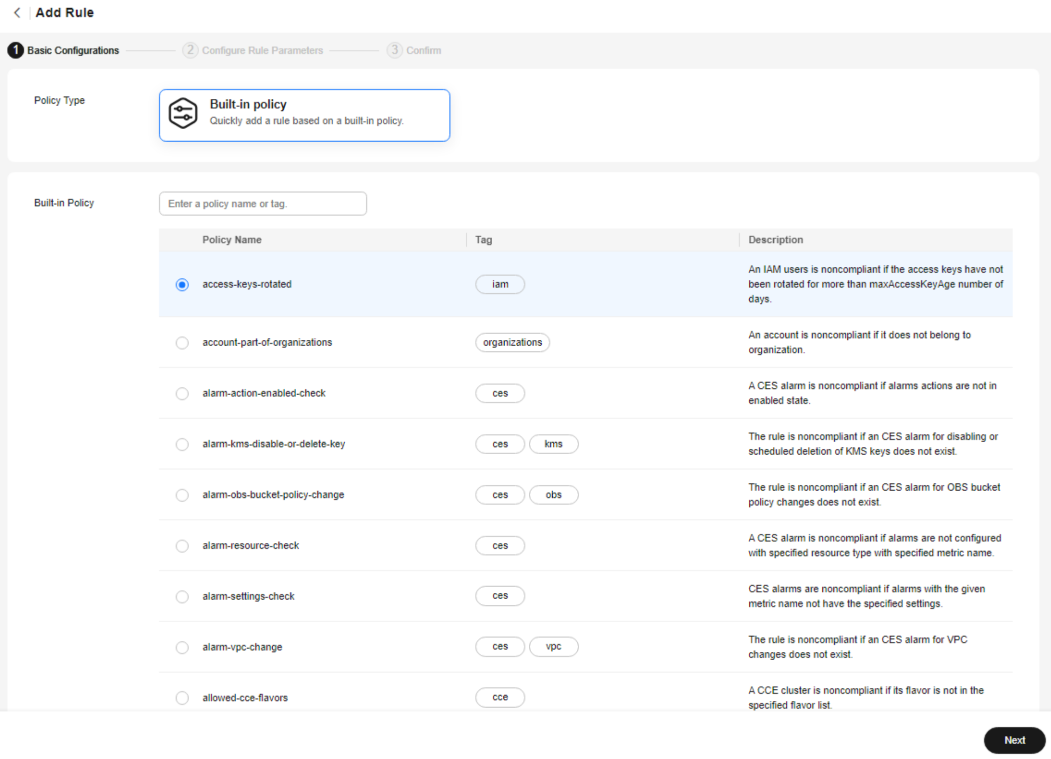
Step 1 Log in to the Config console as an organization administrator or an agency administrator of Config.

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

Step 3 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



< Add Rule

1 Basic Configurations — 2 Configure Rule Parameters — 3 Confirm

Policy Type: Built-in policy
Quickly add a rule based on a built-in policy.

Built-in Policy: Enter a policy name or tag.

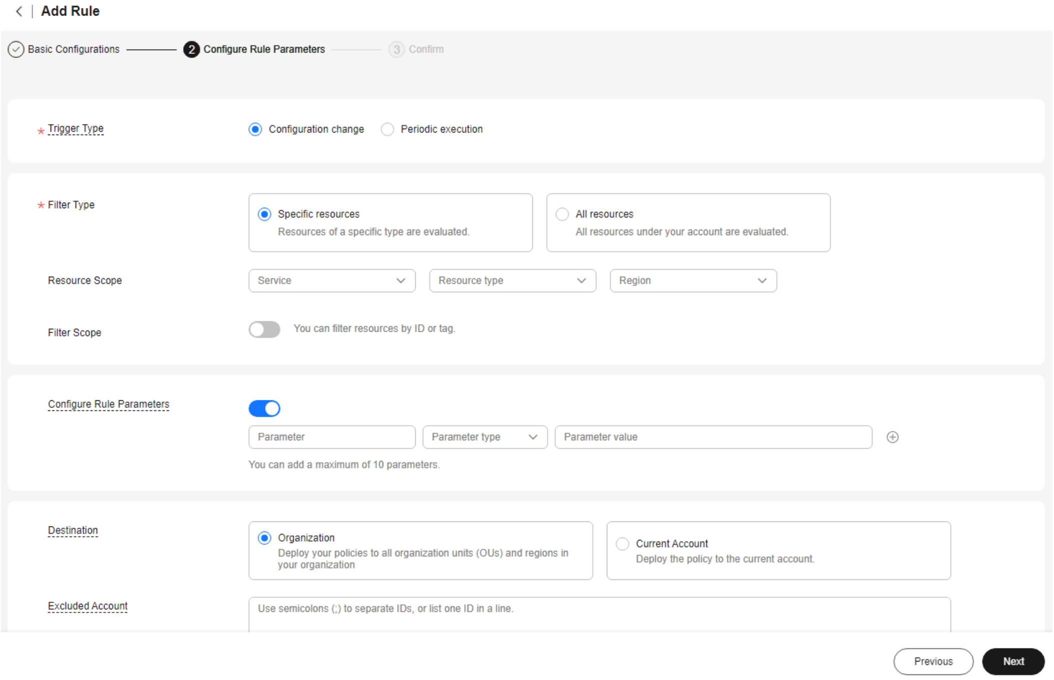
	Policy Name	Tag	Description
●	access-keys-rotated	iam	An IAM users is noncompliant if the access keys have not been rotated for more than maxAccessKeyAge number of days.
○	account-part-of-organizations	organizations	An account is noncompliant if it does not belong to organization.
○	alarm-action-enabled-check	ces	A CES alarm is noncompliant if alarms actions are not in enabled state.
○	alarm-kms-disable-or-delete-key	ces kms	The rule is noncompliant if an CES alarm for disabling or scheduled deletion of KMS keys does not exist.
○	alarm-obs-bucket-policy-change	ces obs	The rule is noncompliant if an CES alarm for OBS bucket policy changes does not exist.
○	alarm-resource-check	ces	A CES alarm is noncompliant if alarms are not configured with specified resource type with specified metric name.
○	alarm-settings-check	ces	CES alarms are noncompliant if alarms with the given metric name not have the specified settings.
○	alarm-vpc-change	ces vpc	The rule is noncompliant if an CES alarm for VPC changes does not exist.
○	allowed-cce-flavors	cce	A CCE cluster is noncompliant if its flavor is not in the specified flavor list.

Table 3-5 Parameters of the basic configuration

Parameter	Description
Policy Type	Select **Built-in policy**. Built-in policies are provided by Config. You can select a built-in policy to quickly add a rule. You can also search for a built-in policy by policy name or tag. For more information about built-in policies, see **Built-In 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



< | **Add Rule**

Basic Configurations — 2 Configure Rule Parameters — 3 Confirm

* Trigger Type ● Configuration change ○ Periodic execution

* Filter Type

● Specific resources
Resources of a specific type are evaluated.

○ All resources
All resources under your account are evaluated.

Resource Scope: Service | Resource type | Region

Filter Scope: You can filter resources by ID or tag.

Configure Rule Parameters: Parameter | Parameter type | Parameter value

You can add a maximum of 10 parameters.

Destination

● Organization
Deploy your policies to all organization units (OUs) and regions in your organization

○ Current Account
Deploy the policy to the current account.

Excluded Account: Use semicolons (;) to separate IDs, or list one ID in a line.

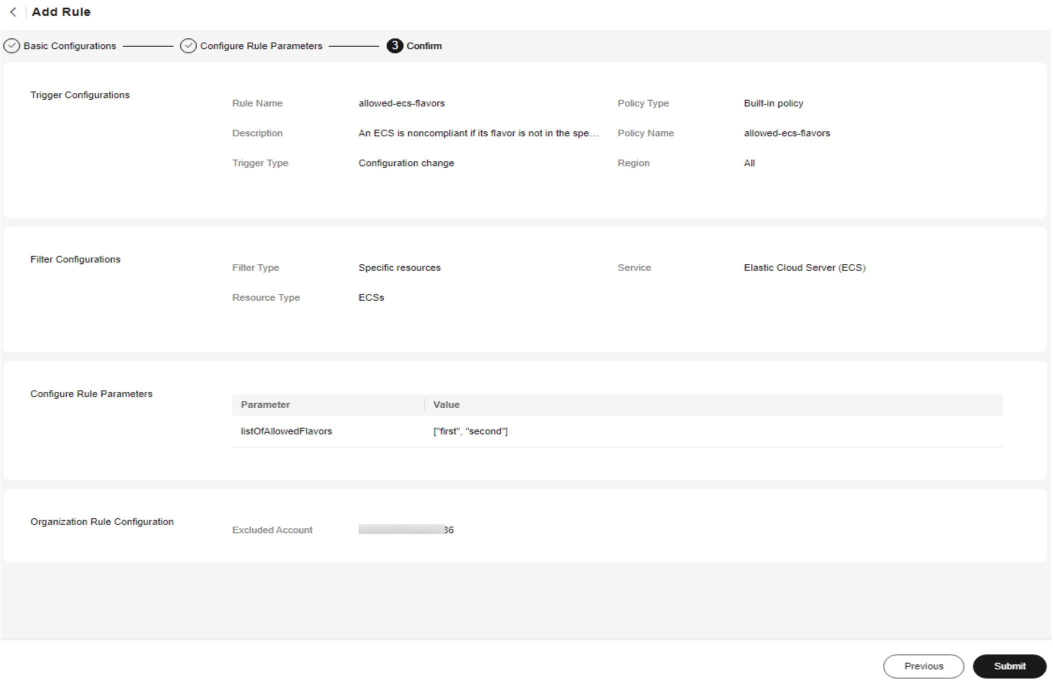
Table 3-6 Rule parameter description

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 the **required-tag-check** policy, you need to specify a tag, so that resources that do not have the tag will be determined as noncompliant. Not all built-in policies require **Configure Rule Parameters**. For example, the rule, **volumes-encrypted-check**, does not require **Configure Rule Parameters**.
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	Member accounts to which organization rules will not be deployed. This parameter is only required when **Destination** is set to **Organization**.

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

Figure 3-14 Confirming a rule



Trigger Configurations

Rule Name: allowed-ecs-flavors

Policy Type: Built-in policy

Description: An ECS is noncompliant if its flavor is not in the spe...

Policy Name: allowed-ecs-flavors

Trigger Type: Configuration change

Region: All

Filter Configurations

Filter Type: Specific resources

Service: Elastic Cloud Server (ECS)

Resource Type: ECSs

Configure Rule Parameters

Parameter	Value
listOfAllowedFlavors	["first", "second"]

Organization Rule Configuration

Excluded Account: [redacted]36

NOTE

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

----End

Triggering a Rule Evaluation

For details about how a member can trigger an organization rule, see **Triggering a Rule**.

3.3.2 Creating a Custom Organization Rule

Scenario

You can create custom organization rules to supplement predefined ones.

To create custom rules, you need to use **Use of FunctionGraph** functions. Each rule is associated with a Function Graph function. Config reports events to the function. The function collects rule parameters and resource attributes from the events; evaluates whether your resources comply with the rule; and return evaluation results using Open APIs of Config. The function is invoked either in response to configuration changes or periodically. When adding a custom organization rule, you need to share the associated FunctionGraph functions with your organization members through RAM.

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

1. **Creating a function using FunctionGraph**
2. **Sharing a FunctionGraph Function**

3. **Creating a Custom Organization Rule**
4. **Triggering a Rule**

Constraints and Limitations

- You can add up to 500 rules in an account.
- The resource recorder must be enabled for adding, modifying, and triggering organization rules. If the resource recorder is disabled, you can only view and delete organization rules.
- The **Organization Rules** tab is inaccessible for an account that is not associated any organizations.
- To deploy an organization rule to a member, the member account must be in the normal state, and the resource recorder must be enabled for the member.

NOTICE

To evaluate resources with rules, you need to enable the resource recorder. Resource evaluation is subject to the following rules:

- If the resource recorder is disabled, no resources will be available for evaluation. You can still view historical evaluation results.
- If the resource recorder is enabled and a monitoring scope is configured, only resources within the monitoring scope can be evaluated.

For details about how to enable and configure the resource recorder, see **Configuring the Resource Recorder**.

Creating a function using FunctionGraph

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

Step 2 In the upper right corner, click **Create Function**.

Step 3 Set **Function Type** to **Event Function** and configure the required IAM agency. The 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

Sharing a FunctionGraph Function

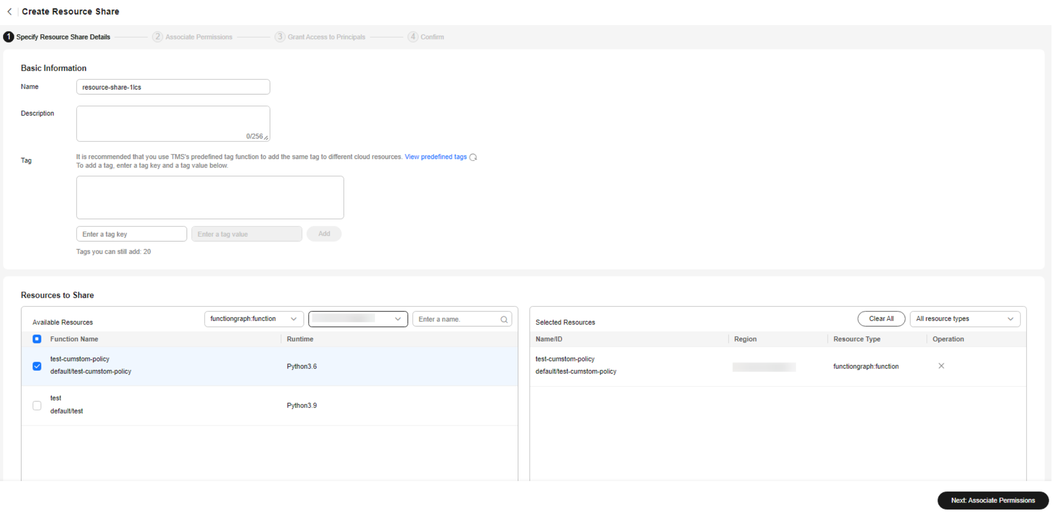
Step 1 Log in to the Config console as an organization administrator or an agency administrator of Config.

Step 2 Click ☰ in the upper left corner and choose **Management & Governance** > **Resource Access Manager**. The **Resource Access Manager** page is displayed.

Step 3 Choose **Shared by Me** > **Resource Shares**.

Step 4 In the upper right corder, click **Create Resource Share**. In the **Basic Information** area, configure basic information. In the **Resources to Share** area, select **functiongraph:function**, and then select a function that is displayed. Click **Next: Associate Permissions**.

Figure 3-15 Specifying **Resources to Share**



Basic Information

Name: resource-share-1lcs

Description: 0/256

Tag: It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. View predefined tags
To add a tag, enter a tag key and a tag value below.

Tags you can still add: 20

Resources to Share

Available Resources: functiongraph:function

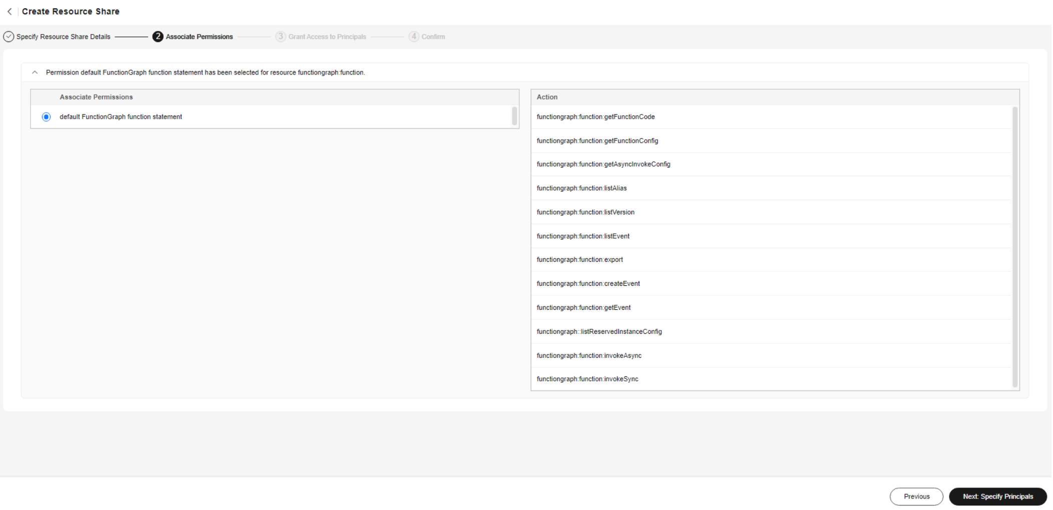
☑	Function Name	Runtime
☑	test-cumstom-policy default/test-cumstom-policy	Python3.6
□	test default/test	Python3.9

Selected Resources

Name/ID	Region	Resource Type	Operation
test-cumstom-policy default/test-cumstom-policy		functiongraph:function	×

Step 5 Click **default FunctionGraph function statement** and click **Next: Specify Principals**.

Figure 3-16 Associate Permissions



Permission default FunctionGraph function statement has been selected for resource functiongraph:function.

	Associate Permissions
●	default FunctionGraph function statement

Action
functiongraph:function:getFunctionCode
functiongraph:function:getFunctionConfig
functiongraph:function:getAsyncInvokeConfig
functiongraph:function:listAlias
functiongraph:function:listVersion
functiongraph:function:listEvent
functiongraph:function:export
functiongraph:function:createEvent
functiongraph:function:getEvent
functiongraph::listReservedInstanceConfig
functiongraph:function:invokeAsync
functiongraph:function:invokeSync

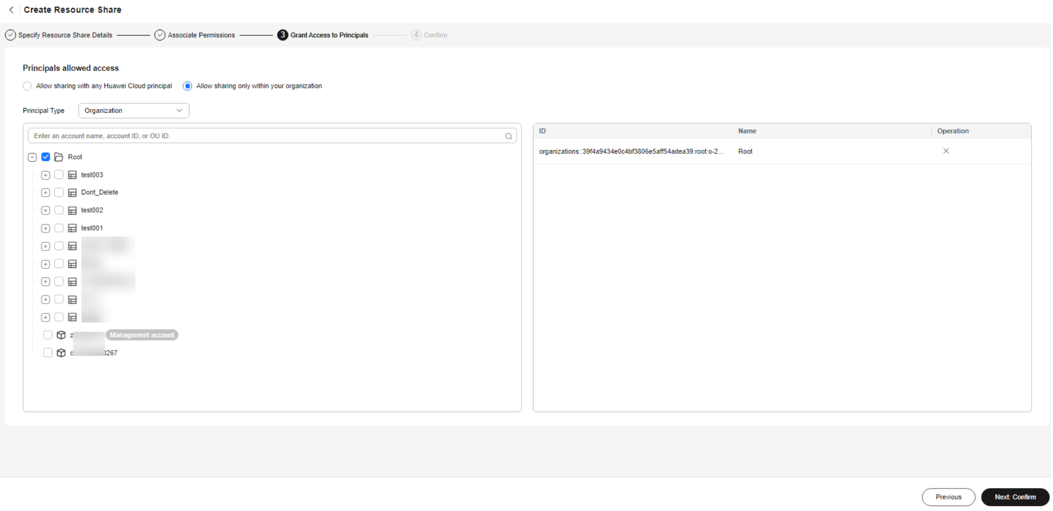
Step 6 On the **Grant Access to Principals** page, specify principals and click **Next: Confirm** in the lower right corner.

- If you select **Allow sharing only within your organization** for **Principals allowed access**, you can only grant access to members in your organization.
- If you select **Organization** for **Principal Type** and then select **Root**, all members in your organization can access the function.

NOTE

If you haven't enabled resource sharing with organizations, you cannot set **Principal Type** to **Organization**. To learn about how to enable resource sharing with organizations, see **Enabling Sharing with Organizations**.

Figure 3-17 Specifying principals



Create Resource Share

Specify Resource Share Details — Associate Permissions — 3 Grant Access to Principals — 4 Confirm

Principals allowed access

○ Allow sharing with any Huawei Cloud principal ● Allow sharing only within your organization

Principal Type: Organization

Enter an account name, account ID, or OU ID.

☑ Root
- □ test003
- □ Dont_Delete
- □ test002
- □ test001
- □ [redacted]
- □ [redacted]
- □ [redacted]
- □ [redacted]
- □ [redacted]
- □ z[redacted] Management account
- □ c[redacted]267

ID	Name	Operation
organizations::39f4a9434e0c4bf3806e5aff54adea39:root:o-2...	Root	×

Step 7 Review and confirm the configuration details of your resource share and select **I have read and agree to Privacy Statement** on the **Confirm** page. Then, click **Submit** in the lower right corner.

----End

Creating a Custom Organization Rule

Step 1 Log in to the management console.

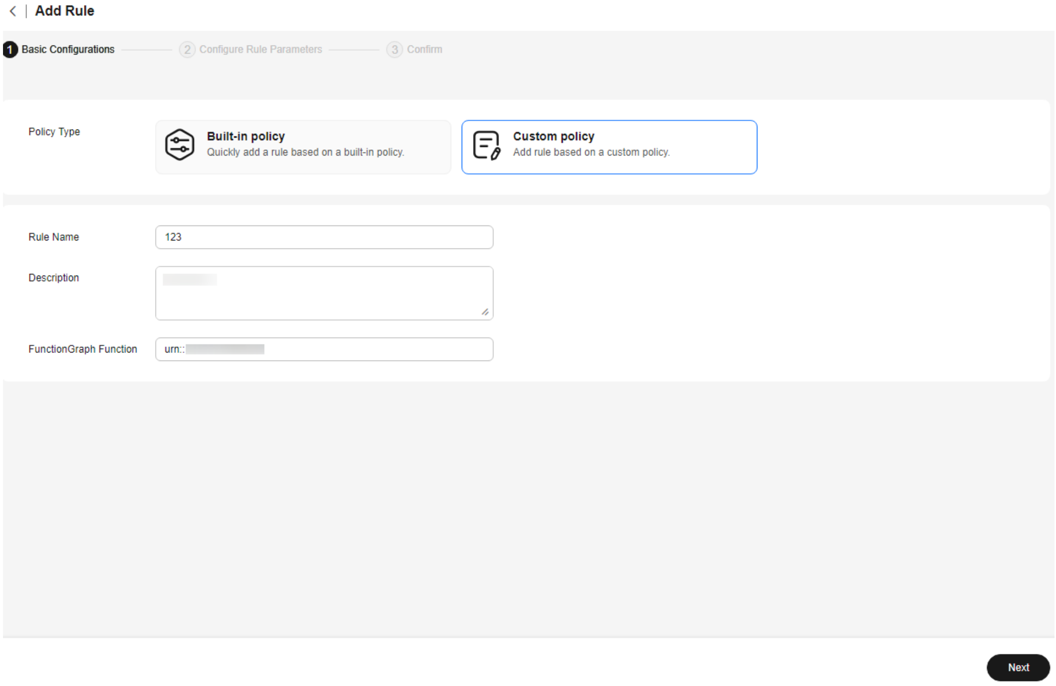
Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

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

Step 4 Select the **Organization Rules** tab and click **Add Rule**.

Step 5 Set **Policy Type** to **Custom policy**, and configure other parameters, and click **Next**.

Figure 3-18 Basic Configurations



< | Add Rule

1 Basic Configurations — 2 Configure Rule Parameters — 3 Confirm

Policy Type
Built-in policy: Quickly add a rule based on a built-in policy.
Custom policy: Add rule based on a custom policy.

Rule Name: 123

Description: [redacted]

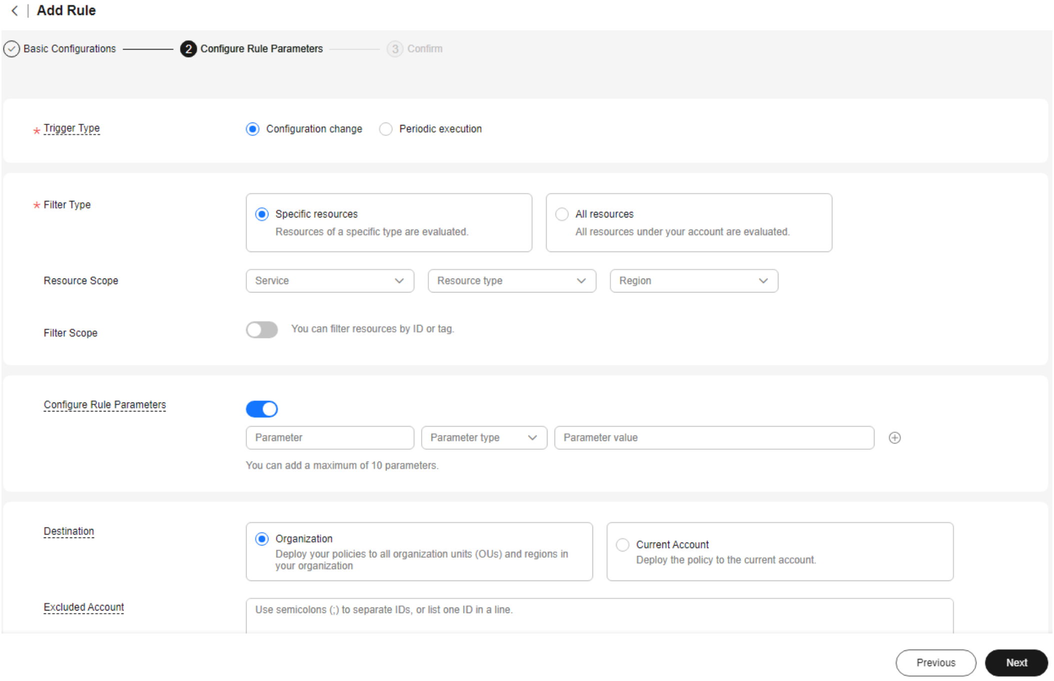
FunctionGraph Function: urn:[redacted]

Table 3-7 Basic parameters

Parameter	Description
Policy Type	Select **Custom policy**. You can create custom policies to supplement built-in policies.
Rule Name	The name of a rule. A rule name must be unique. A rule name can contain only digits, letters, underscores (_), and hyphens (-).
Description	The description of a rule. There are no restrictions on the rule description.
FunctionGraph Function	The URN of a function. For details about how to create a FunctionGraph function, see **Creating a function using FunctionGraph**.

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

Figure 3-19 Configure Rule Parameters



< | **Add Rule**

Basic Configurations — 2 Configure Rule Parameters — 3 Confirm

* Trigger Type ● Configuration change ○ Periodic execution

* Filter Type ● Specific resources Resources of a specific type are evaluated. ○ All resources All resources under your account are evaluated.

Resource Scope: Service, Resource type, Region

Filter Scope: You can filter resources by ID or tag.

Configure Rule Parameters: Parameter, Parameter type, Parameter value

You can add a maximum of 10 parameters.

Destination ● Organization Deploy your policies to all organization units (OUs) and regions in your organization ○ Current Account Deploy the policy to the current account.

Excluded Account: Use semicolons (;) to separate IDs, or list one ID in a line.

Table 3-8 Rule parameters

Parameter	Description
Trigger Type	The condition under which a rule will be triggered. Trigger types are as follows: - **Configuration change**: A rule is triggered when there is a change in resource configurations. - **Periodic execution**: A rule is triggered at a specific frequency.
Filter Type	The type of resources to be evaluated. Filter types are as follows: - **Specific resources**: Resources of a specific type. - **All resources**: All resources from your account. 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**: The service that the resource belongs to. - **Resource type**: The resource type - **Region**: The region where the resource resides. This parameter is mandatory only when **Trigger Type** is set to **Configuration change**.

Parameter	Description
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	How often a rule will be triggered. This parameter is mandatory only when **Trigger Type** is set to **Periodic execution**.
Rule Parameter	You can set up to 10 rule parameters for a custom rule.
Destination	Where the organization rule will be deployed ● **Organization**: A conformance package will be deployed to all members in a specified organization. ● **Current Account**: A conformance package will be deployed to the current account. When creating an organization rule, select **Organization**.
Excluded Account	IDs of member accounts to which organization rules will not be deployed. This parameter is only required when **Destination** is set to **Organization**.

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

----End

Triggering a Rule

For details about how a member can trigger an organization rule, see **Triggering a Rule**.

3.3.3 Viewing an Organization Rule

Scenario

You can view organization rules and their details.

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

Viewing an Organization Rule

You can view details about a created organization rule.

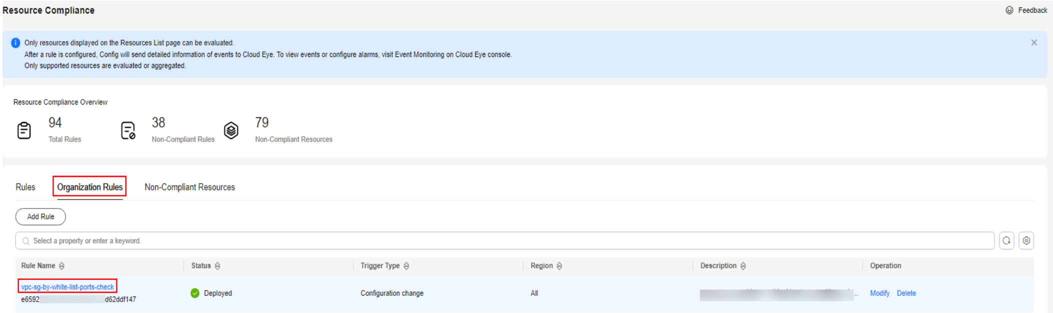
Step 1 Log in to the management console.

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

Figure 3-20 Viewing organization rules



Only resources displayed on the Resources List page can be evaluated.
After a rule is configured, Config will send detailed information of events to Cloud Eye. To view events or configure alarms, visit Event Monitoring on Cloud Eye console.
Only supported resources are evaluated or aggregated.

94 Total Rules
38 Non-Compliant Rules
79 Non-Compliant Resources

Rule Name	Status	Trigger Type	Region	Description	Operation
vpc-sg-by-white-list-ports-check e6592[redacted]d62ddf147	Deployed	Configuration change	All	[redacted]..	Modify Delete

Step 5 On the left of the **Rule Details** page, view member accounts to which the organization rule was deployed, 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. An organization rule can only be modified or deleted with the account that was used to create it. Members can only trigger an organization rule and view evaluation results.

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

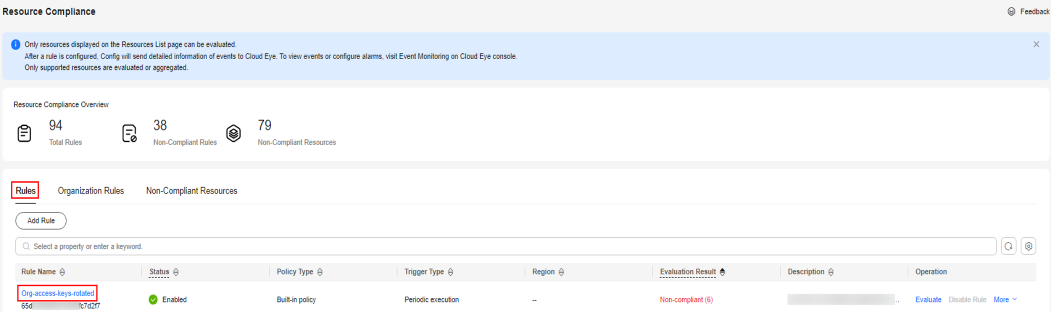
Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

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

Step 4 On the **Rules** tab, 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 3-21 Viewing organization rules deployed to member accounts



Resource Compliance

Feedback

Only resources displayed on the Resources List page can be evaluated.
After a rule is configured, Config will send detailed information of events to Cloud Eye. To view events or configure alarms, visit Event Monitoring on Cloud Eye console.
Only supported resources are evaluated or aggregated.

Resource Compliance Overview

94 Total Rules

38 Non-Compliant Rules

79 Non-Compliant Resources

Rules | Organization Rules | Non-Compliant Resources

Add Rule

Select a property or enter a keyword.

Rule Name	Status	Policy Type	Trigger Type	Region	Evaluation Result	Description	Operation
Org-access-keys-rotated 65d[redacted]fc7d2f7	Enabled	Built-in policy	Periodic execution	--	Non-compliant (6)	[redacted]..	Evaluate Disable Rule More

NOTE

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

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

----End

Deployment Statuses of Organization Rules

Table 3-9 Deployment statuses of organization rules

Value	Status	Description
CREATE_IN_PROGRESS	Deploying	An organization rule is being created.
UPDATE_IN_PROGRESS	Updating	An organization rule is being updated.
DELETE_IN_PROGRESS	Deleting	An organization rule is being deleted.
CREATE_FAILED	Abnormal	An organization rule fails to be deployed to one or more member accounts.
UPDATE_FAILED	Update failed	An organization rule fails to be updated in one or more member accounts.
DELETE_FAILED	Deletion failed	An organization rule fails to be deleted in one or more member accounts.
CREATE_SUCCESSFUL	Deployed	An organization rule has been deployed to all member accounts.
UPDATE_SUCCESSFUL	Updated	An organization rule has been updated in all member accounts.

3.3.4 Modifying an Organization Rule

Scenarios

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

NOTE

The resource recorder must be enabled for adding, modifying, and triggering organization rules. If the resource recorder is disabled, you can only view and delete organization rules.

Procedure

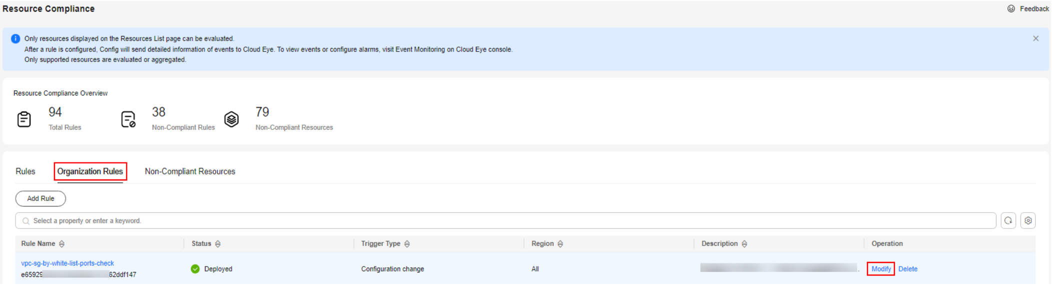
Step 1 Log in to the management console.

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

Figure 3-22 Editing an organization rule



Resource Compliance

Only resources displayed on the Resources List page can be evaluated.
After a rule is configured, Config will send detailed information of events to Cloud Eye. To view events or configure alarms, visit Event Monitoring on Cloud Eye console.
Only supported resources are evaluated or aggregated.

Resource Compliance Overview

94 Total Rules | 38 Non-Compliant Rules | 79 Non-Compliant Resources

Rule Name	Status	Trigger Type	Region	Description	Operation
vpc-sg-by-white-list-ports-check e6592[redacted]62ddf147	Deployed	Configuration change	All	[redacted]	Modify Delete

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

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

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

----End

3.3.5 Deleting an Organization Rule

Scenarios

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

Procedure

Step 1 Log in to the management console.

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

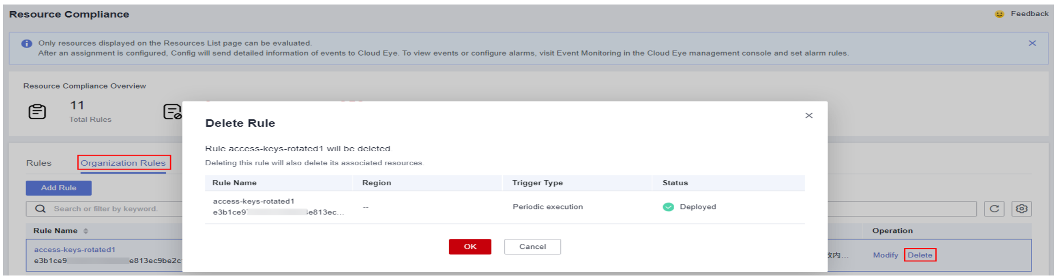
Step 3 In the navigation pane on the left, choose **Resource Compliance**.

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 dialog box, click **OK**.

After an organization rule is deleted, the rule will be automatically deleted from each member account.

Figure 3-23 Deleting organization rules



Only resources displayed on the Resources List page can be evaluated.
After an assignment is configured, Config will send detailed information of events to Cloud Eye. To view events or configure alarms, visit Event Monitoring in the Cloud Eye management console and set alarm rules.

access-keys-rotated1
e3b1ce9[redacted]e813ec9be2c

Delete Rule

Rule access-keys-rotated1 will be deleted.

Deleting this rule will also delete its associated resources.

Rule Name	Region	Trigger Type	Status
access-keys-rotated1 e3b1ce9[redacted]e813ec...	--	Periodic execution	Deployed

----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.

3.3.6 Example Custom Organization Rules

3.3.6.1 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 time
import http.client
from huaweicloudsdkcore.auth.credentials import GlobalCredentials
from huaweicloudsdkcore.exceptions.exceptions import ConnectionException
from huaweicloudsdkcore.exceptions.exceptions import RequestTimeoutException
from huaweicloudsdkcore.exceptions.exceptions import ServiceResponseException
from huaweicloudsdkconfig.v1.region.config_region import ConfigRegion
from huaweicloudsdkconfig.v1.config_client import ConfigClient
from huaweicloudsdkconfig.v1 import PolicyResource, PolicyStateRequestBody
from huaweicloudsdkconfig.v1 import UpdatePolicyStateRequest

'''
The evaluation result of a rule will be either Compliant or NonCompliant.
In this example, if the vpcId of an ECS 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(context, domain_id, evaluation):
    auth = GlobalCredentials(ak=context.getAccessKey(), sk=context.getSecretKey(), domain_id=domain_id)
    client = ConfigClient.new_builder() \
        .with_credentials(credentials=auth) \
        .with_region(region=ConfigRegion.value_of(region_id="cn-north-4")) \
        .build()

    try:
        response = client.update_policy_state(evaluation)
        return 200
    except ConnectionException as e:
        print("A connect timeout exception occurs while the Config performs some operations, exception: ",
e.error_msg)
        return e.status_code
    except RequestTimeoutException as e:
        print("A request timeout exception occurs while the Config performs some operations, exception: ",
e.error_msg)
        return e.status_code
    except ServiceResponseException as e:
        print("There is service error, exception: ", e.status_code, e.error_msg)
        return e.status_code


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

    request_body = UpdatePolicyStateRequest(PolicyStateRequestBody(
        policy_resource = PolicyResource(
            resource_id = resource.get("id"),
            resource_name = resource.get("name"),
            resource_provider = resource.get("provider"),
            resource_type = resource.get("type"),
            region_id = resource.get("region_id"),
            domain_id = event.get("domain_id")
        ),
        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"),
        evaluation_time = event.get("evaluation_time"),
        evaluation_hash = event.get("evaluation_hash")
    ))

    for retry in range(5):
        status_code = update_policy_state(context, domain_id, request_body)
        if status_code == http.client.TOO_MANY_REQUESTS:
            print("TOO_MANY_REQUESTS: retry again")
            time.sleep(1)
        elif status_code == http.client.OK:
            print("Update policyState successfully.")
            break
        else:
            print("Failed to update policyState.")
            break
```

Example Function Triggered Periodically

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

```
import time
import http.client
from huaweicloudsdkcore.auth.credentials import GlobalCredentials
from huaweicloudsdkcore.exceptions.exceptions import ConnectionException
from huaweicloudsdkcore.exceptions.exceptions import RequestTimeoutException
from huaweicloudsdkcore.exceptions.exceptions import ServiceResponseException
from huaweicloudsdkconfig.v1.region.config_region import ConfigRegion
from huaweicloudsdkconfig.v1.config_client import ConfigClient
from huaweicloudsdkconfig.v1 import PolicyResource, PolicyStateRequestBody
from huaweicloudsdkconfig.v1 import UpdatePolicyStateRequest
from huaweicloudsdkiam.v3.region.iam_region import IamRegion
from huaweicloudsdkiam.v3 import IamClient, ShowDomainLoginPolicyRequest

"""
The evaluation result of a rule will be either 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 method is to call the API, ShowDomainLoginPolicy, of IAM.
In this case, you may need to set a timeout and memory limit for the function.
"""
def evaluate_compliance(ak, sk, domain_id):
    credentials = GlobalCredentials(ak, sk)
    client = IamClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(IamRegion.value_of("cn-north-4")) \
        .build()

    try:
        request = ShowDomainLoginPolicyRequest()
        request.domain_id = domain_id
        response = client.show_domain_login_policy(request)
        session_timeout = response.login_policy.session_timeout
        print("session_timeout", session_timeout)
        if not session_timeout:
            return "NonCompliant"
        return "NonCompliant" if session_timeout > 30 else "Compliant"
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)


def update_policy_state(context, domain_id, evaluation):
    auth = GlobalCredentials(ak=context.getAccessKey(), sk=context.getSecretKey(), domain_id=domain_id)
    client = ConfigClient.new_builder() \
        .with_credentials(credentials=auth) \
        .with_region(region=ConfigRegion.value_of(region_id="cn-north-4")) \
        .build()
    try:
        response = client.update_policy_state(evaluation)
        return 200
    except ConnectionException as e:
        print("A connect timeout exception occurs while the Config performs some operations, exception: ",
e.error_msg)
        return e.status_code
    except RequestTimeoutException as e:
        print("A request timeout exception occurs while the Config performs some operations, exception: ",
e.error_msg)
        return e.status_code
    except ServiceResponseException as e:
        print("There is service error, exception: ", e.status_code, e.error_msg)
        return e.status_code

def handler(event, context):
    domain_id = "<manager_domain_id>"
    ak = "<user_ak">
    sk = "<user_sk>
    resource = event.get("invoking_event", {})
    if resource.get("name") != "Account":
        return
    compliance_state = evaluate_compliance(ak, sk, event.get("domain_id"))

    request_body = UpdatePolicyStateRequest(PolicyStateRequestBody(
        policy_resource = PolicyResource(
            resource_id = resource.get("id"),
            resource_name = resource.get("name"),
            resource_provider = resource.get("provider"),
            resource_type = resource.get("type"),
            region_id = resource.get("region_id"),
            domain_id = event.get("domain_id")
        ),
        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"),
        evaluation_time = event.get("evaluation_time"),
        evaluation_hash = event.get("evaluation_hash")
    ))

    for retry in range(5):
        status_code = update_policy_state(context, domain_id, request_body)
        if status_code == http.client.TOO_MANY_REQUESTS:
            print("TOO_MANY_REQUESTS: retry again")
            time.sleep(1)
        elif status_code == http.client.OK:
            print("Update policyState successfully.")
            break
        else:
            print("Failed to update policyState.")
            break
```

Dependency Package

If dependency packages are missing, you need to manually import them. For details, see **Configuring Dependency Packages**. In the preceding example, the dependency packages are **huaweicloudsdkiam** and **huaweicloudsdkconfig**.

3.3.6.2 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
  }
}
```

3.4 Viewing Noncompliant Resources

Scenarios

You can view all noncompliant resources on the **Non-Compliant Resources** tab of the **Resource Compliance** page.

Procedure

Step 1 Log in to the management console.

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

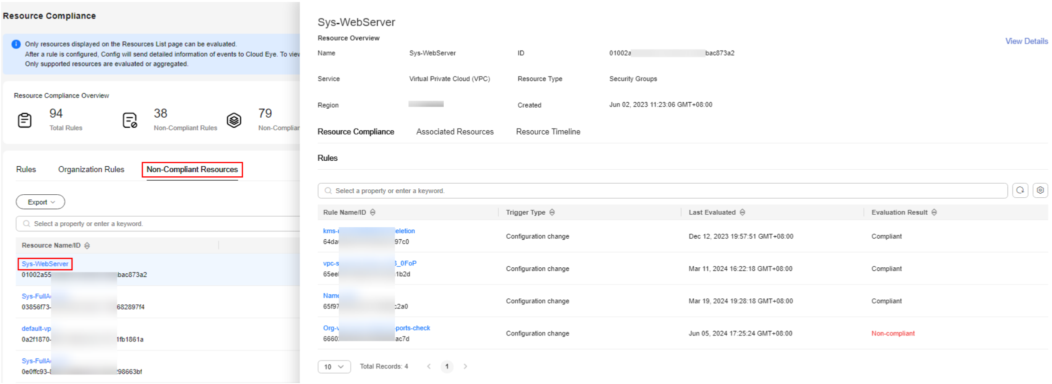
Step 3 In the navigation pane on the left, choose **Resource Compliance**.

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.

Above the list, you can filter non-compliant resources with multiple search options. You can also export the list.

Figure 3-24 Viewing non-compliant resources



Resource Compliance

Only resources displayed on the Resources List page can be evaluated.
After a rule is configured, Config will send detailed information of events to Cloud Eye. To view
Only supported resources are evaluated or aggregated.

Resource Compliance Overview

94 Total Rules | 38 Non-Compliant Rules | 79 Non-Complian

Resource Name/ID
Sys-WebServer 01002a55[redacted]bac873a2
Sys-FullA[redacted] 03856f73-[redacted]682897f4
default-vp[redacted] 0a2f1870-[redacted]1fb1861a
Sys-FullA[redacted] 0e0ffc93-[redacted]98663bf

Sys-WebServer

Resource Overview

View Details

Name	Sys-WebServer	ID	01002a[redacted]bac873a2
Service	Virtual Private Cloud (VPC)	Resource Type	Security Groups
Region	[redacted]	Created	Jun 02, 2023 11:23:06 GMT+08:00

Rule Name/ID	Trigger Type	Last Evaluated	Evaluation Result
kms-[redacted]eletion 64da[redacted]97c0	Configuration change	Dec 12, 2023 19:57:51 GMT+08:00	Compliant
vpc-s[redacted]_0FoP 65ee[redacted]1b2d	Configuration change	Mar 11, 2024 16:22:18 GMT+08:00	Compliant
Name[redacted] 65f97[redacted]c2a0	Configuration change	Mar 19, 2024 19:28:18 GMT+08:00	Compliant
Org-[redacted]ports-check 6660[redacted]ac7d	Configuration change	Jun 05, 2024 17:25:24 GMT+08:00	Non-compliant

----End

3.5 Compliance Rule Concepts

3.5.1 Policy

A policy is a logical expression used to evaluate resource compliance.

A policy cannot work on its own. Instead, you need to attach a policy to a rule.

A policy can be a JSON expression. **Table 3-10** lists policy (JSON expression) parameters.

Table 3-10 Policy parameters (JSON)

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 **Built-In 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.
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**.

3.5.2 Rule

A rule mainly consists of a policy and an applicable scope, for example, some resources in a region.

You can use a JSON expression to represent a rule, as shown in **Table 3-11**.

Table 3-11 Rule parameters (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**: The 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**: The 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**: The value must be an object. ● **key**: The 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**: The 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.
tags	Tags added to a rule	-	● A tag key can contain up to 128 Unicode characters. ● A tag value can contain up to 255 Unicode characters.
created_by	The creator of a rule	-	A rule can be created by a user or a service with the required service-link agency.

NOTE

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

The following shows a predefined policy that is used to check whether ECSs in **regionid_1** have a specific 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": []
    }
  }
  "tags": [],
  "created_by": "custom"
}
```

The following JSON expression shows a custom rule for evaluating 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"}
    }
  }
  "tags": [],
  "created_by": "custom"
}
```

3.5.3 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 3-12**.

Table 3-12 Evaluation result in JSON

Parameter	Description	Remarks
domain_id	Account ID	This parameter is used to distinguish users. **domain_id** will be provided in each evaluation result.

Parameter	Description	Remarks
resource_id	Specifies the ID of the evaluated resource.	N/A
resource_name	Specifies the service type.	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
compliance_state	Specifies the evaluation 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 expression shows 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
}
```

3.6 Built-In Policies

3.6.1 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 3-13 Predefined policies

Service	Policy	Triggered By	Object
General policies	**Resource Names Meet Regular Expression Requirements**	Configuration change	All resources
	Resources Have All the Specified Tags Attached	Configuration change	**Supported Services and Resources**
	Resources Have One of the Specified Tags Attached	Configuration change	**Supported Services and Resources**
	Tag Prefixes and Suffixes Check	Configuration change	**Supported Services and Resources**
	Resources Have at Least One Tags Attached	Configuration change	**Supported Services and Resources**
	Resource Tag Check	Configuration change	**Supported Services and Resources**
	Resources Are in Specified Enterprise Projects	Configuration change	All resources

Service	Policy	Triggered By	Object
	Resources Are in Specified Regions	Configuration change	All resources
	Resource Type Check by Specifying Allowed Resource Types	Configuration change	All resources
	Resource Type Check by Specifying Unallowed Resource Types	Configuration change	All resources
API Gateway (APIG)	**Dedicated API Gateways Have an Authorization Type Set**	Configuration change	apig.instances
	Dedicated API Gateways Have Logging Enabled	Configuration change	apig.instances
	Dedicated API Gateways Use SSL certificates	Configuration change	apig.instances
CodeArts Deploy	**Clusters Are Available**	Configuration change	codeartsdeploy.host-cluster
	Project Parameter Encryption Check	Configuration change	codeartsbuild.CloudBuildServer
MapReduce Service (MRS)	**MRS Clusters Have Specified Security Groups Attached**	Configuration change	mrs.mrs
	MRS Clusters Are in Specified VPCs	Configuration change	mrs.mrs
	MRS Clusters Have Kerberos Enabled	Configuration change	mrs.mrs
	MRS Clusters Support Multi-AZ Deployment	Configuration change	mrs.mrs
	MRS Clusters Do Not Have EIPs Attached	Configuration change	mrs.mrs

Service	Policy	Triggered By	Object
	MRS Clusters Have KMS Encryption Enabled	Configuration change	mrs.mrs
NAT Gateway	**Private NAT Private Gateways Are in Specified VPCs**	Configuration change	nat.privateNatGateways
VPC Endpoint (VPCEP)	**VPC Endpoint Check for Specified Services**	Periodic	Account
Web Application Firewall (WAF)	**WAF Instances Have Protection Policies Attached**	Configuration change	waf.instance
	WAF Protection Policies Are Not Empty	Configuration change	waf.policy
	WAF Instances Have Domain Name Protection Enabled	Periodic	Account
	WAF Policies Have Geolocation Access Control Enabled	Periodic	Account
	WAF Instances Have Block Policies Attached	Configuration change	waf.instance
ELB	**Load Balancers Do Not Have EIPs Attached**	Configuration change	elb.loadbalancers
	ELB Listeners Have Specified Security Policies Added	Configuration change	elb.loadbalancers
	ELB Listeners Are Configured with HTTPS	Configuration change	elb.loadbalancers
	Weight Check for Backend Servers	Configuration change	elb.members
	HTTPS Redirection Check	Configuration change	elb.listeners
	Single-AZ Load Balancer Check	Configuration change	elb.loadbalancers

Service	Policy	Triggered By	Object
	ELB Load Balancers Have Access Logging Configured	Configuration change	elb.loadbalancers
Elastic IP (EIP)	**Bandwidth Check**	Configuration change	vpc.publicips
	Idle Elastic IP Check	Configuration change	vpc.publicips
	Elastic IPs Are Used Within a Given Period of Time	Periodic	vpc.publicips
Auto Scaling (AS)	**Priority Policy Check**	Configuration change	as.scalingGroups
	AS Groups Are Associated with an Elastic Load Balancer that Uses Health Check	Configuration change	as.scalingGroups
	Multi-AZ Deployment Has Been Configured	Configuration change	as.scalingGroups
	IPv6 Bandwidth Check	Configuration change	as.scalingGroups
	AS Groups Are in Specified VPCs	Configuration change	as.scalingGroups
Scalable File Service Turbo (SFS Turbo)	**SFS Turbo File Systems Have KMS Encryption Enabled**	Configuration change	sfsturbo.shares
	SFS Turbo Systems Are Associated with Backup Vaults	Configuration change	sfsturbo.shares
	Backup Time Check	Periodic	sfsturbo.shares
Elastic Cloud Server (ECS)	**Flavor Check**	Configuration change	ecs.cloudservers
	Image Check	Configuration change	ecs.cloudservers

Service	Policy	Triggered By	Object
	Image Check by Tag	Configuration change	ecs.cloudservers
	Security Group Check by ID	Configuration change	ecs.cloudservers
	VPC Check by ID	Configuration change	ecs.cloudservers
	ECSs Have Key Pairs Attached	Configuration change	ecs.cloudservers
	ECSs Cannot Be Accessed Through Public Networks	Configuration change	ecs.cloudservers
	An ECS Does Not Have Multiple EIPs Attached	Configuration change	ecs.cloudservers
	Idle ECS Check	Periodic	ecs.cloudservers
	ECSs Have IAM Agencies Attached	Configuration change	ecs.cloudservers
	Image Check by Name	Configuration change	ecs.cloudservers
	ECSs Have Backup Vaults Attached	Configuration change	ecs.cloudservers
	Backup Time Check	Periodic	ecs.cloudservers
	ECSs Have HSS Agents Attached	Configuration change	ecs.cloudservers
Distributed Cache Service (DCS)	DCS Memcached Instances Support SSL	Configuration change	dcs.memcached
	DCS Memcached Instances Are in a Specified VPC	Configuration change	dcs.memcached

Service	Policy	Triggered By	Object
	DCS Memcached Instances Do Not Have EIPs Attached	Configuration change	dcs.memcached
	Access Mode Check	Configuration change	dcs.memcached
	DCS Redis Instances Support SSL	Configuration change	dcs.redis
	Cross-AZ Deployment Check	Configuration change	dcs.redis
	DCS Redis Instances Are in the Specified VPC	Configuration change	dcs.redis
	DCS Redis Instances Do Not Have EIPs Attached	Configuration change	dcs.redis
	Access Mode Check	Configuration change	dcs.redis
FunctionGraph	**Concurrency Check**	Configuration change	fgs.functions
	Functions Are in the Specified VPC	Configuration change	fgs.functions
	Public Access Check	Configuration change	fgs.functions
	Basic Configuration Check	Configuration change	fgs.functions
	FunctionGraph Functions Have Log Collection Enabled	Configuration change	fgs.functions
Content Delivery Network (CDN)	**CDN Domains Use HTTPS Certificates**	Configuration change	cdn.domains

Service	Policy	Triggered By	Object
	Origin Protocol Policy Check	Configuration change	cdn.domains
	TLS Version Check	Configuration change	cdn.domains
	Certificate Source Check	Configuration change	cdn.domains
Config	The Resource Recorder Is Enabled	Periodic	Account
Data Warehouse Service (DWS)	KMS Encryption Check	Configuration change	dws.clusters
	DWS Clusters Have Enabled Log Transfer	Configuration change	dws.clusters
	DWS Clusters Have Enabled Automated Snapshots	Configuration change	dws.clusters
	DWS Clusters Use SSL	Configuration change	dws.clusters
	DWS Clusters Do Not Have EIPs Attached	Configuration change	dws.clusters
	O&M Time Window Check	Configuration change	dws.clusters
	DWS Clusters Are in Specified VPCs	Configuration change	dws.clusters
Data Replication Service (DRS)	Network Type Check for DR Tasks	Configuration change	drs.dataGuardJob
	Network Type Check for Migration Tasks	Configuration change	drs.migrationJob
	Network Type Check for Synchronization Tasks	Configuration change	drs.synchronizationJob

Service	Policy	Triggered By	Object
Data Encryption Workshop (DEW)	**Key Status Check**	Configuration change	kms.keys
	Key Rotation Has Been Enabled	Configuration change	kms.keys
	CSMS Secrets Are Rotated	Configuration change	csms.secrets
	CSMS Secrets Have Enabled Automatic Rotation	Configuration change	csms.secrets
	CSMS Secrets Have Been Configured with Specified KMS Keys	Configuration change	csms.secrets
	CSMS Secrets Have Been Rotated Within the Specified Period	Periodic	csms.secrets
Identity and Access Management (IAM)	**Key Rotation Check**	Periodic	iam.users
	IAM Policies Do Not Allow Blocked Actions on KMS Keys	Configuration changes	iam.roles&iam.policies
	Each User Group Has at Least One User	Configuration change	iam.groups
	Password Strength Check	Configuration change	iam.users
	Unintended Policy Check	Configuration change	iam.users, iam.groups, iam.agencies
	Admin Permissions Check	Configuration change	iam.roles, iam.policies
	Custom Policies Do Not Allow All Actions for a Service	Configuration change	iam.roles, iam.policies
	The Root User Does Not Have Available Access Keys	Periodic	Account

Service	Policy	Triggered By	Object
	Access Mode Check	Configuration change	iam.users
	Access Key Check	Configuration change	iam.users
	IAM Users Are in Specified User Groups	Configuration change	iam.users
	Last Login Check	Periodic	iam.users
	Multi-Factor Authentication Check	Configuration change	iam.users
	A User Does Not have Multiple Active Access Keys	Configuration change	iam.users
	MFA Has Been Enabled for Console Login	Configuration change	iam.users
	The Root User Has MFA Enabled	Periodic	Account
	All IAM Policies Are in Use	Configuration change	iam.policies
	All IAM Roles Are in Use	Configuration change	iam.roles
	Login Protection Check	Periodic	iam.users
	IAM Agencies Contain Specified Policies	Configuration change	iam.agencies
	The Admin User Group Only Contains the Root User	Configuration change	iam.users
	IAM Users Do Not Have Directly Assigned Policies or Permissions	Configuration change	iam.users
Document Database Service (DDS)	**SSL Has Been Enabled**	Configuration change	dds.instances

Service	Policy	Triggered By	Object
	DDS Instance Type Check	Configuration change	dds.instances
	DDS Instances Do Not Have EPIs Attached	Configuration change	dds.instances
	DDS Instances Do Not Have Unallowed Ports Enabled	Configuration change	dds.instances
	DDS Instance Version Check	Configuration change	dds.instances
	DDS Instances Are in the Specified VPC	Configuration change	dds.instances
Simple Message Notification (SMN)	**Log Reporting to LTS Has Been Enabled**	Configuration change	smn.topic
Virtual Private Cloud (VPC)	**Idle ACL Check**	Configuration change	vpc.firewallGroups
	Default Security Group Check	Configuration change	vpc.securityGroups
	VPCs Have Enabled Flow Logs	Configuration change	vpc.vpcs
	Port Check	Configuration change	vpc.securityGroups
	Inbound Traffic Can Only Access Specified Ports	Configuration change	vpc.securityGroups
	SSH Check	Configuration change	vpc.securityGroups
	Access Control Check for Non-whitelisted Ports	Configuration change	vpc.securityGroups

Service	Policy	Triggered By	Object
	A Security Group is Attached to Elastic Network Interfaces	Configuration change	vpc.securityGroups
Virtual Private Network (VPN)	**Connection State Check**	Configuration change	vpnaas.vpnConnections, vpnaas.ipsec-site-connections
Cloud Eye	**Alarm Rules Are Enabled**	Configuration change	ces.alarms
	Alarm Rules Have Been Configured for Key Disablement and Deletion	Periodic	Account
	There Are Alarm Rules Configured for OBS Bucket Policy Changes	Periodic	Account
	Specified Resources Have Certain Metric Attached	Periodic	Account
	Alarm Rule Configurations Check	Configuration change	ces.alarms
	Alarms Have Been Created for VPC Changes	Periodic	Account
Cloud Container Engine (CCE)	**CCE Clusters Are Supported for Maintenance**	Configuration change	cce.clusters
	Oldest Supported Version Check	Configuration change	cce.clusters
	CCE Clusters Do Not Have EIPs Attached	Configuration change	cce.clusters
	Flavor Check	Configuration change	cce.clusters
	CCE Clusters Are in Specified VPCs	Configuration change	cce.clusters

Service	Policy	Triggered By	Object
Cloud Trace Service (CTS)	**CTS Trackers Have Traces Encrypted**	Configuration change	cts.trackers
	CTS Trackers Have Trace Transfer to LTS Enabled	Configuration change	cts.trackers
	CTS Trackers Have Been Created for the Specified OBS Bucket	Periodic	Account
	Trace File Verification Is Enabled	Configuration change	cts.trackers
	At Least One Tracker Is Enabled	Periodic	Account
	There Are CTS Trackers In the Specified Regions	Periodic	Account
	CTS Trackers Comply with Security Best Practices	Periodic	Account
Relational Database Service (RDS)	**Error Log Collection Is Enabled for RDS Instances**	Configuration change	rds.instances
	Error Log Collection Is Enabled for RDS Instances	Configuration change	rds.instances
	RDS Instances Support Slow Query Logs	Configuration change	rds.instances
	Single-AZ Cluster Check	Configuration change	rds.instances
	RDS Instances Do Not Have EIPs Attached	Configuration change	rds.instances
	RDS Instances Use KMS Encryption	Configuration change	rds.instances
	RDS Instances Are in the Specified VPC	Configuration change	rds.instances
	Both Error Logs and Slow Query Logs Are Collected for RDS Instances	Configuration change	rds.instances

Service	Policy	Triggered By	Object
	Flavor Check	Configuration change	rds.instances
	RDS Instances Have SSL Enabled	Configuration change	rds.instances
	RDS Instance Port Check	Configuration change	rds.instances
	Version Check for RDS Instance Engines	Configuration change	rds.instances
	RDS Instances Have Audit Log Enabled	Configuration change	rds.instances
GaussDB	GaussDB Instances Are in the Specified VPC	Configuration change	gaussdb.instance
	Audit Log Collection Is Enabled	Configuration change	gaussdb.instance
	Automated Backup Is Enabled	Configuration change	gaussdb.instance
	Error Log Collection Is Enabled	Configuration change	gaussdb.instance
	Slow Query Log Collection Is Enabled	Configuration change	gaussdb.instance
	GaussDB Instances Do Not Have EIPs Attached	Configuration change	gaussdb.instance
	Cross-AZ Deployment Check	Configuration change	gaussdb.instance
	Data Transmission Encryption Is Enabled	Configuration change	gaussdb.instance

Service	Policy	Triggered By	Object
TaurusDB	**The Audit Log Is Enabled**	Configuration change	gaussdbformysql.instance
	Backup Is Enabled	Configuration change	gaussdbformysql.instance
	The Error Log Is Enabled	Configuration change	gaussdbformysql.instance
	The Slow Query Log Is Enabled	Configuration change	gaussdbformysql.instance
	Data Transmission Encryption Is Enabled	Configuration change	gaussdbformysql.instance
	Cross-AZ Deployment Check	Configuration change	gaussdbformysql.instance
	EIP Check	Configuration change	gaussdbformysql.instance
	VPC Check	Configuration change	gaussdbformysql.instance
GeminiDB	**Single-AZ Instance Check**	Configuration change	nosql.instances
	GeminiDB Instances Have Backup Enabled	Configuration change	nosql.instances
	GeminiDB Instances Have Disk Encryption Enabled	Configuration change	nosql.instances
	GeminiDB Instances Have Error Log Collection Enabled	Configuration change	nosql.instances
	GeminiDB Instances Have the Slow Log Enabled	Configuration change	nosql.instances

Service	Policy	Triggered By	Object
Cloud Search Service (CSS)	CSS Clusters Have the Security Mode Enabled	Configuration change	css.clusters
	The Snapshot Function Is Enabled for CSS Clusters	Configuration change	css.clusters
	Disk Encryption Is Enabled for CSS Clusters	Configuration change	css.clusters
	HTTPS Access Is Enabled for CSS Clusters	Configuration change	css.clusters
	CSS Clusters Are in Specified VPCs	Configuration change	css.clusters
	Single-AZ CSS Cluster Check	Configuration change	css.clusters
	A CSS Cluster Has at Least Two Instances	Configuration change	css.clusters
	CSS Clusters Are Not Publicly Accessible	Configuration change	css.clusters
	CSS Clusters Support the Security Mode	Configuration change	css.clusters
	CSS Clusters Have Access Control Enabled	Configuration change	css.clusters
	CSS Clusters Have Kibana Public Access Control Enabled	Configuration change	css.clusters
	CSS Clusters Have Slow Query Log Enabled	Configuration change	css.clusters
Elastic Volume Service (EVS)	EVS Disk Type Check	Configuration changes	evs.volumes

Service	Policy	Triggered By	Object
	Disks Are Used Within the Specified Time	Periodic	evs.volumes
	Idle EVS Disk Check	Configuration changes	evs.volumes
	EVS Disks Are Encrypted	Configuration change	evs.volumes
	Disk Encryption Are Enabled	Configuration change	evs.volumes
	EVS Disks Have Backup Vaults Attached	Configuration change	evs.volumes
	EVS Backup Time Check	Periodic	evs.volumes
Cloud Certificate Manager (CCM)	**Private CAs Expiration Check**	Periodic	pca.ca
	Expiration Check for Private Certificates	Periodic	pca.cert
	Private Root CAs Are Disabled	Periodic	pca.ca
	Private CA Algorithm Check	Configuration change	pca.ca, pca.cert
Distributed Message Service (for Kafka)	**DMS Kafka Instances Have SSL Enabled for Private Access**	Configuration change	dms.kafka
	DMS Kafka Instances Have Enabled SSL for Public Access	Configuration change	dms.kafka
	DMS Kafka Instances Are Not Publicly Accessible	Configuration change	dms.kafka
Distributed Message Service (DMS) for RabbitMQ	**RabbitMQ Instances Have SSL Enabled**	Configuration change	dms.rabbitmqs
	DMS RabbitMQ Instances Have Public Access Enabled	Configuration change	dms.rabbitmqs

Service	Policy	Triggered By	Object
Distributed Message Service for RocketMQ (for RocketMQ)	**DMS RocketMQ Instances Have SSL Enabled**	Configuration change	dms.reliabilitys
	RocketMQ Allows Public Access	Configuration change	dms.reliabilitys
Organizations	**Accounts Have Been Added to Organizations**	Periodic	Account
Cloud Firewall (CFW)	**CFW Instances Have Protection Policies Attached**	Configuration change	cfw.cfw_instance
Cloud Backup and Recovery (CBR)	**Backup Encryption Check**	Configuration change	cbr.backup
	Backup Policy Execution Frequency Check	Configuration change	cbr.policy
	Minimum Retention Days of CBR Vault	Configuration change	cbr.vault
Object Storage Service (OBS)	**OBS Bucket Policies Do Not Allow Blacklisted Actions**	Configuration change	obs.buckets
	OBS Bucket Policies Only Allow Access from the Specified Objects	Configuration change	obs.buckets
	Permission Boundary Check	Configuration change	obs.buckets
	OBS Bucket Policies Do Not Allow Public Read Access	Configuration change	obs.buckets
	OBS Bucket Policies Do Not Allow Public Write Access	Configuration change	obs.buckets
	OBS Buckets Do Not Allow HTTP Requests	Configuration change	obs.buckets

Service	Policy	Triggered By	Object
Image Management Service (IMS)	**Private Images Have Encryption Enabled**	Configuration change	ims.images
Bare Metal Server (BMS)	**BMSs Have Key Pair Login Enabled**	Configuration change	bms.servers
Graph Engine Service (GES)	**GES Graphs Are Encrypted Using KMS**	Configuration change	ges.graphs
	GES Graphs Have LTS Enabled	Configuration change	ges.graphs
	GES Graphs Support Cross-AZ HA	Configuration change	ges.graphs

3.6.2 General Policies

3.6.2.1 Resource Names Meet Regular Expression Requirements

Rule Details

Table 3-14 Rule details

Parameter	Description
Rule Name	regular-matching-of-names
Identifier	regular-matching-of-names
Description	If a resource name that does not comply with regular expression requirements, this resource name is 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.

3.6.2.2 Resources Have All the Specified Tags Attached

Rule Details

Table 3-15 Rule details

Parameter	Description
Rule Name	required-all-tags
Identifier	required-all-tags
Description	If a resource is missing any of the specified tags, this resource is noncompliant.
Tag	tag
Trigger Type	Configuration change
Filter Type	**Supported Services and Resources**
Configure Rule Parameters	● TagKeys: Indicates the specified tag keys. ● TagValues: Indicates the specified tag values.

3.6.2.3 Resources Have One of the Specified Tags Attached

Rule Details

Table 3-16 Rule details

Parameter	Description
Rule Name	required-tag-exist
Identifier	required-tag-exist
Description	If a resource is missing all the specified tags, this resource is noncompliant.
Tag	tag
Trigger Type	Configuration change
Filter Type	**Supported Services and Resources**
Configure Rule Parameters	● TagKeys: Indicates the specified tags. ● TagValues: Indicates the specified tag values.

3.6.2.4 Tag Prefixes and Suffixes Check

Rule Details

Table 3-17 Rule details

Parameter	Description
Rule Name	resource-tag-key-prefix-suffix
Identifier	resource-tag-key-prefix-suffix
Description	If a resource does not have any tags that are specified with specific key prefixes and suffixes, this resource is not compliant.
Tag	tag
Trigger Type	Configuration change
Filter Type	**Supported Services and Resources**
Configure Rule Parameters	● tagKeyPrefix: Indicates a tag key prefix. An empty string indicates that all tag key prefixes are allowed. ● tagKeySuffix: Indicates a tag key suffix. An empty string indicates that all tag key sffixes are allowed.

3.6.2.5 Resources Have at Least One Tags Attached

Rule Details

Table 3-18 Rule details

Parameter	Description
Rule Name	resource-tag-not-empty
Identifier	resource-tag-not-empty
Description	If a resource is not tagged, this resource is noncompliant.
Tag	tag
Trigger Type	Configuration change
Filter Type	**Supported Services and Resources**
Configure Rule Parameters	None

3.6.2.6 Resource Tag Check

Rule Details

Table 3-19 Rule details

Parameter	Description
Rule Name	required-tag-check
Identifier	required-tag-check
Description	If a resource does not have the specified tag attached, this resource is considered noncompliant.
Tag	tag
Trigger Type	Configuration change
Filter Type	**Supported Services and 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.

3.6.2.7 Resources Are in Specified Enterprise Projects

Rule Details

Table 3-20 Rule details

Parameter	Description
Rule Name	resource-in-enterprise-project
Identifier	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.

3.6.2.8 Resources Are in Specified Regions

Rule Details

Table 3-21 Rule details

Parameter	Description
Rule Name	resources-in-supported-region
Identifier	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, set this parameter to **global**.

3.6.2.9 Resource Type Check by Specifying Allowed Resource Types

Rule Details

Table 3-22 Rule Details

Parameter	Description
Rule Name	resources-in-allowed-types
Identifier	resources-in-allowed-types
Description	If a resource type does not match any of the specified resource types, this resource type is noncompliant.
Tag	type
Trigger Type	Configuration change
Filter Type	All resources
Rule Parameter	**providerAndTypes**: resource types. The value format is ['provider.type'].

3.6.2.10 Resource Type Check by Specifying Unallowed Resource Types

Rule Details

Table 3-23 Rule details

Parameter	Description
Rule Name	resources-in-not-allowed-types
Identifier	resources-in-not-allowed-types
Description	If a resource type matches one of the specified resource types, this resource type is noncompliant.
Tag	type
Trigger Type	Configuration change
Filter Type	All resources
Rule Parameter	providerAndTypes: Resource types. The value format is ['provider.type'].

3.6.3 API Gateway

3.6.3.1 Dedicated API Gateways Have an Authorization Type Set

Rule Details

Table 3-24 Rule details

Parameter	Description
Rule Name	apig-instances-authorization-type-configured
Identifier	apig-instances-authorization-type-configured
Description	If a dedicated APIG gateway does not have any types of API authentication configured, this APIG gateway is noncompliant.
Tag	apig
Trigger Type	Configuration change
Filter Type	apig.instances
Configure Rule Parameters	None

3.6.3.2 Dedicated API Gateways Have Logging Enabled

Rule Details

Table 3-25 Rule details

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

3.6.3.3 Dedicated API Gateways Use SSL certificates

Rule Details

Table 3-26 Rule details

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

3.6.4 CodeArts Deploy

3.6.4.1 Clusters Are Available

Rule Details

Table 3-27 Rule details

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

3.6.4.2 Project Parameter Encryption Check

Rule Details

Table 3-28 Rule details

Parameter	Description
Rule Name	cloudbuildserver-encryption-parameter-check
Identifier	cloudbuildserver-encryption-parameter-check
Description	If encryption is not enabled for custom parameters of a CodeArts project, this project is noncompliant.
Tag	codeartsbuild
Trigger Type	Configuration change
Filter Type	codeartsbuild.CloudBuildServer
Rule Parameter	None

3.6.5 MapReduce Service

3.6.5.1 MRS Clusters Have Specified Security Groups Attached

Rule Details

Table 3-29 Rule details

Parameter	Description
Rule Name	mrs-cluster-in-allowed-security-groups
Identifier	mrs-cluster-in-allowed-security-groups
Description	If an MRS cluster does not have any of the specified security groups attached, this cluster is noncompliant.
Tag	mrs
Trigger Type	Configuration change
Filter Type	mrs.mrs
Configure Rule Parameters	**mrsSecurityGroupsId**: indicates a security group ID. This is an array type parameter.

3.6.5.2 MRS Clusters Are in Specified VPCs

Rule Details

Table 3-30 Rule Details

Parameter	Description
Rule Name	mrs-cluster-in-vpc
Identifier	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**: VPC ID of an MRS cluster

Applicable Scenario

A VPC is a private network on the cloud. You can create VPCs to logically isolate your MRS clusters. For more details, see **What Is Virtual Private Cloud?**

Solution

You cannot change the VPC of an MRS cluster. Exercise caution when selecting a VPC when creating resources. However, changing VPC subnets is supported. For details, see **Changing the VPC Subnet of an MRS Cluster**.

Rule Logic

- If an MRS cluster is not in the specified VPC, this cluster is noncompliant.
- If an MRS cluster is in the specified VPC, this cluster is compliant.

3.6.5.3 MRS Clusters Have Kerberos Enabled

Rule Details

Table 3-31 Rule details

Parameter	Description
Rule Name	mrs-cluster-kerberos-enabled
Identifier	mrs-cluster-kerberos-enabled
Description	If kerberos 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

3.6.5.4 MRS Clusters Support Multi-AZ Deployment

Rule Details

Table 3-32 Rule details

Parameter	Description
Rule Name	mrs-cluster-multiAZ-deployment
Identifier	mrs-cluster-multiAZ-deployment
Description	If an MRS cluster does not support multi-AZ deployment, this cluster is noncompliant.
Tag	mrs
Trigger Type	Configuration change

Parameter	Description
Filter Type	mrs.mrs
Configure Rule Parameters	None

3.6.5.5 MRS Clusters Do Not Have EIPs Attached

Rule Details

Table 3-33 Rule details

Parameter	Description
Rule Name	mrs-cluster-no-public-ip
Identifier	mrs-cluster-no-public-ip
Description	If an MRS cluster has an EIP attached, this cluster is noncompliant.
Tag	mrs
Trigger Type	Configuration change
Filter Type	mrs.mrs
Configure Rule Parameters	None

3.6.5.6 MRS Clusters Have KMS Encryption Enabled

Rule Details

Table 3-34 Rule details

Parameter	Description
Rule Name	mrs-cluster-encrypt-enable
Identifier	mrs-cluster-encrypt-enable
Description	If KMS encryption is not enabled for an MRS cluster, this cluster is noncompliant.
Tag	mrs
Trigger Type	Configuration change
Filter Type	mrs.mrs

Parameter	Description
Configure Rule Parameters	None

3.6.6 NAT Gateway

3.6.6.1 Private NAT Private Gateways Are in Specified VPCs

Rule Details

Table 3-35 Rule details

Parameter	Description
Rule Name	private-nat-gateway-authorized-vpc-only
Identifier	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**: VPC IDs. If there are no VPCs specified, all values are allowed. This is an array type parameter. You can include up to 10 VPCs.

3.6.7 VPC Endpoint

3.6.7.1 VPC Endpoint Check for Specified Services

Rule Details

Table 3-36 Rule details

Parameter	Description
Rule Name	vpcep-endpoint-enabled
Identifier	vpcep-endpoint-enabled

Parameter	Description
Description	If there are no VPC endpoints for a specified service, this rule is noncompliant.
Tag	vpcep
Trigger Type	Periodic
Filter Type	Account
Configure rule parameters	serviceName: indicates the specified service name

3.6.8 Web Application Firewall

3.6.8.1 WAF Instances Have Protection Policies Attached

Rule Details

Table 3-37 Rule details

Parameter	Description
Rule name	waf-instance-policy-not-empty
Identifier	waf-instance-policy-not-empty
Description	If a WAF instance does not have a protection policy attached, this instance is noncompliant.
Tag	waf
Trigger Type	Configuration change
Filter Type	waf.instance
Configure Rule Parameters	None

3.6.8.2 WAF Protection Policies Are Not Empty

Rule Details

Table 3-38 Rule details

Parameter	Description
Rule Name	waf-policy-not-empty

Parameter	Description
Identifier	waf-policy-not-empty
Description	If no rules are added for a WAF protection policy, this policy is noncompliant.
Tag	waf
Trigger Type	Configuration change
Filter Type	waf.policy
Rule Parameter	None

3.6.8.3 WAF Instances Have Domain Name Protection Enabled

Rule Details

Table 3-39 Rule details

Parameter	Description
Rule Name	waf-instance-enable-protect
Identifier	instance-enable-protect
Description	If domain name protection is not enabled for a WAF instance, this instance is noncompliant.
Tag	waf
Trigger Type	Periodic
Filter Type	Account
Configure Rule Parameters	None

3.6.8.4 WAF Policies Have Geolocation Access Control Enabled

Rule Details

Table 3-40 Rule details

Parameter	Description
Rule Name	waf-policy-enable-geoip
Identifier	waf-policy-enable-geoip

Parameter	Description
Description	If there is a WAF protection policy that does not have geolocation access control configured or enabled, the current account is noncompliant.
Tag	waf
Trigger Type	Periodic
Filter Type	Account
Configure Rule Parameters	None

3.6.8.5 WAF Instances Have Block Policies Attached

Rule Details

Table 3-41 Rule details

Parameter	Description
Rule Name	waf-instance-enable-block-policy
Identifier	waf-instance-enable-block-policy
Description	If a WAF instance does not have a block policy associated, this instance is noncompliant.
Tag	waf
Trigger Type	Configuration change
Filter Type	waf.instance
Configure Rule Parameters	None

3.6.9 Elastic Load Balance

3.6.9.1 Load Balancers Do Not Have EIPs Attached

Rule Details

Table 3-42 Rule details

Parameter	Description
Rule Name	elb-loadbalancers-no-public-ip
Identifier	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

3.6.9.2 ELB Listeners Have Specified Security Policies Added

Rule Details

Table 3-43 Rule details

Parameter	Description
Rule Name	elb-predefined-security-policy-https-check
Identifier	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 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**.

3.6.9.3 ELB Listeners Are Configured with HTTPS

Rule Details

Table 3-44 Rule details

Parameter	Description
Rule Name	elb-tls-https-listeners-only
Identifier	elb-tls-https-listeners-only
Description	If any listener of a load balancer does not have the frontend protocol set to HTTPS, this load balancer is noncompliant.
Tag	elb
Trigger Type	Configuration change
Filter Type	elb.loadbalancers
Configure Rule Parameters	None

3.6.9.4 Weight Check for Backend Servers

Rule Details

Table 3-45 Rule details

Parameter	Description
Rule Name	elb-members-weight-check
Identifier	elb-members-weight-check
Description	If the weight of a backend server is 0 and the type of the forwarding rule is not SOURCE_IP, this rule 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

3.6.9.5 HTTPS Redirection Check

Rule Details

Table 3-46 Rule details

Parameter	Description
Rule Name	elb-http-to-https-redirection-check
Identifier	elb-http-to-https-redirection-check
Description	If requests to an HTTP listener cannot be redirected to an HTTPS listener, this HTTP listener is noncompliant.
Tag	elb
Trigger Type	Configuration change
Filter Type	elb.listeners
Rule Parameter	None

3.6.9.6 Single-AZ Load Balancer Check

Rule Details

Table 3-47 Rule details

Parameter	Description
Rule Name	elb-multiple-az-check
Identifier	elb-multiple-az-check
Description	If a load balancer is mapped to fewer than two AZs, this load balancer is noncompliant.
Tag	elb
Trigger Type	Configuration change
Filter Type	elb.loadbalancers
Rule Parameter	None

3.6.9.7 ELB Load Balancers Have Access Logging Configured

Rule Details

Table 3-48 Rule details

Parameter	Description
Rule Name	elb-logging-enabled
Identifier	elb-logging-enabled
Description	If a load balancer does not have access logging configured, this load balancer is noncompliant.
Tag	elb
Trigger Type	Configuration change
Filter Type	elb.loadbalancers
Configure Rule Parameters	None

Applicable Scenario

ELB logs HTTP, HTTPS, and TLS requests received by load balancers, including the time when the requests were sent, client IP addresses, request paths, and server responses.

If there are service faults or exceptions resulted from faulty services, you can check logs of requests to load balancers and analyze response status codes to quickly locate unhealthy backend servers. For details, see **Access Logging**.

Solution

You can configure access logging for noncompliant load balancers based on **Configuring Access Logging**.

Rule Logic

- If a load balancer does not have access logging configured, this load balancer is noncompliant.
- If a load balancer has access logging configured, this load balancer is compliant.

3.6.10 Elastic IP

3.6.10.1 Bandwidth Check

Rule Details

Table 3-49 Rule details

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

3.6.10.2 Idle Elastic IP Check

Rule Details

Table 3-50 Rule details

Parameter	Description
Rule Name	eip-unbound-check
Identifier	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

3.6.10.3 Elastic IPs Are Used Within a Given Period of Time

Rule Details

Table 3-51 Rule details

Parameter	Description
Rule Name	eip-use-in-specified-days
Identifier	eip-use-in-specified-days
Description	If an EIP is not used within the 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.

3.6.11 Auto Scaling

3.6.11.1 Priority Policy Check

Rule Details

Table 3-52 Rule details

Parameter	Description
Rule Name	as-capacity-rebalancing
Identifier	as-capacity-rebalancing
Description	If the priority policy EQUILIBRIUM_DISTRIBUTE is not enabled, this rule is noncompliant.
Tag	as
Trigger Type	Configuration change
Filter Type	as.scalingGroups
Configure Rule Parameters	None

3.6.11.2 AS Groups Are Associated with an Elastic Load Balancer that Uses Health Check

Rule Details

Table 3-53 Rule details

Parameter	Description
Rule Name	as-group-elb-healthcheck-required
Identifier	as-group-elb-healthcheck-required
Description	If an AS group is not using Elastic Load Balancing health check, this rule is noncompliant.
Tag	as
Trigger Type	Configuration change
Filter Type	as.scalingGroups
Configure Rule Parameters	None

3.6.11.3 Multi-AZ Deployment Has Been Configured

Rule Details

Table 3-54 Rule details

Parameter	Description
Rule Name	as-multiple-az
Identifier	as-multiple-az
Description	If an AS group is deployed in a single AZ, this AS group is noncompliant.
Tag	as
Trigger Type	Configuration change
Filter Type	as.scalingGroups
Configure Rule Parameters	None

3.6.11.4 IPv6 Bandwidth Check

Rule Details

Table 3-55 Rule details

Parameter	Description
Rule Name	as-group-ipv6-disabled
Identifier	as-group-ipv6-disabled
Description	If an IPv6 shared bandwidth is assigned to an AS group, this AS group is noncompliant
Tag	as
Trigger Type	Configuration change
Filter Type	as.scalingGroups
Rule Parameter	None

3.6.11.5 AS Groups Are in Specified VPCs

Rule Details

Table 3-56 Rule details

Parameter	Description
Rule Name	as-group-in-vpc
Identifier	as-group-in-vpc
Description	If an AS group is not in any of the specified VPCs, this AS group is noncompliant.
Tag	as
Trigger Type	Configuration change
Filter Type	as.scalingGroups
Configure Rule Parameters	**VpcIdList**: VPC IDs

Applicable Scenario

A VPC is a private network on the cloud. You can create VPCs to logically isolate your AS groups. For more details, see **What Is Virtual Private Cloud?**

Solution

You can redeploy noncompliant AS groups to required VPCs.

Rule Logic

- If an AS group is not in any of the specified VPCs, this AS group is noncompliant.
- If an AS group is in one of the specified VPCs, this AS group is compliant.

3.6.12 Scalable File Service Turbo (SFS Turbo)

3.6.12.1 SFS Turbo File Systems Have KMS Encryption Enabled

Rule Details

Table 3-57 Rule details

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

3.6.12.2 SFS Turbo Systems Are Associated with Backup Vaults

Rule Details

Table 3-58 Rule Details

Parameter	Description
Rule Name	sfsturbo-protected-by-cbr
Identifier	sfsturbo-protected-by-cbr
Description	If an SFS Turbo system is not associated with a backup vault, this system is noncompliant.

Parameter	Description
Tag	cbr, sfsturbo
Trigger Type	Configuration change
Filter Type	sfsturbo.shares
Rule Parameter	None

3.6.12.3 Backup Time Check

Rule Details

Table 3-59 Rule details

Parameter	Description
Rule Name	sfsturbo-last-backup-created
Identifier	sfsturbo-last-backup-created
Description	If an SFS Turbo system does not have a backup created within the specified period, this system is noncompliant.
Tag	cbr, sfsturbo
Trigger Type	Periodic
Filter Type	sfsturbo.shares
Configure Rule Parameters	**lastBackupAgeValue**: The required backup time interval (in hours) for SFS Turbo systems.

3.6.13 Elastic Cloud Server

3.6.13.1 Flavor Check

Rule Details

Table 3-60 Rule details

Parameter	Description
Rule Name	allowed-ecs-flavors
Identifier	allowed-ecs-flavors

Parameter	Description
Description	If an ECS's flavor is not one of the specified flavors, this ECS is noncompliant.
Tag	ecs
Trigger Type	Configuration change
Filter Type	ecs.cloudservers
Configure Rule Parameters	**listOfAllowedFlavors**: 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.

3.6.13.2 Image Check

Rule Details

Table 3-61 Rule details

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

3.6.13.3 Image Check by Tag

Rule Details

Table 3-62 Rule details

Parameter	Description
Rule Name	approved-ims-by-tag

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

3.6.13.4 Security Group Check by ID

Rule Details

Table 3-63 Rule details

Parameter	Description
Rule Name	ecs-in-allowed-security-groups
Identifier	ecs-in-allowed-security-groups
Description	If an ECS does not have any of the specified security groups attached, this ECS is noncompliant.
Tag	ecs
Trigger Type	Configuration change
Filter Type	ecs.cloudservers
Configure Rule Parameters	● **specifiedECSTagKey**: Tag key of an ECS. The value must be a string. ● **specifiedECSTagValue**: Tag value of an ECS tag. If no value is specified, all values are allowed. The value must be an array with up to 10 elements. ● **specifiedSecurityGroupIds**: IDs of security groups. The value must be an array with up to 10 elements.

3.6.13.5 VPC Check by ID

Rule Details

Table 3-64 Rule details

Parameter	Description
Rule Name	ecs-instance-in-vpc
Identifier	ecs-instance-in-vpc
Description	If an ECS is not in the specified VPC, this ECS is noncompliant.
Tag	ecs, vpc
Trigger Type	Configuration change
Filter Type	ecs.cloudservers
Configure Rule Parameters	**vpcId**: VPC ID of an ECS

Applicable Scenario

A VPC is a private network on the cloud. You can create VPCs to logically isolate your resources. When creating a VPC, you can configure security groups, VPN, IP address segments, and bandwidth. This facilitates internal network management and configuring, allowing you to change network configurations in a secure, convenient manner. Additionally, you can control ECS access within and across security groups to enhance security.

For more information about VPC, see **What Is Virtual Private Cloud?**

Solution

You cannot change the VPC of an ECS. Exercise cause when selecting a VPC.

Rule Logic

- If an ECS is not in the specified VPC, this ECS is noncompliant.
- If an ECS is in the specified VPC, this ECS is compliant.

3.6.13.6 ECSs Have Key Pairs Attached

Rule Details

Table 3-65 Rule details

Parameter	Description
Rule Name	ecs-instance-key-pair-login
Identifier	ecs-instance-key-pair-login
Description	If an ECS does not have a key pair configured, this ECS is noncompliant.
Tag	ecs
Trigger Type	Configuration change
Filter Type	ecs.cloudservers
Configure Rule Parameters	None

3.6.13.7 ECSs Cannot Be Accessed Through Public Networks

Rule Details

Table 3-66 Rule details

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

3.6.13.8 An ECS Does Not Have Multiple EIPs Attached

Rule Details

Table 3-67 Rule details

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

3.6.13.9 Idle ECS Check

Rule Details

Table 3-68 Rule details

Parameter	Description
Rule Name	stopped-ecs-date-diff
Identifier	stopped-ecs-date-diff
Description	If an ECS has been stopped for longer than the time allowed, and no operations have been performed on it, this ECS is noncompliant.
Tag	ecs
Trigger Type	Periodic
Filter Type	ecs.cloudservers
Configure Rule Parameters	**allowDays**: The number of days allowed. The value must be a string.

3.6.13.10 ECSs Have IAM Agencies Attached

Rule Details

Table 3-69 Rule details

Parameter	Description
Rule Name	ecs-instance-agency-attach-iam-agency
Identifier	ecs-instance-agency-attach-iam-agency
Description	If an ECS does not have any IAM agencies attached, this ECS is noncompliant.
Tag	ecs
Trigger Type	Configuration change
Filter Type	ecs.cloudservers
Rule Parameter	None

3.6.13.11 Image Check by Name

Rule Details

Table 3-70 Rule details

Parameter	Description
Rule Name	allowed-images-by-name
Identifier	allowed-images-by-name
Description	If an ECS does not have one of the specified images attached, this ECS is noncompliant. Images are specified by name.
Tag	ecs
Trigger Type	Configuration change
Filter Type	ecs.cloudservers
Rule Parameter	**imageNames**: names of images. This rule allows partial match of image names.

Rule Logic

- If the image of an ECS is fully or partially matched with one of the specified images by name, this ECS is compliant.

- If the image of an ECS is not fully or partially matched with one of the specified images by name, this ECS is noncompliant.

3.6.13.12 ECSs Have Backup Vaults Attached

Rule Details

Table 3-71 Rule details

Parameter	Description
Rule Name	ecs-protected-by-cbr
Identifier	ecs-protected-by-cbr
Description	If an ECS does not have a backup vault attached, this ECS is noncompliant.
Tag	cbr, ecs
Trigger Type	Configuration change
Filter Type	ecs.cloudservers
Rule Parameter	None

3.6.13.13 Backup Time Check

Rule Details

Table 3-72 Rule details

Parameter	Description
Rule Name	ecs-last-backup-created
Identifier	ecs-last-backup-created
Description	If an ECS does not have a backup created within the specified period, this ECS is noncompliant.
Tag	cbr, ecs
Trigger Type	Periodic
Filter Type	ecs.cloudservers
Configure Rule Parameters	**lastBackupAgeValue**: The required backup time interval (in hours) for ECSs.

3.6.13.14 ECSs Have HSS Agents Attached

Rule Details

Table 3-73 Rule details

Parameter	Description
Rule Name	ecs-attached-hss-agents-check
Identifier	ECSs Have HSS Agents Attached
Description	If an ECS does not have an HSS agent installed or the protection mode enabled, this ECS is noncompliant.
Tag	ecs
Trigger Type	Configuration change
Filter Type	ecs.cloudservers
Configure Rule Parameters	None

3.6.14 Distributed Cache Service

3.6.14.1 DCS Memcached Instances Support SSL

Rule Details

Table 3-74 Rule details

Parameter	Description
Name	dcs-memcached-enable-ssl
Identifier	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

3.6.14.2 DCS Memcached Instances Are in a Specified VPC

Rule Details

Table 3-75 Rule details

Parameter	Description
Rule Name	dcs-memcached-in-vpc
Identifier	dcs-memcached-in-vpc
Description	If a DCS Memcached 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**: The VPC ID. The value must be a string.

Applicable Scenario

A VPC is a private network on the cloud. You can create VPCs to logically isolate your DCS Memcached instances. For more details, see **What Is Virtual Private Cloud?**

Solution

You can redeploy noncompliant DCS Memcached instances to required VPCs. DCS Memcached has been discontinued. You are advised to use DCS for Redis instead. For details, see **Huawei Cloud Distributed Cache Service Memcached Is Discontinued**.

Rule Logic

- If a DCS Memcached instance is not in the specified VPC, this instance is noncompliant.
- If a DCS Memcached instance is in the specified VPC, this instance is compliant.

3.6.14.3 DCS Memcached Instances Do Not Have EIPs Attached

Rule Details

Table 3-76 Rule details

Parameter	Description
Rule Name	dcs-memcached-no-public-ip
Identifier	dcs-memcached-no-public-ip
Description	If a DCS Memcached instance has an EIP attached, this instance is noncompliant.
Tag	dcs
Trigger Type	Configuration change
Filter Type	dcs.memcached
Configure Rule Parameters	None

3.6.14.4 Access Mode Check

Rule Details

Table 3-77 Rule details

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

3.6.14.5 DCS Redis Instances Support SSL

Rule Details

Table 3-78 Rule details

Parameter	Description
Rule Name	dcs-redis-enable-ssl
Identifier	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

3.6.14.6 Cross-AZ Deployment Check

Rule Details

Table 3-79 Rule details

Parameter	Description
Rule Name	dcs-redis-high-tolerance
Identifier	cs-redis-high-tolerance
Description	If a DCS Redis instance does not have cross-AZ deployment enabled, this instance is noncompliant.
Tag	dcs
Trigger Type	Configuration change
Filter Type	dcs.redis
Configure Rule Parameters	None

3.6.14.7 DCS Redis Instances Are in the Specified VPC

Rule Details

Table 3-80 Rule details

Parameter	Description
Rule Name	dcs-redis-in-vpc
Identifier	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**: The VPC ID. The value must be a string.

Applicable Scenario

A VPC is a private network on the cloud. You can create VPCs to logically isolate your DCS Redis instances. For more details, see **What Is Virtual Private Cloud?**

Solution

You can redeploy noncompliant DCS Redis instances to required VPCs. For details, see **Viewing and Modifying Basic Settings of a DCS Instance**.

Rule Logic

- If a DCS Redis instance is not in the specified VPC, this instance is noncompliant.
- If a DCS Redis instance is in the specified VPC, this instance is compliant.

3.6.14.8 DCS Redis Instances Do Not Have EIPs Attached

Rule Details

Table 3-81 Rule details

Parameter	Description
Rule Name	dcs-redis-no-public-ip
Identifier	dcs-redis-no-public-ip

Parameter	Description
Description	If a DCS Redis instance has an EIP attached, this instance is noncompliant.
Tag	dcs
Trigger Type	Configuration change
Filter Type	dcs.redis
Configure Rule Parameters	None

3.6.14.9 Access Mode Check

Rule Details

Table 3-82 Rule details

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

3.6.15 FunctionGraph

3.6.15.1 Concurrency Check

Rule Details

Table 3-83 Rule details

Parameter	Description
Rule Name	function-graph-concurrency-check

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

3.6.15.2 Functions Are in the Specified VPC

Rule Details

Table 3-84 Rule details

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

3.6.15.3 Public Access Check

Rule Details

Table 3-85 Rule details

Parameter	Description
Rule Name	function-graph-public-access-prohibited
Identifier	function-graph-public-access-prohibited
Description	If a function can be accessed over a public network, this function is noncompliant.
Tag	fgs
Trigger Type	Configuration change
Filter Type	fgs.functions
Configure Rule Parameters	None

3.6.15.4 Basic Configuration Check

Rule Details

Table 3-86 Rule details

Parameter	Description
Rule Name	function-graph-settings-check
Identifier	function-graph-settings-check
Description	If the runtime, timeout, or memory limit of a function is not within the specified ranges, this function is noncompliant.
Tag	fgs
Trigger Type	Configuration change
Filter Type	fgs.functions
Configure Rule Parameters	● **runtimeList**: runtime identifiers, such as Python3.6 ● **timeout**: execution timeout, in seconds ● **memorySize**: memory size of a function instance, in MB

Rule Logic

- If the runtime of a FunctionGraph function is not within the specified runtimes, this function is noncompliant.
- If the execution timeout of a FunctionGraph function is greater than the specified timeout, this function is noncompliant.
- If the memory size of a FunctionGraph function is greater than the specified memory size, this function is noncompliant.
- If a function does not meet any of the above conditions, this function is noncompliant.

3.6.15.5 FunctionGraph Functions Have Log Collection Enabled

Rule Details

Table 3-87 Rule details

Parameter	Description
Rule Name	function-graph-logging-enabled
Identifier	function-graph-logging-enabled
Description	If a function does not have log collection enabled, this function is noncompliant.
Tag	fgs
Trigger Type	Configuration change
Filter Type	fgs.functions
Configure Rule Parameters	None

3.6.16 Content Delivery Network (CDN)

3.6.16.1 CDN Domains Use HTTPS Certificates

Rule Details

Table 3-88 Rule details

Parameter	Description
Rule Name	cdn-enable-https-certificate
Identifier	cdn-enable-https-certificate

Parameter	Description
Description	If a domain does not have an HTTPS certificate configured, this domain is noncompliant.
Tag	cdn
Trigger Type	Configuration change
Filter Type	cdn.domains
Configure Rule Parameters	None

3.6.16.2 Origin Protocol Policy Check

Rule Details

Table 3-89 Rule details

Parameter	Description
Rule Name	cdn-origin-protocol-no-http
Identifier	cdn-origin-protocol-no-http
Description	If a domain does not have HTTPS configured for communication between CDN and origins, this domain is noncompliant.
Tag	cdn
Trigger Type	Configuration change
Filter Type	cdn.domains
Configure Rule Parameters	None

3.6.16.3 TLS Version Check

Rule Details

Table 3-90 Rule details

Parameter	Description
Rule Name	cdn-security-policy-check
Identifier	cdn-security-policy-check

Parameter	Description
Description	If a domain uses a TLS version earlier than version 1.2, this domain is noncompliant.
Tag	cdn
Trigger Type	Configuration change
Filter Type	cdn.domains
Configure Rule Parameters	None

3.6.16.4 Certificate Source Check

Rule Details

Table 3-91 Rule details

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

3.6.17 Config

3.6.17.1 The Resource Recorder Is Enabled

Rule Details

Table 3-92 Rule details

Parameter	Description
Rule Name	tracker-config-enabled-check

Parameter	Description
Identifier	tracker-config-enabled-check
Description	If the resource recorder is not enabled, this rule is noncompliant.
Tag	config
Trigger Type	Periodic
Filter Type	Account
Configure Rule Parameters	None

3.6.18 Data Warehouse Service

3.6.18.1 KMS Encryption Check

Rule Details

Table 3-93 Rule details

Parameter	Description
Rule Name	dws-enable-kms
Identifier	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

3.6.18.2 DWS Clusters Have Enabled Log Transfer

Rule Details

Table 3-94 Rule details

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

3.6.18.3 DWS Clusters Have Enabled Automated Snapshots

Rule Details

Table 3-95 Rule details

Parameter	Description
Rule Name	dws-enable-snapshot
Identifier	dws-enable-snapshot
Description	If automated 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

3.6.18.4 DWS Clusters Use SSL

Rule Details

Table 3-96 Rule details

Parameter	Description
Rule Name	dws-enable-ssl
Identifier	dws-enable-ssl
Description	If SSL 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

3.6.18.5 DWS Clusters Do Not Have EIPs Attached

Rule Details

Table 3-97 Rule details

Parameter	Description
Rule Name	dws-clusters-no-public-ip
Identifier	dws-clusters-no-public-ip
Description	If a DWS cluster has an EIP attached, this cluster is noncompliant.
Tag	dws
Trigger Type	Configuration change
Filter Type	dws.clusters
Rule Parameter	None

3.6.18.6 O&M Time Window Check

Rule Details

Table 3-98 Rule details

Parameter	Description
Rule Name	dws-maintain-window-check
Identifier	dws-maintain-window-check
Description	If the O&M time window of a DWS cluster is not consistent with the specified time window, this cluster is noncompliant.
Tag	dws
Trigger Type	Configuration change
Filter Type	dws.clusters
Rule Parameter	● **maintainDay**: Date of the O&M time window. ● **maintainStartTime**: Start time of the O&M time window.

3.6.18.7 DWS Clusters Are in Specified VPCs

Rule Details

Table 3-99 Rule details

Parameter	Description
Rule Name	dws-clusters-in-vpc
Identifier	dws-clusters-in-vpc
Description	If a DWS cluster is not in any of the specified VPCs, this cluster is noncompliant.
Tag	dws
Trigger Type	Configuration change
Filter Type	dws.clusters
Configure Rule Parameters	**VpcIdList**: VPC IDs

Applicable Scenario

A VPC is a private network on the cloud. You can create VPCs to logically isolate your DWS clusters. For more details, see **What Is Virtual Private Cloud?**

Solution

You can redeploy noncompliant DWS clusters to required VPCs.

Rule Logic

- If a DWS cluster is not in any of the specified VPCs, this cluster is noncompliant.
- If a DWS cluster is in one of the specified VPCs, this cluster is compliant.

3.6.19 Data Replication Service

3.6.19.1 Network Type Check for DR Tasks

Rule Details

Table 3-100 Rule details

Parameter	Description
Rule Name	drs-data-guard-job-not-public
Identifier	drs-data-guard-job-not-public
Description	If the network type of a DR task is not set to public network, this task is noncompliant.
Tag	drs
Trigger Type	Configuration change
Filter Type	drs.dataGuardJob
Configure Rule Parameters	None

3.6.19.2 Network Type Check for Migration Tasks

Rule Details

Table 3-101 Rule details

Parameter	Description
Rule Name	drs-migration-job-not-public

Parameter	Description
Identifier	drs-migration-job-not-public
Description	If the network type of a migration task is not set to public network, this task is noncompliant.
Tag	drs
Trigger Type	Configuration change
Filter Type	drs.migrationJob
Configure Rule Parameters	None

3.6.19.3 Network Type Check for Synchronization Tasks

Rule Details

Table 3-102 Rule details

Parameter	Description
Rule Name	drs-synchronization-job-not-public
Identifier	drs-synchronization-job-not-public
Description	If the network type of a synchronization task is not set to public network, this task is noncompliant.
Tag	drs
Trigger Type	Configuration change
Filter Type	drs.synchronizationJob
Configure Rule Parameters	None

3.6.20 Data Encryption Workshop

3.6.20.1 Key Status Check

Rule Details

Table 3-103 Rule details

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

3.6.20.2 Key Rotation Has Been Enabled

Rule Details

Table 3-104 Rule details

Parameter	Description
Rule Name	kms-rotation-enabled
Identifier	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

3.6.20.3 CSMS Secrets Are Rotated

Rule Details

Table 3-105 Rule details

Parameter	Description
Rule Name	csms-secrets-rotation-success-check
Identifier	csms-secrets-rotation-success-check
Description	If a CSMS secret fails to be rotated, this secret is noncompliant.
Tag	csms
Trigger Type	Configuration change
Filter Type	csms.secrets
Rule Parameter	None

3.6.20.4 CSMS Secrets Have Enabled Automatic Rotation

Rule Details

Table 3-106 Rule details

Parameter	Description
Rule Name	csms-secrets-auto-rotation-enabled
Identifier	csms-secrets-auto-rotation-enabled
Description	If a CSMS does not have automatic rotation enabled, this secret is noncompliant.
Tag	csms
Trigger Type	Configuration change
Filter Type	csms.secrets
Configure Rule Parameters	None

Applicable Scenario

Secret rotation enables you to periodically rotate your secret, so that even if your secret is leaked, unauthorized users can only use your secret during the non-rotated period. You are advised to configure a proper rotation interval for your secrets.

Solution

You can enable automatic secret rotation and configure a proper **rotation policy** and interval.

Rule Logic

- If a CSMS secret does not have automatic rotation enabled, this secret is noncompliant.
- If a CSMS secret has automatic rotation enabled, this secret is compliant.

3.6.20.5 CSMS Secrets Have Been Configured with Specified KMS Keys

Rule Details

Table 3-107 Rule details

Parameter	Description
Rule Name	csms-secrets-using-cmk
Identifier	csms-secrets-using-cmk
Description	If a CSMS secret has not been configured with one of the specified KMS keys, this secret is noncompliant.
Tag	csms
Trigger Type	Configuration change
Filter Type	csms.secrets
Configure Rule Parameters	**kmsIdList**: KMS key IDs. This value must be an array.

3.6.20.6 CSMS Secrets Have Been Rotated Within the Specified Period

Rule Details

Table 3-108 Rule details

Parameter	Description
Rule Name	csms-secrets-periodic-rotation
Identifier	csms-secrets-periodic-rotation
Description	If a CSMS secret has not been rotated within the specified period, this secret is noncompliant.
Tag	csms
Trigger Type	Periodic

Parameter	Description
Filter Type	csms.secrets
Configure Rule Parameters	**maxRotationDays**: maximum number of days that a secret is allowed to remain not rotated. The default value is **90**.

Applicable Scenario

Secret rotation enables you to periodically rotate your secret, so that even if your secret is leaked, unauthorized users can only use your secret during the non-rotated period. You are advised to configure a proper rotation interval for your secrets.

Solution

You can enable automatic secret rotation and configure a proper **rotation policy** and interval.

Rule Logic

- If less time has passed since a CSM secret was created than the specified period, the secret is compliant.
- If more time has passed since a CSMS secret was created than the specified period, and within the specified period, the secret has not been rotated, the secret is noncompliant.
- If more time has passed since a CSMS secret was created than the specified period, and within the specified period, the secret has been rotated, the secret is compliant.

3.6.21 Identity and Access Management

3.6.21.1 Key Rotation Check

Rule Details

Table 3-109 Rule details

Parameter	Description
Rule Name	access-keys-rotated
Identifier	access-keys-rotated
Description	If an IAM user's access key has not been rotated within the specified number of days, this user is noncompliant.
Tag	iam

Parameter	Description
Trigger Type	Periodic
Filter Type	iam.users
Configure Rule Parameters	**maxAccessKeyAge**: the maximum number of days that the AK/SK is allowed to remain unchanged. The default value is 90.

Applicable Scenario

Access keys (AK/SK) are commonly used for API access in an enterprise. Rotating access keys regularly can help to reduce security threats, such as key leakage.

Solution

You can create two keys to use them alternately and periodically create a new key to rotate out the old one. For more details, see **Periodically Change Your Identity Credentials**.

Rule Logic

- If an IAM user does not have an access key, the IAM user is compliant.
- If an IAM user is disabled, the IAM user is compliant.
- If an IAM user is in the enabled state, and its access key has been rotated within the specified period, this user is compliant.
- If an IAM user is in the enabled state, but its access key has not been rotated within the specified period, this user is noncompliant.

3.6.21.2 IAM Policies Do Not Allow Blocked Actions on KMS Keys

Rule Details

Table 3-110 Rule details

Parameter	Description
Rule Name	iam-customer-policy-blocked-kms-actions
Identifier	iam-customer-policy-blocked-kms-actions
Description	If an IAM policy allows any blocked actions on KMS keys, this policy is noncompliant.
Tag	obs, access-analyzer-verified
Trigger Type	Configuration change
Filter Type	iam.roles, iam.policies

Parameter	Description
Configure Rule Parameters	**blockedActionsPatterns**: indicates blocked actions for KMS. The value must be an array.

Applicable Scenario

This rule allows you to apply the principles of least privilege and separation of duties to access control. With this rule, you can detect IAM policies that allow blocked actions on KMS keys to prevent unintended data encryption and decryption.

Solution

You can modify noncompliant IAM policies based on the evaluation results. For more details, see **Modifying or Deleting a Custom Policy**.

Rule Logic

- If an IAM policy or role does not allow the specified blocked actions on KMS keys, this policy or role is compliant.
- If an IAM policy or role allows the specified blocked actions on KMS keys, this policy or role is noncompliant.

3.6.21.3 Each User Group Has at Least One User

Rule Details

Table 3-111 Rule details

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

Applicable Scenario

Users inherit permissions from their user groups. Adding or removing users from a user group allows you to efficiently manage user permissions. This rule allows you to detect user groups that do not have any users.

Solution

The administrator can assign permissions to user groups and add users to these groups. For more details, see **Adding Users to or Removing Users from a User Group**

Rule Logic

- If an IAM user group has no users, this user group is noncompliant.
- If an IAM user group has one or more users, this user group is compliant.

3.6.21.4 Password Strength Check

Rule Details

Table 3-112 Rule details

Parameter	Description
Rule Name	iam-password-policy
Identifier	iam-password-policy
Description	If the password of an IAM user does not meet the password strength requirements, this IAM 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**. **NOTE** Password strength: ● Strong: A password contains 8 to 32 characters and must include at least three character types among uppercase letters, lowercase letters, digits, special characters, and spaces. ● Medium: A password contains 8 to 32 characters and two character types among uppercase letters, lowercase letters, digits, special characters, and spaces. ● Low: A password contains 8 to 32 characters with the same type. The character type can be uppercase letters, lowercase letters, digits, special characters or spaces.

Applicable Scenario

This rule allows you to detect passwords that do not meet the specified password strength requirements. For more details, see **Set a Strong Password Policy**.

Solution

You can modify noncompliant passwords. For details, see **Changing the Login Password of an IAM User**.

Rule Logic

- If an IAM user does not have a password configured, this user is compliant.
- If an IAM user is in the disabled state, this user is compliant.
- If an IAM user is in the enabled state and their password meets the specified strength requirements, this user is compliant.
- If an IAM user is in the enabled state and their password does not neet the specified strength requirements, this user is noncompliant

3.6.21.5 Unintended Policy Check

Rule Details

Table 3-113 Rule details

Parameter	Description
Rule Name	iam-policy-blacklisted-check
Identifier	iam-policy-blacklisted-check
Description	If a blacklisted policy is attached to an IAM user, a user group, or an agency, this 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**: URNs of IAM policies. Built-in policies are not supported.

Applicable Scenario

This rule allows you to ensure that only intended permissions are assigned to an IAM user, a user group, or an IAM agency. For more details, see **Grant Least Privilege**.

Solution

You can revoke unintended permissions from noncompliant IAM users, user groups, and agencies.

Rule Logic

- If an IAM user, a user group, or an agency has an unintended policy attached, this user, user group, or agency is noncompliant.
- If an IAM user, a user group, or an agency does not have an unintended policy attached, this user, user group, or agency is compliant.

3.6.21.6 Admin Permissions Check

Rule Details

Table 3-114 Rule details

Parameter	Description
Rule Name	iam-policy-no-statements-with-admin-access
Identifier	iam-policy-no-statements-with-admin-access
Description	If a custom policy or role allows all actions (with the action element set to ***:*:***, ***:***, or *****) for all cloud services, this policy or role is noncompliant.
Tag	iam
Trigger Type	Configuration change
Filter Type	iam.roles, iam.policies
Configure Rule Parameters	None

Applicable Scenario

This rule allows you to detect IAM users, user groups, and agencies that have unintended policies attached. An IAM policy with the action element set to ***:*:***, ***:***, or ***** is of high security risk.

Solution

The administrator can modify noncompliant IAM policies or roles. For more details, see **Modifying or Deleting a Custom Policy**.

Rule Logic

- If a custom policy or role allows all actions (with the action element set to ***:*:***, ***:***, or *****) for all cloud services, this policy or role is noncompliant.

- If a custom policy or role does not allow all actions for all cloud services, this policy or role is compliant.

3.6.21.7 Custom Policies Do Not Allow All Actions for a Service

Rule Details

Table 3-115 Rule details

Parameter	Description
Rule Name	iam-role-has-all-permissions
Identifier	iam-role-has-all-permissions
Description	If a custom policy or role allows all actions for a cloud service, this policy or role is noncompliant.
Tag	iam
Trigger Type	Configuration change
Filter Type	iam.roles, iam.policies
Configure Rule Parameters	None

Applicable Scenario

This rule allows you to ensure that your IAM users or agencies do not have unintended permissions attached. To ensure resource security, an IAM role or policy should not allow all actions for a cloud service.

Solution

The administrator can modify noncompliant IAM policies or roles. For more details, see **Modifying or Deleting a Custom Policy**.

Rule Logic

- If a custom policy or role allows all actions for a cloud service, this policy or role is noncompliant.
- If a custom policy or role denies one or more actions for a cloud service, this policy or role is compliant.

3.6.21.8 The Root User Does Not Have Available Access Keys

Rule Details

Table 3-116 Rule details

Parameter	Description
Rule Name	iam-root-access-key-check
Identifier	iam-root-access-key-check
Description	If the root user access key is available, the account is noncompliant.
Tag	iam
Trigger Type	Periodic
Filter Type	Account
Configure Rule Parameters	None

Applicable Scenario

To enhance account security, you are advised to only use the password to log in to the console. Do not create access keys for your root user.

Solution

You can delete or disable access keys for the root user. For more details, see **Managing Access Keys for an IAM User**.

Rule Logic

- If a root user does not have an enabled access key, the account is compliant.
- If a root user has an enabled access key, the account is noncompliant.

3.6.21.9 Access Mode Check

Rule Details

Table 3-117 Rule details

Parameter	Description
Rule Name	iam-user-access-mode
Identifier	iam-user-access-mode

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

Applicable Scenario

This rule ensures that an IAM user cannot access cloud services through both the console and APIs. There are two methods for accessing a cloud service:

- Programmatic access: Users access cloud services by using development tools, such as APIs, CLI, and SDKs with access keys.
- Management console access: Users access cloud services through the management console with passwords.

NOTICE

It is advised to not use passwords for programmatic access.

Solution

You can allow IAM users to access cloud services either using programmatic methods or through the console. Ensure that an IAM user does not have both a password and an access key.

Rule Logic

- If an IAM user is disabled, this user is compliant.
- If an IAM user is enabled, but is not allowed to access cloud services by using both the programmatic methods and the management console, this user is compliant.
- If an enabled IAM user does not have both an access key and a password, this IAM user is compliant.
- If an IAM user does not meet any of the above conditions, this user is noncompliant.

3.6.21.10 Access Key Check

Rule Details

Table 3-118 Rule details

Parameter	Description
Rule Name	iam-user-console-and-api-access-at-creation
Identifier	iam-user-console-and-api-access-at-creation
Description	If an IAM user can access the Huawei Cloud console and has AK/SK that was created when the IAM user was created, this user is noncompliant.
Tag	iam
Trigger Type	Configuration change
Filter Type	iam.users
Configure Rule Parameters	None

Applicable Scenario

To improve resource security, you are advised not to set access keys for IAM users who are allowed to access the management console.

Solution

You can delete access keys for noncompliant IAM users.

Rule Logic

- If an IAM user is disabled, this user is compliant.
- If an IAM user is not allowed to access the management console, this user is compliant.
- If an IAM user does not have an access key, this user is compliant.
- If an IAM user does not meet any of the above three conditions, this user is noncompliant.

3.6.21.11 IAM Users Are in Specified User Groups

Rule Details

Table 3-119 Rule details

Parameter	Description
Rule Name	iam-user-group-membership-check
Identifier	iam-user-group-membership-check
Description	If an IAM user is not in any of the specified IAM user groups, this user is noncompliant.
Tag	iam
Trigger Type	Configuration change
Filter Type	iam.users
Configure Rule Parameters	**groupIds**: user group IDs. If no user group IDs are specified, the evaluation covers all user groups. The value must be an array with up to 10 elements.

Applicable Scenario

The administrator can assign permissions to user groups and add users to these groups. Adding or removing users from a user group allows you to efficiently manage user permissions.

Solution

You can add noncompliant IAM users to some user groups. You can also disable or delete these users if you do not need them any longer.

Rule Logic

- If an IAM user is disabled, this user is compliant.
- If an enabled IAM user has been added to at least one user group, and no user groups are specified, this IAM user is compliant.
- If an enabled IAM user has not been added to any user groups, and no user groups are specified, this IAM user is noncompliant.
- If an enabled IAM user has been added to any of the specified user groups, this IAM user is compliant.
- If an enabled IAM user has not been added to any of the specified user groups, this IAM user is noncompliant.

3.6.21.12 Last Login Check

Rule Details

Table 3-120 Rule details

Parameter	Description
Rule Name	iam-user-last-login-check
Identifier	iam-user-last-login-check
Description	If an IAM user has not logged in to the system within the specified period of time, this user is non-compliant.
Tag	iam
Trigger Type	Periodic
Filter Type	iam.users
Configure Rule Parameters	**allowedInactivePeriod**: the specified period of time. The value must be an integer. The default value is 90.

Applicable Scenario

This rule helps you identify idle IAM users to improve account security

Solution

You can use noncompliant IAM users to log in to Huawei Cloud console or delete these users as needed. For more details, see **Logging In as an IAM User** and **Deleting an IAM User**.

Rule Logic

- If an IAM user is disabled, this user is compliant.
- If an IAM user is not allowed to access the management console, this user is compliant.
- If an enabled IAM user who is allowed to access the management console has logged in to the system within the specified period of time, this user is compliant.
- If an enabled IAM user who is allowed to access the management console has not logged in to the system within the specified period of time, this user is noncompliant.

3.6.21.13 Multi-Factor Authentication Check

Rule Details

Table 3-121 Rule details

Parameter	Description
Rule Name	iam-user-mfa-enabled
Identifier	iam-user-mfa-enabled
Description	If multi-factor authentication 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

Applicable Scenario

Multi-factor authentication (MFA) adds an additional layer of security protection on top of the identity credentials for an account. It is recommended that you enable MFA authentication for your account and privileged users created using your account. After MFA authentication is enabled, you need to enter verification codes after your username and password are authenticated. MFA devices, together with your username and password, ensure the security of your account and resources.

Solution

To enable the MFA, you need to install an MFA application (such as the Google Authenticator or Microsoft Authenticator) on your mobile device. For details, see **Binding a Virtual MFA Device**.

Rule Logic

- If an IAM user is disabled, this user is compliant.
- If an IAM user is enabled and has MFA enabled, this user is compliant.
- If an IAM user is enabled, but does not have MFA enabled, this user is noncompliant.

3.6.21.14 A User Does Not have Multiple Active Access Keys

Rule Details

Table 3-122 Rule details

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

Applicable Scenario

Access keys are identity credentials that IAM users can use to call APIs. To improve resource security, each IAM user is advised to be assigned only one active access key.

Solution

You can delete or disable the additional access keys for noncompliant IAM users. For more details, see **Managing Access Keys for an IAM User**.

Rule Logic

- If an IAM user is in the disabled state, this user is compliant.
- If an IAM user that is in the enabled state has only one active access key, this IAM user is compliant.
- If an IAM user that is in the enabled state has multiple active access keys, this IAM user is noncompliant.

3.6.21.15 MFA Has Been Enabled for Console Login

Rule Details

Table 3-123 Rule details

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

Applicable Scenario

Multi-factor authentication (MFA) adds an additional layer of security protection on top of the identity credentials for an account. It is recommended that you enable MFA authentication for your account and privileged users created using your account. After MFA authentication is enabled, you need to enter verification codes after your username and password are authenticated. MFA devices, together with your username and password, ensure the security of your account and resources.

Solution

Before binding a virtual MFA device, ensure that you have installed an MFA application (such as Google Authenticator or Microsoft Authenticator) on your mobile device. For details, see **Binding a Virtual MFA Device**.

Rule Logic

- If an IAM user is in the disabled state, this user is compliant.
- If an IAM user is not allowed to access the management console, this user is compliant.
- If an enabled IAM user who is allowed to access the management console has MFA enabled, this user is compliant.
- If an enabled IAM user who is allowed to access the management console has MFA disabled, this user is noncompliant.

3.6.21.16 The Root User Has MFA Enabled

Rule Details

Table 3-124 Rule details

Parameter	Description
Rule Name	root-account-mfa-enabled
Identifier	root-account-mfa-enabled
Description	If the root user does not have MFA enabled, this root user is noncompliant.
Tag	iam
Trigger Type	Periodic
Filter Type	Account
Configure Rule Parameters	None

Applicable Scenario

Multi-factor authentication (MFA) adds an additional layer of security protection on top of the identity credentials for an account. It is recommended that you enable MFA authentication for your account and privileged users created using your account. After MFA authentication is enabled, you need to enter verification codes after your username and password are authenticated. MFA devices, together with your username and password, ensure the security of your account and resources.

Solution

Before binding a virtual MFA device, ensure that you have installed an MFA application (such as Google Authenticator or Microsoft Authenticator) on your mobile device. For details, see **Binding a Virtual MFA Device**.

Rule Logic

- If the root user already has MFA enabled, this root user is compliant.
- If the root user does not have MFA enabled, this root user is noncompliant.

3.6.21.17 All IAM Policies Are in Use

Rule Details

Table 3-125 Rule details

Parameter	Description
Rule Name	iam-policy-in-use
Identifier	iam-policy-in-use
Description	If an IAM policy has not been attached to any IAM users, user groups, or agencies, this policy is noncompliant.
Tag	iam
Trigger Type	Configuration change
Filter Type	iam.policies
Rule Parameter	None

Applicable Scenario

This rule allows you to detect IAM policies that haven't been attached to any IAM users, user groups, or agencies, so that you can avoid unintended authorization with these policies.

Solution

If you need the detected unused policies, attach these policies to IAM users, user groups or agencies. If you do not, delete them.

Rule Logic

- If an IAM policy has been attached to an IAM user, user group, or agency, this policy is compliant.
- If an IAM policy has not been attached to any IAM users, user groups, or agencies, this policy is noncompliant.

3.6.21.18 All IAM Roles Are in Use

Rule Details

Table 3-126 Rule details

Parameter	Description
Rule Name	iam-role-in-use
Identifier	iam-role-in-use

Parameter	Description
Description	If an IAM role has not been attached to any IAM users, user groups, or agencies, this role is noncompliant.
Tag	iam
Trigger Type	Configuration change
Filter Type	iam.roles
Rule Parameter	None

Applicable Scenario

This rule allows you to detect IAM roles that haven't been attached to any IAM users, user groups, or agencies, so that you can avoid unintended authorization with these policies.

Solution

If you need the detected unused roles, attach these roles to IAM users, user groups or agencies. If you do not, delete them.

Rule Logic

- If an IAM role has been attached to an IAM user, user group, or agency, this role is compliant.
- If an IAM role has not been attached to any IAM users, user groups, or agencies, this role is noncompliant.

3.6.21.19 Login Protection Check

Rule Details

Table 3-127 Rule details

Parameter	Description
Rule Name	iam-user-login-protection-enabled
Identifier	iam-user-login-protection-enabled
Description	If login protection is not enabled for an IAM user, this user is noncompliant.
Tag	iam
Trigger Type	Configuration change
Filter Type	iam.users
Rule Parameter	None

Applicable Scenario

To improve account security and prevent phishing attacks and password leakage, the root or administrative user can enable login protection for IAM users. If login protection is enabled, a verification code will be required in addition to the username and password during login. You can use a mobile number, email address, or virtual MFA for login authentication.

Solution

You can enable login protection for the noncompliant IAM users. For more details, see **Login Protection**.

Rule Logic

- If an IAM user is in the disabled state, this user is compliant.
- If an IAM user that is enabled has MFA enabled, this user is compliant.
- If an IAM user that is enabled does not have MFA enabled, this user is noncompliant.

3.6.21.20 IAM Agencies Contain Specified Policies

Rule Details

Table 3-128 Rule details

Parameter	Description
Rule Name	iam-agencies-managed-policy-check
Identifier	iam-agencies-managed-policy-check
Description	If an IAM agency does not contain the specified policies and roles, this agency is noncompliant.
Tag	iam
Trigger Type	Configuration change
Filter Type	iam.agencies
Configure Rule Parameters	● **roleIdList**: role IDs. System-defined roles are not supported. ● **policyIdList**: policy IDs. System-defined policies are not supported.

Applicable Scenario

When you assign permissions to control resource access, the least privilege principles should be applied. This rule allows you to detect agencies that do not contain the required policies or rules, so that you can avoid granting excessive permissions with these agencies.

Solution

You can attach the required roles or policies to the noncompliant agencies. For more details, see **Authorizing IAM Users to Manage Resources of an Account**.

Rule Logic

- If an IAM agency does not contain all the specified policies and roles, this agency is noncompliant.
- If an IAM agency contains all the specified policies and roles, this agency is compliant.

3.6.21.21 The Admin User Group Only Contains the Root User

Rule Details

Table 3-129 Rule details

Parameter	Description
Rule Name	iam-user-check-non-admin-group
Identifier	iam-user-check-non-admin-group
Description	If a non-root user was added to the **admin** user group, this user is noncompliant.
Tag	iam
Trigger Type	Configuration change
Filter Type	iam.users
Configure Rule Parameters	None

Applicable Scenario

The **admin** user group is a default user group and has full permissions for all cloud resources in an account. It is insecure if non-root users are added to the **admin** user group or share the same enterprise administrator account. You can add IAM users to related user groups and attach only the necessary permissions to the user groups, so that related personnel or applications can access only the required cloud resources to complete their tasks.

Solution

You can delete non-root users from the **admin** user group. For more details, see **Adding Users to or Removing Users from a User Group**.

Rule Logic

- If an IAM user is the root user, this user is compliant.
- If an IAM user is disabled, this user is compliant.
- If a non-root IAM user in the enabled state was added to the **admin** user group, this user is noncompliant.
- If a non-root IAM user in the enabled state is not in the **admin** user group, this user is compliant.

3.6.21.22 IAM Users Do Not Have Directly Assigned Policies or Permissions

Rule Details

Table 3-130 Rule details

Parameter	Description
Rule Name	iam-user-no-policies-check
Identifier	iam-user-no-policies-check
Description	If an IAM user has any policies or permissions directly assigned , the IAM user is noncompliant.
Tag	iam
Trigger Type	Configuration change
Filter Type	iam.users
Configure Rule Parameters	None

Applicable Scenario

To assign IAM users permissions, you are advised to add users to a user group and assign permissions to the user group. This makes it easier to manage permissions and helps prevent excessive authorization. For more details, see **Assigning Permissions to an IAM User**.

Solution

You can remove the policies or permissions from noncompliant IAM users and then, create a user group, add the users to the user group, and add the policies or permissions to the user group.

Rule Logic

- If an IAM user has any directly assigned policies or permissions, the IAM user is noncompliant.
- If an IAM user does not have directly assigned policies or permissions, the IAM user is compliant.

3.6.22 Document Database Service

3.6.22.1 SSL Has Been Enabled

Rule Details

Table 3-131 Rule details

Parameter	Description
Rule Name	dds-instance-enable-ssl
Identifier	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

3.6.22.2 DDS Instance Type Check

Rule Details

Table 3-132 Rule details

Parameter	Description
Rule Name	dds-instance-hamode
Identifier	dds-instance-hamode
Description	If a DDS instance is not of 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.

3.6.22.3 DDS Instances Do Not Have EPIs Attached

Rule Details

Table 3-133 Rule details

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

3.6.22.4 DDS Instances Do Not Have Unallowed Ports Enabled

Rule Details

Table 3-134 Rule details

Parameter	Description
Rule Name	dds-instance-port-check
Identifier	dds-instance-port-check
Description	If a DDS instance has unallowed ports enabled, this instance is noncompliant.
Tag	dds
Trigger Type	Configuration change
Filter Type	dds.instances
Configure Rule Parameters	**disabledPortsPatterns**: Unallowed ports. The value must be an array.

3.6.22.5 DDS Instance Version Check

Rule Details

Table 3-135 Rule details

Parameter	Description
Rule Name	dds-instance-engine-version-check
Identifier	dds-instance-engine-version-check
Description	If the version of a DDS instance is lower than the specified version, this instance is noncompliant.
Tag	dds
Trigger Type	Configuration change
Filter Type	dds.instances
Configure Rule Parameters	**specifiedVersion**: Version ID, such as 4.2.

3.6.22.6 DDS Instances Are in the Specified VPC

Rule Details

Table 3-136 Rule details

Parameter	Description
Rule Name	dds-instance-in-vpc
Identifier	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**: The VPC ID. The value must be a string.

3.6.23 Simple Message Notification

3.6.23.1 Log Reporting to LTS Has Been Enabled

Rule Details

Table 3-137 Rule details

Parameter	Description
Name	smn-lts-enable
Identifier	smn-lts-enable
Description	If **Report Logs to LTS** has not been enabled for a topic, this topic is noncompliant.
Tag	smn
Trigger Type	Configuration change
Filter Type	smn.topic
Configure Rule Parameters	None

3.6.24 Virtual Private Cloud

3.6.24.1 Idle ACL Check

Rule Details

Table 3-138 Rule details

Parameter	Description
Rule Name	vpc-acl-unused-check
Identifier	vpc-acl-unused-check
Description	If a network ACL is not attached to any subnets, this ACL is noncompliant.
Tag	vpc
Trigger Type	Configuration change
Filter Type	vpc.firewallGroups
Configure Rule Parameters	None

3.6.24.2 Default Security Group Check

Rule Details

Table 3-139 Rule details

Parameter	Description
Rule Name	vpc-default-sg-closed
Identifier	vpc-default-sg-closed
Description	If a default security group allows any inbound or outbound traffic, it is considered noncompliant.
Tag	vpc
Trigger Type	Configuration change
Filter Type	vpc.securityGroups
Configure Rule Parameters	None

Rule Logic

- All non-default security groups are compliant.
- If a default security group denies all inbound or outbound traffic, it is considered compliant.
- If a default security group allows any inbound or outbound traffic, it is considered noncompliant.

NOTE

A security group typically contains multiple rules, and these rules follow a certain order to take effect. For details, see **How Traffic Matches Security Group Rules**. This Config rule bypasses all **Deny** rules. If any **Allow** rule is detected, the security group which the rule belongs to will be considered noncompliant.

3.6.24.3 VPCs Have Enabled Flow Logs

Rule Details

Table 3-140 Rule details

Parameter	Description
Rule Name	vpc-flow-logs-enabled
Identifier	vpc-flow-logs-enabled
Description	If the flow log has not been enabled for a VPC, this VPC is noncompliant.

Parameter	Description
Tag	vpc
Trigger Type	Configuration change
Filter Type	vpc.vpcs
Configure Rule Parameters	None

3.6.24.4 Port Check

Rule Details

Table 3-141 Rule details

Parameter	Description
Rule Name	vpc-sg-ports-check
Identifier	vpc-sg-ports-check
Description	If a security group allows all inbound traffic (**Source**: 0.0.0.0/0) and opens all TCP/UDP ports, this security group is noncompliant.
Tag	vpc
Trigger Type	Configuration change
Filter Type	vpc.securityGroups
Configure Rule Parameters	None

Rule Logic

- If a security group does not have the source address set to **0.0.0.0/0** or **::/0**, or does not open all TCP/UDP ports, this security group is compliant.
- If a security group has the source address set to **0.0.0.0/0** or **::/0** and opens all TCP/UDP ports, this security group is noncompliant.

NOTE

A security group typically contains multiple rules, and these rules follow a certain order to take effect. For details, see **How Traffic Matches Security Group Rules**. This Config rule bypasses all **Deny** rules. If any **Allow** rule is detected, the security group which the rule belongs to will be considered noncompliant.

3.6.24.5 Inbound Traffic Can Only Access Specified Ports

Rule Details

Table 3-142 Rule details

Parameter	Description
Rule Name	vpc-sg-restricted-common-ports
Identifier	vpc-sg-restricted-common-ports
Description	If a security group allows all IPv4 and IPv6 traffic (with the source address set to **0.0.0.0/0** or **::/0**) to the specified ports, 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

Rule Logic

- If a security group does not allow all IPv4 and IPv6 traffic (with the source address set to **0.0.0.0/0** or **::/0**) to the specified ports, this security group is compliant.
- If a security group allows all IPv4 and IPv6 traffic (with the source address set to **0.0.0.0/0** or **::/0**) to the specified ports, this security group is noncompliant.

NOTE

A security group typically contains multiple rules, and these rules follow a certain order to take effect. For details, see **How Traffic Matches Security Group Rules**. This Config rule bypasses all **Deny** rules. If any **Allow** rule is detected, the security group which the rule belongs to will be considered noncompliant.

3.6.24.6 SSH Check

Rule Details

Table 3-143 Rule details

Parameter	Description
Rule Name	vpc-sg-restricted-ssh
Identifier	vpc-sg-restricted-ssh
Description	If a security group allows all inbound traffic (with the source address set to **0.0.0.0/0** or **::/0**) and opens the TCP 22 port, this security group is noncompliant.
Tag	vpc
Trigger Type	Configuration change
Filter Type	vpc.securityGroups
Configure Rule Parameters	None

Rule Logic

- If a security group does not allow all IPv4 and IPv6 traffic (with the source address set to **0.0.0.0/0** or **::/0**) to the TCP port 22, this security group is compliant.
- If a security group allows all IPv4 and IPv6 traffic (with the source address set to **0.0.0.0/0** or **::/0**) to the TCP port 22, this security group is noncompliant.

NOTE

A security group typically contains multiple rules, and these rules follow a certain order to take effect. For details, see **How Traffic Matches Security Group Rules**. This Config rule bypasses all **Deny** rules. If any **Allow** rule is detected, the security group which the rule belongs to will be considered noncompliant.

3.6.24.7 Access Control Check for Non-whitelisted Ports

Rule Details

Table 3-144 Rule details

Parameter	Description
Rule Name	vpc-sg-by-white-list-ports-check
Identifier	vpc-sg-by-white-list-ports-check

Parameter	Description
Description	If a security group allows traffic to a non-whitelisted port, this security group is noncompliant.
Tag	vpc
Trigger Type	Configuration change
Filter Type	vpc.securityGroups
Rule Parameter	**whiteListPorts**: whitelisted ports

Rule Logic

- If a security group denies both inbound and outbound traffic to all non-whitelisted ports, this security group is compliant.
- If a security group allows traffic to any non-whitelisted port, this security group is noncompliant.

NOTE

A security group typically contains multiple rules, and these rules follow a certain order to take effect. For details, see **How Traffic Matches Security Group Rules**. This Config rule bypasses all **Deny** rules. If any **Allow** rule is detected, the security group which the rule belongs to will be considered noncompliant.

3.6.24.8 A Security Group is Attached to Elastic Network Interfaces

Rule Details

Table 3-145 Rule details

Parameter	Description
Rule Name	vpc-sg-attached-ports
Identifier	vpc-sg-attached-ports
Description	This rule checks if a security group is associated with any elastic network interface. If a security group is not attached to any elastic network interface, this security group is noncompliant.
Tag	vpc
Trigger Type	Configuration change
Filter Type	vpc.securityGroups
Rule Parameter	None

3.6.25 Virtual Private Network

3.6.25.1 Connection State Check

Rule Details

Table 3-146 Rule details

Parameter	Description
Rule Name	vpn-connections-active
Identifier	vpn-connections-active
Description	If a VPN is not normally connected, this rule is noncompliant.
Tag	vpnaas
Trigger Type	Configuration change
Filter Type	vpnaas.vpnConnections, vpnaas.ipsec-site-connections
Configure Rule Parameters	None

3.6.26 Cloud Eye

3.6.26.1 Alarm Rules Are Enabled

Rule Details

Table 3-147 Rule details

Parameter	Description
Rule Name	alarm-action-enabled-check
Identifier	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

3.6.26.2 Alarm Rules Have Been Configured for Key Disablement and Deletion

Rule Details

Table 3-148 Rule details

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

Rule Logic

- If there are no alarm rules configured for disabling KMS or deleting keys, this rule is noncompliant.
- If there are alarm rules configured for disabling KMS or deleting keys, this rule is compliant.
- For details about the system events supported by Cloud Eye, see **Events Supported by Event Monitoring**.

3.6.26.3 There Are Alarm Rules Configured for OBS Bucket Policy Changes

Rule Details

Table 3-149 Rule details

Parameter	Description
Rule Name	alarm-obs-bucket-policy-change
Identifier	alarm-obs-bucket-policy-change
Description	If there are no alarm rules configured for bucket policy changes, this rule is noncompliant.
Tag	ces, obs
Trigger Type	Periodic

Parameter	Description
Filter Type	Account
Configure Rule Parameters	None

Rule Logic

- If there are no alarm rules configured for modifying or deleting OBS bucket policies, this rule is noncompliant.
- If there are alarm rules configured for modifying or deleting OBS bucket policies, this rule is compliant.
- For details about the system events supported by Cloud Eye, see **Events Supported by Event Monitoring**.

3.6.26.4 Specified Resources Have Certain Metric Attached

Rule Details

Table 3-150 Rule details

Parameter	Description
Rule Name	alarm-resource-check
Identifier	alarm-resource-check
Description	If a resource does not have the specified metric attached, this resource is noncompliant.
Tag	ces
Trigger Type	Periodic
Filter Type	Account
Configure Rule Parameters	● **provider**: a cloud service name. The value must be a string. ● **resourceType**: a resource type. The value must be a string. ● **metricName**: a metric name. The value must be a string.

3.6.26.5 Alarm Rule Configurations Check

Rule Details

Table 3-151 Rule details

Parameter	Description
Rule Name	alarm-settings-check
Identifier	alarm-settings-check
Description	If the alarm rule configurations of the specified metric do not match the specified conditions, this rule is noncompliant.
Tag	ces
Trigger Type	Configuration change
Filter Type	ces.alarms
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.

3.6.26.6 Alarms Have Been Created for VPC Changes

Rule Details

Table 3-152 Rule details

Parameter	Description
Rule Name	alarm-vpc-change
Identifier	alarm-vpc-change

Parameter	Description
Description	If there are no alarm rules configured for VPC changes, the current account is noncompliant.
Tag	ces, vpc
Trigger Type	Periodic
Filter Type	Account
Configure Rule Parameters	None

Rule Logic

- If no alarm rules are configured for VPC changes, this rule is noncompliant.
- If there are alarms configured for VPC changes, this rule is compliant.
- For details about the system events supported by Cloud Eye, see **Events Supported by Event Monitoring**.

3.6.27 Cloud Container Engine

3.6.27.1 CCE Clusters Are Supported for Maintenance

Rule Details

Table 3-153 Rule details

Parameter	Description
Rule Name	cce-cluster-end-of-maintenance-version
Identifier	cce-cluster-end-of-maintenance-version
Description	If the version of a CCE cluster is no longer supported for maintenance, this cluster is noncompliant.
Tag	cce
Trigger Type	Configuration change
Filter Type	cce.clusters
Configure Rule Parameters	None

3.6.27.2 Oldest Supported Version Check

Rule Details

Table 3-154 Rule details

Parameter	Description
Rule Name	cce-cluster-oldest-supported-version
Identifier	cce-cluster-oldest-supported-version
Description	If a CCE cluster is running the oldest supported version, this cluster is noncompliant.
Tag	cce
Trigger Type	Configuration change
Filter Type	cce.clusters
Configure Rule Parameters	None

3.6.27.3 CCE Clusters Do Not Have EIPs Attached

Rule Details

Table 3-155 Rule details

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

3.6.27.4 Flavor Check

Rule Details

Table 3-156 Rule details

Parameter	Description
Rule Name	allowed-cce-flavors
Identifier	allowed-cce-flavors
Description	If the flavor of a CCE cluster does not match any of the specified flavors, this cluster is noncompliant.
Tag	cce
Trigger Type	Configuration change
Filter Type	cce.clusters
Rule Parameter	listOfAllowedFlavors: CCE cluster flavors. For details about flavor enumerated values (such as cce.s1.small), see **Reading a Specified Cluster**.

Rule Logic

- If the flavor of a CCE cluster matches one of the specified flavors, this cluster is compliant.
- If the flavor of a CCE cluster does not match any of the specified flavors, this cluster is noncompliant.

3.6.27.5 CCE Clusters Are in Specified VPCs

Rule Details

Table 3-157 Rule details

Parameter	Description
Rule Name	cce-cluster-in-vpc
Identifier	cce-cluster-in-vpc
Description	If a CCE cluster is not in any of the specified VPCs, this cluster is noncompliant.
Tag	cce
Trigger Type	Configuration change
Filter Type	cce.clusters

Parameter	Description
Configure Rule Parameters	**VpcIdList**: VPC IDs. The value must be an array.

Applicable Scenario

A Virtual Private Cloud (VPC) is a private network on the cloud. VPCs allow you to logically isolate you CCE clusters. You can design VPC networks based on your security requirements.

Solution

You can redeploy noncompliant CCE clusters to required VPCs. For details, see **Modifying Cluster Configurations**.

Rule Logic

- If a CCE cluster is not in any of the specified VPCs, this cluster is noncompliant.
- If a CCE cluster is in one of the specified VPCs, this cluster is noncompliant.

3.6.28 Cloud Trace Service

3.6.28.1 CTS Trackers Have Traces Encrypted

Rule Details

Table 3-158 Rule details

Parameter	Description
Rule Name	cts-kms-encrypted-check
Identifier	cts-kms-encrypted-check
Description	If a CTS tracker does not have trace encryption enabled, this tracker is noncompliant.
Tag	cts
Trigger Type	Configuration change
Filter Type	cts.trackers
Configure Rule Parameters	None

Applicable Scenario

This rule ensures that the traces dumped by a CTS tracker to an OBS bucket are encrypted.

Solution

You are advised to enable trace encryption for the noncompliant trackers.

Rule Logic

- If a CTS tracker (disabled or enabled) does not have trace encryption enabled, this tracker is noncompliant.
- If a CTS tracker (disabled or enabled) has trace encryption enabled, this tracker is compliant.

Constraints

If an organization CTS tracker is involved, and this rule is triggered with a member account from this organization, there may be a lag of up to 24 hours in updating the evaluating results due to the delay in collecting tracker resources deployed by the organization administrator.

3.6.28.2 CTS Trackers Have Trace Transfer to LTS Enabled

Rule Details

Table 3-159 Rule details

Parameter	Description
Rule Name	cts-lts-enable
Identifier	cts-lts-enable
Description	If a CTS tracker does not have trace transfer to LTS enabled, this tracker is noncompliant.
Tag	cts
Trigger Type	Configuration change
Filter Type	cts.trackers
Configure Rule Parameters	None

Applicable Scenario

CTS records tenant operations on cloud resources, such as creating, modifying, and deleting cloud resources, and stores operations as traces on CTS console for seven days. To store traces for more than seven days, configure trace transfer to LTS.

Solution

You can enable trace transfer to LTS for the noncompliant CTS trackers. For details, see **Transferring CTS Traces to LTS and Viewing Them**.

Rule Logic

- If a CTS tracker (disabled or enabled) has trace transfer to LTS enabled, this tracker is compliant.
- If a CTS tracker (disabled or enabled) does not have trace transfer to LTS enabled, this tracker is noncompliant.

Constraints

If an organization CTS tracker is involved, and this rule is triggered with a member account from this organization, there may be a lag of up to 24 hours in updating the evaluating results due to the delay in collecting tracker resources deployed by the organization administrator.

3.6.28.3 CTS Trackers Have Been Created for the Specified OBS Bucket

Rule Details

Table 3-160 Rule details

Parameter	Description
Rule Name	cts-obs-bucket-track
Identifier	cts-obs-bucket-track
Description	If there are no CTS trackers created for the specified OBS bucket, the current account is noncompliant.
Tag	cts
Trigger Type	Periodic
Filter Type	Account
Configure Rule Parameters	**trackBucket**: the name of a specified OBS bucket. The value must be a string.

Applicable Scenario

CTS allows you to create data trackers to record operations (such as upload and download) on data that is stored in OBS buckets

Solution

You can configure an OBS bucket, trace transfer to LTS, and key trace notifications for noncompliant trackers on CTS console. For more details, see **Configuring a Tracker**.

Rule Logic

- If there is a CTS tracker that only records read or write operations for the specified OBS bucket, the current account is compliant.
- If there is an enabled CTS tracker created for the specified OBS bucket, the current account is compliant.
- If none of the enabled CTS trackers record data operations for the specified OBS, the current account is noncompliant.
- If all CTS trackers are disabled, the current account is noncompliant.

3.6.28.4 Trace File Verification Is Enabled

Rule Details

Table 3-161 Rule details

Parameter	Description
Rule Name	cts-support-validate-check
Identifier	cts-support-validate-check
Description	If a CTS tracker does not have trace file verification enabled, this tacker is noncompliant.
Tag	cts
Trigger Type	Configuration change
Filter Type	cts.trackers
Configure Rule Parameters	None

Applicable Scenario

Operation records can provide reliable, effective evidence for security audit and troubleshooting. It is important to protect these records from being deleted or tampered with. This rule allows you to verify the integrity of a trace file.

Solution

You can enable trace file verification for noncompliant CTS trackers. For details, see **Enabling Verification of Trace File Integrity**.

Rule Logic

- If a CTS tracker (disabled or enabled) has trace file verification enabled, this tracker is compliant.
- If a CTS tracker (disabled or enabled) does not have trace file verification enabled, this tracker is noncompliant.

Constraints

If an organization CTS tracker is involved, and this rule is triggered with a member account from this organization, there may be a lag of up to 24 hours in updating the evaluating results due to the delay in collecting tracker resources deployed by the organization administrator.

3.6.28.5 At Least One Tracker Is Enabled

Rule Details

Table 3-162 Rule details

Parameter	Description
Rule Name	cts-tracker-exists
Identifier	cts-tracker-exists
Description	If there are no trackers or all trackers are disabled in an account, this account is noncompliant.
Tag	cts
Trigger Type	Periodic
Filter Type	Account
Configure Rule Parameters	None

Applicable Scenario

CTS allows you to create data trackers to record operations (such as upload and download) on data that is stored in OBS buckets

Solution

When you log in to CTS console for the first time to enable CTS, a management tracker named **system** will be automatically created. You can also create and enable data trackers. For details, see **Creating a Tracker**.

Rule Logic

- If there are no trackers in an account, this account is noncompliant.
- If all CTS trackers are disabled in an account, this account is noncompliant.
- If there is at least one enabled CTS tracker in an account, this account is compliant.

Constraints

If an organization CTS tracker is involved, and this rule is triggered with a member account from this organization, there may be a lag of up to 24 hours in updating the evaluating results due to the delay in collecting tracker resources deployed by the organization administrator.

3.6.28.6 There Are CTS Trackers In the Specified Regions

Rule Details

Table 3-163 Rule details

Parameter	Description
Rule Name	multi-region-cts-tracker-exists
Identifier	multi-region-cts-tracker-exists
Description	If there are no CTS trackers in any of the specified regions, this rule is noncompliant.
Tag	cts
Trigger Type	Periodic
Filter Type	Account
Configure Rule Parameters	**regionList**: indicates the specified regions. The value must be an array.

Applicable Scenario

CTS allows you to record and query operations on cloud resources. When you enable CTS for the first time, a management tracker, **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.

Solution

When you log in to CTS console for the first time to enable CTS, a management tracker named **system** will be automatically created. You can also create and enable data trackers. For details, see **Creating a Tracker**.

Rule Logic

- If there are enabled CTS trackers in the specified regions, this rule is compliant.
- If there are no enabled CTS trackers in any of the specified regions, this rule is noncompliant.

Constraints

If an organization CTS tracker is involved, and this rule is triggered with a member account from this organization, there may be a lag of up to 24 hours in updating the evaluating results due to the delay in collecting tracker resources deployed by the organization administrator.

3.6.28.7 CTS Trackers Comply with Security Best Practices

Rule Details

Table 3-164 Rule details

Parameter	Description
Rule Name	cts-tracker-enabled-security
Identifier	cts-tracker-enabled-security
Description	If there is no tracker that complies with security best practices, this rule is noncompliant.
Tag	cts
Trigger Type	Periodic
Filter Type	Account
Rule Parameter	Regions: Regions where CTS trackers reside. If no regions are specified, this rule will be applied to all regions.

Applicable Scenario

CTS records operations on cloud resources in your account. You can use the traces to perform security analysis, track resource changes, audit compliance, and locate faults. Security best practices must be met to avoid trace files loss, tampering, or disclosure.

- Trace file verification: When this function is enabled, integrity verification will be performed to check whether trace files in OBS buckets have been tampered with.
- Trace file encryption: After enabling trace transfer, you can use Data Encryption Workshop (DEW) to encrypt trace files stored in OBS buckets.
- Trace transfer to LTS: When this function is enabled, traces are transferred to a specified OBS bucket.

Solution

You can enable trace file verification, encryption, and transfer to LTS on CTS console. For details, see **Configuring a Tracker**.

Rule Logic

- If **Verify Trace File**, **Encrypt Trace File**, and **Transfer to LTS** are all enabled for a CTS tracker, this tracker is considered to comply with security best practices.
- When no regions are specified, the current account is compliant if there is any tracker that complies with the security best practices.
- When no regions are specified, the current account is noncompliant if there are no trackers that comply with the security best practices.

- When one or more regions are specified, the current account is compliant if there is any tracker that complies with the security best practices in any of the specified regions.
- When one or more regions are specified, the current account is noncompliant if there are no trackers that comply with the security best practices in any of the specified regions.

Constraints

If an organization CTS tracker is involved, and this rule is triggered with a member account from this organization, there may be a lag of up to 24 hours in updating the evaluating results due to the delay in collecting tracker resources deployed by the organization administrator.

3.6.29 Relational Database Service

3.6.29.1 Error Log Collection Is Enabled for RDS Instances

Rule Details

Table 3-165 Rule details

Parameter	Description
Rule Name	rds-instance-enable-backup
Identifier	rds-instance-enable-backup
Description	If 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

3.6.29.2 Error Log Collection Is Enabled for RDS Instances

Rule Details

Table 3-166 Rule details

Parameter	Description
Rule Name	rds-instance-enable-errorLog

Parameter	Description
Identifier	rds-instance-enable-errorLog
Description	If error log collection 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

3.6.29.3 RDS Instances Support Slow Query Logs

Rule Details

Table 3-167 Rule details

Parameter	Description
Rule Name	rds-instance-enable-slowLog
Identifier	rds-instance-enable-slowLog
Description	If an RDS instance does not support slow query logs, this instance is noncompliant.
Tag	rds
Trigger Type	Configuration change
Filter Type	rds.instances
Configure Rule Parameters	None

3.6.29.4 Single-AZ Cluster Check

Rule Details

Table 3-168 Rule details

Parameter	Description
Name	rds-instance-multi-az-support
Identifier	rds-instance-multi-az-support

Parameter	Description
Description	If an RDS instance does not support multi-AZ deployment, this RDS instance is noncompliant.
Tag	rds
Trigger Type	Configuration change
Filter Type	rds.instances
Configure Rule Parameters	None

3.6.29.5 RDS Instances Do Not Have EIPs Attached

Rule Details

Table 3-169 Rule details

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

3.6.29.6 RDS Instances Use KMS Encryption

Rule Details

Table 3-170 Rule details

Parameter	Description
Rule Name	rds-instances-enable-kms
Identifier	rds-instances-enable-kms

Parameter	Description
Description	If KMS 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

3.6.29.7 RDS Instances Are in the Specified VPC

Rule Details

Table 3-171 Rule details

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

Applicable Scenario

A VPC is a private network on the cloud. You can create VPCs to logically isolate your RDS instances. For more details, see **What Is Virtual Private Cloud?**

Solution

You cannot change VPCs or subnets of RDS instances. You can use an RDS backup to create a new RDS instance and deploy the instance to the desired VPC and subnet. For details, see **Restoring a DB Instance from Backups**.

Rule Logic

- If an RDS instance is not in the specified VPC, this instance is noncompliant.
- If an RDS instance is in the specified VPC, this instance is compliant.

3.6.29.8 Both Error Logs and Slow Query Logs Are Collected for RDS Instances

Rule Details

Table 3-172 Rule details

Parameter	Description
Rule Name	rds-instance-logging-enabled
Identifier	rds-instance-logging-enabled
Description	If neither error logs nor slow query logs are collected for an RDS instance, this instance is noncompliant.
Tag	rds
Trigger Type	Configuration change
Filter Type	rds.instances
Configure Rule Parameters	None

3.6.29.9 Flavor Check

Rule Details

Table 3-173 Rule Details

Parameter	Description
Rule Name	allowed-rds-flavors
Identifier	allowed-rds-flavors
Description	If the flavor of an RDS instance is not within the specified scope, this cluster is noncompliant.
Tag	rds
Trigger Type	Configuration change
Filter Type	rds.instances
Rule Parameter	listOfAllowedFlavors: RDS instance flavors

3.6.29.10 RDS Instances Have SSL Enabled

Rule Details

Table 3-174 Rule details

Parameter	Description
Rule Name	rds-instance-ssl-enable
Identifier	rds-instance-ssl-enable
Description	If SSL 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

3.6.29.11 RDS Instance Port Check

Rule Details

Table 3-175 Rule details

Parameter	Description
Rule Name	rds-instance-port-check
Identifier	rds-instance-port-check
Description	If an RDS instance has unallowed ports enabled, this instance is noncompliant.
Tag	rds
Trigger Type	Configuration change
Filter Type	rds.instances

Parameter	Description
Configure Rule Parameters	● **blockedPortsForMysql**: Unallowed MySQL database ports. The value must be an array. ● **blockedPortsForMariadb**: Unallowed MariaDB ports. The value must be an array. ● **blockedPortsForPostgresql**: Unallowed PostgreSQL ports. The value must be an array. ● **blockedPortsForSqlserver**: Unallowed SQLServer ports. The value must be an array.

3.6.29.12 Version Check for RDS Instance Engines

Rule Details

Table 3-176 Rule details

Parameter	Description
Rule Name	rds-instance-engine-version-check
Identifier	instance-engine-version-check
Description	If the version of an RDS instance engine is lower than the specified version, this instance is noncompliant.
Tag	rds
Trigger Type	Configuration change
Filter Type	rds.instances
Configure Rule Parameters	● **mysqlVersion**: ID of MySQL database engine, such as 8.0.28 ● **postgresqlVersion**: ID of PostgreSQL database engine, such as 10.16 ● **mariadbVersion**: ID of MariaDB database engine, such as 10.5. ● **sqlserverVersion**: ID of SQLServer database engine, such as 2017.

3.6.29.13 RDS Instances Have Audit Log Enabled

Rule Details

Table 3-177 Rule details

Parameter	Description
Rule Name	rds-instance-enable-auditLog
Identifier	rds-instance-enable-auditLog
Description	If an RDS instance does not have the audit log enabled or has audit logs kept for less than the specified number of days, this instance is noncompliant.
Tag	rds
Trigger Type	Configuration change
Filter Type	rds.instances
Configure Rule Parameters	**keepDays**: number of days for storing audit logs

3.6.30 GaussDB

3.6.30.1 GaussDB Instances Are in the Specified VPC

Rule Details

Table 3-178 Rule details

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

Applicable Scenario

A VPC is a private network on the cloud. You can create VPCs to logically isolate your GaussDB instances. For more details, see **What Is Virtual Private Cloud?**

Solution

You cannot change VPCs or subnets of GaussDB instances. You can use a GaussDB backup to create a new RDS instance and deploy the instance to the desired VPC and subnet. For details, see **Data Restoration**.

Rule Logic

- If a GaussDB instance is not in the specified VPC, this instance is noncompliant.
- If a GaussDB instance is in the specified VPC, this instance is compliant.

3.6.30.2 Audit Log Collection Is Enabled

Rule Details

Table 3-179 Rule details

Parameter	Description
Rule Name	gaussdb-instance-enable-auditLog
Identifier	gaussdb-instance-enable-auditLog
Description	If the audit log is not enabled for a GaussDB instance, this instance is noncompliant.
Tag	gaussdb
Trigger Type	Configuration change
Filter Type	gaussdb.instance
Configure Rule Parameters	None

3.6.30.3 Automated Backup Is Enabled

Rule Details

Table 3-180 Rule details

Parameter	Description
Rule Name	gaussdb-instance-enable-backup
Identifier	gaussdb-instance-enable-backup

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

3.6.30.4 Error Log Collection Is Enabled

Rule Details

Table 3-181 Rule details

Parameter	Description
Rule Name	gaussdb-instance-enable-errorLog
Identifier	gaussdb-instance-enable-errorLog
Description	If error log collection is not enabled for a GaussDB instance, this instance is noncompliant.
Tag	gaussdb
Trigger Type	Configuration change
Filter Type	gaussdb.instance
Configure Rule Parameters	None

3.6.30.5 Slow Query Log Collection Is Enabled

Rule Details

Table 3-182 Rule details

Parameter	Description
Rule Name	gaussdb-instance-enable-slowLog
Identifier	gaussdb-instance-enable-slowLog

Parameter	Description
Description	If the slow log is not enabled for a GaussDB instance, this instance is noncompliant.
Tag	gaussdb
Trigger Type	Configuration change
Filter Type	gaussdb.instance
Configure Rule Parameters	None

3.6.30.6 GaussDB Instances Do Not Have EIPs Attached

Rule Details

Table 3-183 Rule details

Parameter	Description
Rule Name	gaussdb-instance-no-public-ip-check
Identifier	gaussdb-instance-no-public-ip-check
Description	If a GaussDB instance is attached to any EIPs, this instance is noncompliant.
Tag	gaussdb
Trigger Type	Configuration change
Filter Type	gaussdb.instance
Configure Rule Parameters	None

3.6.30.7 Cross-AZ Deployment Check

Rule Details

Table 3-184 Rule details

Parameter	Description
Rule Name	gaussdb-instance-multiple-az-check
Identifier	gaussdb-instance-no-public-ip-check

Parameter	Description
Description	If a GaussDB instance does not support cross-AZ deployment, this instance is noncompliant.
Tag	gaussdb
Trigger Type	Configuration change
Filter Type	gaussdb.instance
Configure Rule Parameters	None

3.6.30.8 Data Transmission Encryption Is Enabled

Rule Details

Table 3-185 Rule details

Parameter	Description
Rule Name	gaussdb-instance-ssl-enable
Identifier	gaussdb-instance-ssl-enable
Description	If a GaussDB instance does not have SSL enabled, this instance is noncompliant.
Tag	gaussdb
Trigger Type	Configuration change
Filter Type	gaussdb.instance
Configure Rule Parameters	None

3.6.31 TaurusDB

3.6.31.1 The Slow Query Log Is Enabled

Rule Details

Table 3-186 Rule details

Parameter	Description
Rule Name	gaussdb-mysql-instance-enable-slowlog

Parameter	Description
Identifier	gaussdb-mysql-instance-enable-slowlog
Description	If the slow query log is not enabled for a TaurusDB instance, this instance is noncompliant.
Tag	taurusdb
Trigger Type	Configuration change
Filter Type	gaussdbformysql.instance
Configure Rule Parameters	None

3.6.31.2 The Error Log Is Enabled

Rule Details

Table 3-187 Rule details

Parameter	Description
Rule Name	gaussdb-mysql-instance-enable-errorlog
Identifier	gaussdb-mysql-instance-enable-errorlog
Description	If the error log is not enabled for a TaurusDB instance, this instance is noncompliant.
Tag	taurusdb
Trigger Type	Configuration change
Filter Type	gaussdbformysql.instance
Configure Rule Parameters	None

3.6.31.3 Backup Is Enabled

Rule Details

Table 3-188 Rule details

Parameter	Description
Rule Name	gaussdb-mysql-instance-enable-backup
Identifier	gaussdb-mysql-instance-enable-backup

Parameter	Description
Description	If the backup is disabled for a TaurusDB instance, this instance is noncompliant.
Tag	taurusdb
Trigger Type	Configuration change
Filter Type	gaussdbformysql.instance
Configure Rule Parameters	None

3.6.31.4 The Audit Log Is Enabled

Rule Details

Table 3-189 Rule details

Parameter	Description
Rule Name	gaussdb-mysql-instance-enable-auditlog
Identifier	gaussdb-mysql-instance-enable-auditlog
Description	If the audit log is not enabled for a TaurusDB instance, this instance is noncompliant.
Tag	taurusdb
Trigger Type	Configuration change
Filter Type	gaussdbformysql.instance
Configure Rule Parameters	None

3.6.31.5 Data Transmission Encryption Is Enabled

Rule Details

Table 3-190 Rule details

Parameter	Description
Rule Name	gaussdb-mysql-instance-ssl-enable
Identifier	gaussdb-mysql-instance-ssl-enable

Parameter	Description
Description	If a TaurusDB instance does not have SSL enabled, this instance is noncompliant.
Tag	taurusdb
Trigger Type	Configuration change
Filter Type	gaussdbformysql.instance
Configure Rule Parameters	None

3.6.31.6 Cross-AZ Deployment Check

Rule Details

Table 3-191 Rule details

Parameter	Description
Rule Name	gaussdb-mysql-instance-multiple-az-check
Identifier	gaussdb-mysql-instance-multiple-az-check
Description	If a TaurusDB instance does not support cross-AZ deployment, this instance is noncompliant.
Tag	taurusdb
Trigger Type	Configuration change
Filter Type	gaussdbformysql.instance
Configure Rule Parameters	None

3.6.31.7 EIP Check

Rule Details

Table 3-192 Rule details

Parameter	Description
Rule Name	gaussdb-mysql-instance-no-public-ip-check
Identifier	gaussdb-mysql-instance-no-public-ip-check

Parameter	Description
Description	If a TaurusDB instance has an EIP associated, this instance is noncompliant.
Tag	taurusdb
Trigger Type	Configuration change
Filter Type	gaussdbformysql.instance
Configure Rule Parameters	None

3.6.31.8 VPC Check

Rule Details

Table 3-193 Rule details

Parameter	Description
Rule Name	gaussdb-mysql-instance-in-vpc
Identifier	gaussdb-mysql-instance-in-vpc
Description	If a TaurusDB instance is not in any of the specified VPCs, this instance is noncompliant.
Tag	taurusdb
Trigger Type	Configuration change
Filter Type	gaussdbformysql.instance
Configure Rule Parameters	**VpcIdList**: VPC IDs. The value must be an array.

Applicable Scenario

A VPC is a private network on the cloud. You can create VPCs to logically isolate your TaurusDB instances. For more details, see **What Is Virtual Private Cloud?**

Solution

You cannot change the VPC of a TaurusDB instance. Exercise caution when selecting a VPC. For details, see description of VPC in **Buying a Pay-per-Use DB Instance**.

Rule Logic

- If a TaurusDB instance is not in any of the specified VPCs, this instance is noncompliant.
- If a TaurusDB instance is in one of the specified VPCs, this instance is compliant.

3.6.32 GeminiDB

3.6.32.1 GeminiDB Instances Have the Slow Log Enabled

Rule Details

Table 3-194 Rule details

Parameter	Description
Name	gaussdb-nosql-support-slow-log
Identifier	gaussdb-nosql-support-slow-log
Description	If a GeminiDB instance does not have the slow log enabled, this instance is noncompliant.
Tag	gemini db
Trigger Type	Configuration change
Filter Type	nosql.instances
Configure Rule Parameters	None

3.6.32.2 GeminiDB Instances Have Error Log Collection Enabled

Rule Details

Table 3-195 Rule details

Parameter	Description
Name	gaussdb-nosql-enable-error-log
Identifier	gaussdb-nosql-enable-error-log
Description	If a GeminiDB instance does not have error log collection enabled, this instance is noncompliant.
Tag	gemini db
Trigger Type	Configuration change

Parameter	Description
Filter Type	nosql.instances
Configure Rule Parameters	None

3.6.32.3 GeminiDB Instances Have Disk Encryption Enabled

Rule Details

Table 3-196 Rule details

Parameter	Description
Name	gaussdb-nosql-enable-disk-encryption
Identifier	gaussdb-nosql-enable-disk-encryption
Description	If a GeminiDB instance does not have disk encryption enabled, this instance is noncompliant.
Tag	gemini db
Trigger Type	Configuration change
Filter Type	nosql.instances
Configure Rule Parameters	None

3.6.32.4 GeminiDB Instances Have Backup Enabled

Rule Details

Table 3-197 Rule details

Parameter	Description
Name	gaussdb-nosql-enable-backup
Identifier	gaussdb-nosql-enable-backup
Description	If a GeminiDB instance does not have backup enabled, this instance is noncompliant.
Tag	gemini db
Trigger Type	Configuration change
Filter Type	nosql.instances

Parameter	Description
Configure Rule Parameters	None

3.6.32.5 Single-AZ Instance Check

Rule Details

Table 3-198 Rule details

Parameter	Description
Rule Name	gaussdb-nosql-deploy-in-single-az
Identifier	gaussdb-nosql-deploy-in-single-az
Description	If there is a single-AZ GeminiDB instance, this rule is noncompliant.
Tag	gemini db
Trigger Type	Configuration change
Filter Type	nosql.instances
Configure Rule Parameters	None

3.6.33 Cloud Search Service

3.6.33.1 CSS Clusters Have the Security Mode Enabled

Rule Details

Table 3-199 Rule details

Parameter	Description
Rule Name	css-cluster-authority-enable
Identifier	css-cluster-authority-enable
Description	If a CSS cluster does not have the security mode enabled, this cluster is noncompliant.
Tag	css
Trigger Type	Configuration change

Parameter	Description
Filter Type	css.clusters
Configure Rule Parameters	None

Applicable Scenario

If the security mode is enabled for a cluster, identity authentication is required when users access the cluster. You can also authorize other users to access Kibana of the security cluster. For details, see **Authentication and Access Control**.

Solution

You can enable the security mode for clusters that support it. To enable the security mode, call the **Configuring the Security Mode** API.

Rule Logic

- If a CSS cluster does not have the security mode enabled, this cluster is noncompliant.
- If a CSS cluster has the security mode enabled, this cluster is compliant.

3.6.33.2 The Snapshot Function Is Enabled for CSS Clusters

Rule Details

Table 3-200 Rule details

Parameter	Description
Rule Name	css-cluster-backup-available
Identifier	css-cluster-backup-available
Description	If the snapshot function 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

Applicable Scenario

You can back up index data in clusters to avoid data loss. If data loss occurs or you want to retrieve data of a specified duration, users can restore the index data to obtain the data quickly. Index backup is implemented by creating cluster snapshots. When creating a backup for the first time, you are advised to back up data of all indexes.

Solution

You can enable the snapshot function for noncompliant CSS clusters. For details, see **Setting Automatic Snapshot Creation**.

Rule Logic

- If the snapshot function is not enabled for a CSS cluster, this cluster is noncompliant.
- If the snapshot function is enabled for a CSS cluster, this cluster is noncompliant.

3.6.33.3 Disk Encryption Is Enabled for CSS Clusters

Rule Details

Table 3-201 Rule details

Parameter	Description
Rule Name	css-cluster-disk-encryption-check
Identifier	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

Applicable Scenario

Disk encryption is helpful for data protection, especially when there is sensitive data.

Solution

Currently, CSS does not support disk encryption. Do not store sensitive data in CSS clusters.

Rule Logic

- If disk encryption is disabled for a CSS cluster, this cluster is noncompliant.
- If disk encryption is enabled for a CSS cluster, this cluster is compliant.

3.6.33.4 HTTPS Access Is Enabled for CSS Clusters

Rule Details

Table 3-202 Rule details

Parameter	Description
Rule Name	css-cluster-https-required
Identifier	css-cluster-https-required
Description	If **HTTPS Access** 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

Applicable Scenario

You can enable HTTPS for CSS clusters. If HTTPS is disabled, HTTP is used for cluster communication. This compromises data security, and public access cannot be enabled. For details, see **Changing the Security Mode of an Elasticsearch Cluster**.

Solution

To enable HTTPS access, the security mode must be enabled for the cluster. Once HTTPS access is enabled, all communication with the cluster will be encrypted. To enable the security mode, call the **Configuring the Security Mode** API.

Rule Logic

- If a CSS cluster does not have the security mode enabled, this cluster is noncompliant.
- If a CSS cluster has the security mode enabled but has HTTPS disabled, this cluster is noncompliant.
- If a CSS cluster has HTTPS enabled, this cluster is compliant.

3.6.33.5 CSS Clusters Are in Specified VPCs

Rule Details

Table 3-203 Rule details

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

Applicable Scenario

A VPC is a private network on the cloud. You can create VPCs to logically isolate your CSS clusters. For more details, see **What Is Virtual Private Cloud?**

Solution

You can redeploy noncompliant CSS clusters to required VPCs.

Rule Logic

- If a CSS cluster is not in any of the specified VPCs, this cluster is noncompliant.
- If a CSS cluster is in one of the specified VPCs, this cluster is compliant.

3.6.33.6 Single-AZ CSS Cluster Check

Rule Details

Table 3-204 Rule details

Parameter	Description
Rule Name	css-cluster-multiple-az-check
Identifier	css-cluster-multiple-az-check

Parameter	Description
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

Applicable Scenario

By deploying a CSS cluster across multiple AZs, you can increase the cluster's availability, lower the likelihood of data loss, and minimize service downtime. You can deploy a cluster across two or three AZs within a region. For details, see **Elasticsearch Cluster Planning Suggestions**

Solution

You can deploy a cluster across two or three AZs to enable cross-AZ HA. Ensure that nodes are distributed evenly across these AZs.

Rule Logic

- If a CSS cluster is deployed in a single AZ, this cluster is noncompliant.
- If a CSS cluster is deployed in at least two AZs, this cluster is compliant.

3.6.33.7 A CSS Cluster Has at Least Two Instances

Rule Details

Table 3-205 Rule details

Parameter	Description
Rule Name	css-cluster-multiple-instances-check
Identifier	css-cluster-multiple-instances-check
Description	If a CSS cluster only has one instance, this cluster is noncompliant.
Tag	css
Trigger Type	Configuration change
Filter Type	css.clusters

Parameter	Description
Configure Rule Parameters	None

Applicable Scenario

You can deploy a CSS cluster across multiple AZs to increase availability, lower the likelihood of data loss, and minimize service downtime. Ensure that there are at least two instances in a CSS cluster.

Solution

You can increase instances for noncompliant CSS clusters. For details, see **Scaling Out a Cluster**.

Rule Logic

- If a CSS cluster has only one node, this cluster is noncompliant.
- If a CSS cluster has at least two nodes, this cluster is compliant.

3.6.33.8 CSS Clusters Are Not Publicly Accessible

Rule Details

Table 3-206 Rule details

Parameter	Description
Rule Name	css-cluster-no-public-zone
Identifier	css-cluster-no-public-zone
Description	If a CSS cluster has public access enabled, this cluster is noncompliant.
Tag	css
Trigger Type	Configuration change
Filter Type	css.clusters
Configure Rule Parameters	None

Applicable Scenario

You can disable public access for noncompliant CSS clusters especially when there is sensitive data in those clusters. For details, see **Configuring Public Network Access for an Elasticsearch Cluster**.

Solution

You can call the **Disabling Public Network Access** API to disable public access for CSS clusters.

Rule Logic

- If a CSS cluster has public access enabled, this cluster is noncompliant.
- If a CSS cluster does not have public access enabled, this cluster is compliant.

3.6.33.9 CSS Clusters Support the Security Mode

Rule Details

Table 3-207 Rule details

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

Applicable Scenario

Clusters in non-security mode can be accessed without security authentication, and HTTP protocol is used to transmit data. Ensure access environment security and do not expose the access APIs to the public network. A security-mode cluster requires security authentication and supports authorization and encryption. It is advised to use HTTPS for communication to ensure data security. For details, see **Changing the Security Mode of an Elasticsearch Cluster**.

Solution

Some cluster versions do not support the security mode. Use a version that supports the security mode, for example, Elasticsearch 7.10.2.

Rule Logic

- If a CSS cluster does not support the security mode, this cluster is noncompliant.

- If a CSS cluster supports the security mode, this cluster is compliant.

3.6.33.10 CSS Clusters Have Access Control Enabled

Rule Details

Table 3-208 Rule details

Parameter	Description
Rule Name	css-cluster-not-enable-white-list
Identifier	css-cluster-not-enable-white-list
Description	If a CSS cluster does not have access control enabled, this cluster is noncompliant.
Tag	css
Trigger Type	Configuration change
Filter Type	css.clusters
Configure Rule Parameters	None

Applicable Scenario

If a CSS cluster has access control disabled, it is publically accessible by all IP addresses. If the access control is enabled, it is only accessible by whitelisted IP addresses over public networks. For details, see **Configuring Public Network Access**.

Solution

You can **enable access control** for noncompliant CSS clusters and configure an IP address white list to allow public access.

Rule Logic

- If a CSS cluster does not have pubic access enabled, this cluster is compliant.
- If a CSS cluster has public access enabled but does not have access control enabled, this cluster is noncompliant.
- If a CSS cluster has both public access and access control enabled, this cluster is compliant.

3.6.33.11 CSS Clusters Have Kibana Public Access Control Enabled

Rule Details

Table 3-209 Rule details

Parameter	Description
Rule Name	css-cluster-kibana-not-enable-white-list
Identifier	css-cluster-kibana-not-enable-white-list
Description	If a CSS cluster does not have Kibana public access control enabled, this cluster is noncompliant.
Tag	css
Trigger Type	Configuration change
Filter Type	css.clusters
Configure Rule Parameters	None

Applicable Scenario

If a CSS cluster has Kibana access control disabled, Kibana is publically accessible by all IP addresses. If Kibana access control is enabled, it is only accessible by whitelisted IP addresses over public networks. For details, see **Logging In to an Elasticsearch Cluster Using Kibana**.

Solution

You can call the **Enabling Kibana Public Access** API to whitelist IP addresses that can access Kibana.

Rule Logic

- If a CSS cluster does not have Kibana public access enabled, this cluster is compliant.
- If a CSS cluster has Kibana public access enabled but does not have access control enabled, this cluster is noncompliant.
- If a CSS cluster has both Kibana public access and access control enabled, this cluster is compliant.

3.6.33.12 CSS Clusters Have Slow Query Log Enabled

Rule Details

Table 3-210 Rule details

Parameter	Description
Rule Name	css-cluster-slowLog-enable
Identifier	css-cluster-slowLog-enable
Description	If a CSS cluster does not have slow query log enabled, this cluster is noncompliant.
Tag	css
Trigger Type	Configuration change
Filter Type	css.clusters
Configure Rule Parameters	None

Applicable Scenario

Elasticsearch and OpenSearch clusters provide deprecation logs, run logs, index slow logs, and search slow logs for users to trouble shoot related issues. For details, see **Querying and Managing Elasticsearch Cluster Logs**.

Solution

By default, CSS clusters provide slow query logs. If you need longer storage, you can dump the logs into an OBS bucket. For details, see **Modifying Basic Log Configurations**.

Rule Logic

- If a CSS cluster has slow query log disabled, this cluster is noncompliant.
- If a CSS cluster has slow query log enabled, this cluster is compliant.

3.6.34 Elastic Volume Service

3.6.34.1 EVS Disk Type Check

Rule Details

Table 3-211 Rule details

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

3.6.34.2 Disks Are Used Within the Specified Time

Rule Details

Table 3-212 Rule details

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

3.6.34.3 Idle EVS Disk Check

Rule Details

Table 3-213 Rule details

Parameter	Description
Rule Name	volume-unused-check
Identifier	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

3.6.34.4 EVS Disks Are Encrypted

Rule Details

Table 3-214 Rule details

Parameter	Description
Rule Name	volumes-encrypted-check
Identifier	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

3.6.34.5 Disk Encryption Are Enabled

Rule Details

Table 3-215 Rule details

Parameter	Description
Rule Name	volumes-encrypted-check-by-default
Identifier	volumes-encrypted-check-by-default
Description	If an EVS disk is not encrypted, this disk is noncompliant.
Tag	evs
Trigger Type	Configuration change
Filter Type	evs.volumes
Rule Parameter	None

3.6.34.6 EVS Disks Have Backup Vaults Attached

Rule Details

Table 3-216 Rule details

Parameter	Description
Rule Name	evs-protected-by-cbr
Identifier	evs-protected-by-cbr
Description	If an EVS disk does not have a backup vault attached, this disk is noncompliant.
Tag	cbr, evs
Trigger Type	Configuration change
Filter Type	evs.volumes
Rule Parameter	None

3.6.34.7 EVS Backup Time Check

Rule Details

Table 3-217 Rule details

Parameter	Description
Rule Name	evs-last-backup-created
Identifier	evs-last-backup-created
Description	If an EVS disk does not have a backup created within the specified period, this disk is noncompliant.
Tag	cbr, evs
Trigger Type	Periodic
Filter Type	evs.volumes
Configure Rule Parameters	**lastBackupAgeValue**: The required backup time interval (in hours) for EVS disks.

3.6.35 Cloud Certificate Manager

3.6.35.1 Private CAs Expiration Check

Rule Details

Table 3-218 Rule details

Parameter	Description
Rule Name	pca-certificate-authority-expiration-check
Identifier	pca-certificate-authority-expiration-check
Description	If the validity period of a private CA is not within the specified period, this CA is noncompliant.
Tag	pca
Trigger Type	Periodic
Filter Type	pca.ca
Configure Rule Parameters	**daysToExpiration**: indicates a validity period. This is an integer type parameter.

3.6.35.2 Expiration Check for Private Certificates

Rule Details

Table 3-219 Rule details

Parameter	Description
Rule Name	pca-certificate-expiration-check
Identifier	pca-certificate-expiration-check
Description	If the validity period of a certificate is not within the specified range, this certificate is noncompliant.
Tag	pca
Trigger Type	Periodic
Filter Type	pca.cert
Configure Rule Parameters	**daysToExpiration**: indicates a validity period. This is an integer type parameter.

3.6.35.3 Private Root CAs Are Disabled

Rule Details

Table 3-220 Rule details

Parameter	Description
Rule Name	pca-certificate-authority-root-disable
Identifier	pca-certificate-authority-root-disable
Description	If private root CAs are not disabled, this rule is noncompliant.
Tag	pca
Trigger Type	Configuration change
Filter Type	pca.ca
Configure Rule Parameters	None

3.6.35.4 Private CA Algorithm Check

Rule Details

Table 3-221 Rule details

Parameter	Description
Rule Name	pca-algorithm-check
Identifier	Algorithm Check
Description	If a private certificate or CA prohibits key-based algorithms or signature-based hash algorithms, the private certificate or CA is noncompliant.
Tag	pca
Trigger Type	Configuration change
Filter Type	pca.ca, pca.cert
Configure Rule Parameters	● **blockedKeyAlgorithm**: key algorithms. The value must be an array, for example, ["SM2", "RSA2048", "EC256"]. ● **blockedSignatureAlgorithm**: signature algorithms. The value must be an array, for example, ["SHA256"].

Applicable Scenario

Secure algorithms are critical for private CA and certificate security. You are advised to use algorithms that can ensure enough security for your resources. This will not costs much as they used to.

Solution

You can remove noncompliant private CAs and certificates, and purchase new ones that meet your security requirements.

Rule Logic

- If a private certificate or CA prohibits key-based algorithms or signature-based hash algorithms, the private certificate or CA is noncompliant.
- If a private certificate or CA does not prohibit key-based algorithms or signature-based hash algorithms, the private certificate or CA is compliant.

3.6.36 Distributed Message Service for Kafka

3.6.36.1 DMS Kafka Instances Have SSL Enabled for Private Access

Rule Details

Table 3-222 Rule details

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

3.6.36.2 DMS Kafka Instances Have Enabled SSL for Public Access

Rule Details

Table 3-223 Rule details

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

3.6.36.3 DMS Kafka Instances Are Not Publicly Accessible

Rule Details

Table 3-224 Rule Details

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

3.6.37 Distributed Message Service for RabbitMQ

3.6.37.1 RabbitMQ Instances Have SSL Enabled

Rule Details

Table 3-225 Rule details

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

3.6.37.2 DMS RabbitMQ Instances Have Public Access Enabled

Rule Details

Table 3-226 Rule details

Parameter	Description
Rule Name	dms-rabbitmq-public-access-enabled-check
Identifier	dms-rabbitmq-public-access-enabled-check
Description	If a DMS RabbitMQ instance has public access enabled, this instance is noncompliant.
Tag	dms
Trigger Type	Configuration change
Filter Type	dms.rabbitmqs
Configure Rule Parameters	None

Applicable Scenario

To access a RabbitMQ instance over a public network, enable public access for the instance. If public access is no longer required, disable it in a timely manner.

Solution

You can **disable public access** for noncompliant RabbitMQ instances to protect them form public network access.

Rule Logic

- If a DMS RabbitMQ instance has public access enabled, this instance is noncompliant.
- If a DMS RabbitMQ instance does not have public access enabled, this instance is compliant.

3.6.38 Distributed Message Service for RocketMQ

3.6.38.1 DMS RocketMQ Instances Have SSL Enabled

Rule Details

Table 3-227 Rule details

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

3.6.38.2 RocketMQ Allows Public Access

Rule Details

Table 3-228 Rule details

Parameter	Description
Rule Name	dms-reliability-public-access-enabled-check
Identifier	dms-reliability-public-access-enabled-check
Description	If a DMS RocketMQ instance allows public access, the RocketMQ instance is noncompliant.
Tag	dms
Trigger Type	Configuration change
Filter Type	dms.reliabilitys
Configure Rule Parameters	None

Applicable Scenario

To access a RocketMQ instance over a public network, enable public access and configure EIPs for the instance. If you no longer need public access to the instance, disable it.

Solution

You can **disable public access** for noncompliant RocketMQ instances to protect them form public network access.

Rule Logic

- If a DMS RocketMQ instance allows public access, this instance is noncompliant.
- If a DMS RocketMQ instance does not allow public access, this instance is compliant.

3.6.39 Organizations

3.6.39.1 Accounts Have Been Added to Organizations

Rule Details

Table 3-229 Rule details

Parameter	Description
Rule Name	account-part-of-organizations
Identifier	account-part-of-organizations
Description	If an account has not been added to any organizations or to a specified organization, this account is noncompliant.
Tag	organizations
Trigger Type	Periodic
Filter Type	Account
Rule Parameter	domainId: The account ID an organization administrator. An empty string indicates any account ID.

3.6.40 Cloud Firewall

3.6.40.1 CFW Instances Have Protection Policies Attached

Rule Details

Table 3-230 Rule details

Parameter	Description
Rule Name	cfw-policy-not-empty

Parameter	Description
Identifier	cfw-policy-not-empty
Description	If a CFW instance does not have a protection policy attached, this instance is noncompliant.
Tag	cfw
Trigger Type	Configuration change
Filter Type	cfw.cfw_instance
Rule Parameter	None

3.6.41 Cloud Backup and Recovery

3.6.41.1 Backup Encryption Check

Rule Details

Table 3-231 Rule details

Parameter	Description
Rule Name	cbr-backup-encrypted-check
Identifier	cbr-backup-encrypted-check
Description	If a CBR backup is not encrypted, this backup is noncompliant.
Tag	cbr
Trigger Type	Configuration change
Filter Type	cbr.backup
Configure Rule Parameters	None

3.6.41.2 Backup Policy Execution Frequency Check

Rule Details

Table 3-232 Rule details

Parameter	Description
Rule Name	cbr-policy-minimum-frequency-check
Identifier	cbr-policy-minimum-frequency-check
Description	If the execution frequency of a backup policy is lower within the specified frequency, this policy is noncompliant.
Tag	cbr
Trigger Type	Configuration change
Filter Type	cbr.policy
Configure Rule Parameters	**requiredFrequency**: Backup interval, in hours.

Rule Logic

- If a backup policy is disabled, this rule is noncompliant.
- If the backup interval of a policy is less than or equal to the specified interval, this rule is compliant.
- If the backup interval of a policy is greater than the specified interval, this rule is noncompliant.

3.6.41.3 Minimum Retention Days of CBR Vault

Rule Details

Table 3-233 Rule details

Parameter	Description
Rule Name	cbr-vault-minimum-retention-check
Identifier	cbr-vault-minimum-retention-check
Description	If a CBR vault has no policies attached or has a policy that is retained for less than the specified period (in days), this vault is noncompliant.
Tag	cbr
Trigger Type	Configuration change

Parameter	Description
Filter Type	cbr.vault
Configure Rule Parameters	**requiredRetentionDays**: The required retention days for a vault policy.

3.6.42 Object Storage Service

3.6.42.1 OBS Bucket Policies Do Not Allow Blacklisted Actions

Rule Details

Table 3-234 Rule details

Parameter	Description
Rule Name	obs-bucket-blacklisted-actions-prohibited
Identifier	obs-bucket-blacklisted-actions-prohibited
Description	If an OBS bucket has a policy that allows blacklisted actions for principals from other accounts, this bucket is noncompliant.
Tag	obs, access-analyzer-verified
Trigger Type	Configuration change
Filter Type	obs.buckets
Configure Rule Parameters	**blockedActionsPatterns**: Blacklisted actions.

Applicable Scenario

A bucket policy applies to the configured OBS bucket and objects in the bucket. You can use bucket policies to control the access of IAM users or other account to your OBS buckets. You are advised to apply the least privilege principle to ensure that a bucket policy only grants necessary permissions for certain tasks.

Solution

You can modify policies of noncompliant buckets through the **visual editor** or the **JSON view** to block the blacklisted actions.

Rule Logic

- If an OBS bucket does not have a policy that allows blacklisted actions for principals from other accounts, this bucket is compliant.

- If an OBS bucket has a policy that allows blacklisted actions for principals from other accounts, this bucket is noncompliant.

3.6.42.2 OBS Bucket Policies Only Allow Access from the Specified Objects

Rule Details

Table 3-235 Rule details

Parameter	Description
Rule Name	obs-bucket-policy-grantee-check
Identifier	obs-bucket-policy-grantee-check
Description	If an OBS bucket has a policy that allows access from an object that is not one of the specified ones, this bucket is noncompliant.
Tag	obs, access-analyzer-verified
Trigger Type	Configuration change
Filter Type	obs.buckets
Configure Rule Parameters	● **principal**: authorized identities, for example, *domain/aaaa:user/111111* and *domain/bbbb* ● **sourceIp**: authorized source IPs, for example 192.168.0.0/16 ● **sourceVpc**: authorized source VPCs. Enter VPC IDs, for example, *vpcidaaaa*. ● **sourceVpce**: authorized VPC endpoints. Enter VPC endpoint IDs, for example, *vpceidaaaa*. Note: The parameters should have the same format as the principals or conditions in OBS bucket policies.

Applicable Scenario

A bucket policy applies to the configured OBS bucket and objects in the bucket. You can use bucket policies to control the access of IAM users or other account to your OBS buckets. You are advised to apply the least privilege principle to ensure that a bucket policy only grants necessary permissions for certain tasks.

Solution

You can modify policies for noncompliant buckets through the **visual editor** or the **JSON view** to restrict access from other objects than the authorized ones.

Rule Logic

- If an OBS bucket does not have any policies that allow access from an object except the specified ones, this bucket is compliant.

- If an OBS bucket has a policy that allows access from an object that is not one of the specified ones, this bucket is noncompliant.
- Note: The parameters specified in **Configure Rule Parameters** must have the same format as the principals or conditions in OBS bucket policies.

3.6.42.3 Permission Boundary Check

Rule Details

Table 3-236 Rule details

Parameter	Description
Rule Name	obs-bucket-policy-not-more-permissive
Identifier	obs-bucket-policy-not-more-permissive
Description	If an OBS bucket has a policy that allows more permissions than the specified policy, this bucket is noncompliant.
Tag	obs, access-analyzer-verified
Trigger Type	Configuration change
Filter Type	obs.buckets
Configure Rule Parameters	**controlPolicy**: the provided policy that defines the permission boundary. **NOTE** ● Parameter example 1: A bucket policy grants only permissions for operating objects instead of buckets. {"Statement": [{"Action": ["*Object*"], "Resource": ["*/*"], "Effect": "Allow", "Principal": {"ID": ["*"]}}]} ● Example 2: A policy grants access only to Huawei Cloud accounts instead of federated users or anonymous users. {"Statement": [{"Action": ["*"], "Resource": ["*"], "Effect": "Allow", "Principal": {"ID": ["domain/*"]}}]}

Applicable Scenario

A bucket policy applies to the configured OBS bucket and objects in the bucket. You can use bucket policies to control the access of IAM users or other account to your OBS buckets. You are advised to apply the least privilege principle to ensure that a bucket policy only grants necessary permissions for certain tasks.

Solution

You can modify policies for noncompliant buckets through the **visual editor** or the **JSON view** to restrict access from other objects than the authorized ones.

Rule Logic

- If an OBS bucket policy allows more permissions than the specified **controlPolicy**, this bucket is noncompliant.
- If an OBS bucket policy does not allow more permissions than the specified **controlPolicy**, this bucket is compliant.

3.6.42.4 OBS Bucket Policies Do Not Allow Public Read Access

Rule Details

Table 3-237 Rule details

Parameter	Description
Rule Name	obs-bucket-public-read-policy-check
Identifier	obs-bucket-public-read-policy-check
Description	If an OBS bucket allows public read access, this bucket is noncompliant.
Tag	obs, access-analyzer-verified
Trigger Type	Configuration change
Filter Type	obs.buckets
Configure Rule Parameters	None

Applicable Scenario

A bucket policy applies to the configured OBS bucket and objects in the bucket. You can use bucket policies to control the access of IAM users or other account to your OBS buckets. You are advised to apply the least privilege principle to ensure that a bucket policy only grants necessary permissions for certain tasks.

Solution

You can modify policies of noncompliant buckets through the **visual editor** or the **JSON view** to block public read access.

Rule Logic

- If an OBS bucket has a policy that allows read access from other accounts, this bucket is noncompliant.
- An OBS bucket has an ACL that allows read access from principles in addition to the current account and the log delivery user groups of the bucket, this bucket is noncompliant.
- If an OBS bucket has neither a policy nor an ACL as described above, this bucket is compliant.

3.6.42.5 OBS Bucket Policies Do Not Allow Public Write Access

Rule Details

Table 3-238 Rule details

Parameter	Description
Rule Name	obs-bucket-public-write-policy-check
Identifier	obs-bucket-public-write-policy-check
Description	If an OBS bucket allows public write access, this bucket is noncompliant.
Tag	obs, access-analyzer-verified
Trigger Type	Configuration change
Filter Type	obs.buckets
Configure Rule Parameters	None

Applicable Scenario

A bucket policy applies to the configured OBS bucket and objects in the bucket. You can use bucket policies to control the access of IAM users or other account to your OBS buckets. You are advised to apply the least privilege principle to ensure that a bucket policy only grants necessary permissions for certain tasks.

Solution

You can modify policies of noncompliant buckets through the **visual editor** or the **JSON view** to block public write access.

Rule Logic

- If an OBS bucket has a policy that allows write access from other accounts, this bucket is noncompliant.
- An OBS bucket has an ACL that allows write access from principles in addition to the current account and the log delivery user groups of the bucket, this bucket is noncompliant.
- If an OBS bucket has neither a policy nor an ACL as described above, this bucket is compliant.

3.6.42.6 OBS Buckets Do Not Allow HTTP Requests

Rule Details

Table 3-239 Rule details

Parameter	Description
Rule Name	obs-bucket-ssl-requests-only
Identifier	bucket-ssl-requests
Description	If an OBS bucket allows HTTP requests, this bucket is noncompliant.
Tag	obs, access-analyzer-verified
Trigger Type	Configuration change
Filter Type	obs.buckets
Configure Rule Parameters	None

Applicable Scenario

This rule prevents data theft and tampering during transmission to OBS.

Solution

To prevent clients from using HTTP to perform OBS operations, you are advised to include the **SecureTransport** condition in the bucket policy, specifying that only HTTPS requests are allowed. If **SecureTransport** is set to **True**, requests must be encrypted using SSL. For details about how to configure **Condition** and **SecureTransport** in a bucket policy, see **Bucket Policy Parameters**.

To block HTTP requests, add the condition: **"Condition": {"Bool": {"g:SecureTransport": ["true"]}}** to bucket policies.

Rule Logic

- If an OBS bucket denies requests that are not encrypted with SSL, this bucket is compliant.
- If an OBS bucket allows requests that are not encrypted with SSL, this bucket is noncompliant.
- Whether an OBS bucket policy allows requests that are not encrypted with SSL is determined through the **SecureTransport** or **g:SecureTransport** parameter.

3.6.43 Image Management Service

3.6.43.1 Private Images Have Encryption Enabled

Rule Details

Table 3-240 Rule details

Parameter	Description
Rule Name	ims-images-enable-encryption
Identifier	ims-images-enable-encryption
Description	If a private image does not have encryption enabled, this image is noncompliant.
Tag	ims
Trigger Type	Configuration change
Filter Type	ims.images
Configure Rule Parameters	None

3.6.44 Bare Metal Server

3.6.44.1 BMSs Have Key Pair Login Enabled

Rule Details

Table 3-241 Rule details

Parameter	Description
Rule Name	bms-key-pair-security-login
Identifier	bms-key-pair-security-login
Description	If a BMS does not have key pair login enabled, ths BMS is noncompliant.
Tag	bms
Trigger Type	Configuration change
Filter Type	bms.servers
Configure Rule Parameters	None

3.6.45 Graph Engine Service

3.6.45.1 GES Graphs Are Encrypted Using KMS

Rule Details

Table 3-242 Rule details

Parameter	Description
Rule Name	ges-graphs-encrypted-check
Identifier	ges-graphs-encrypted-check
Description	If a GES graph is not encrypted using KMS, this graph is noncompliant.
Tag	ges
Trigger Type	Configuration change
Filter Type	ges.graphs
Configure Rule Parameters	None

Applicable Scenario

This rule ensures that your GES graphs are encrypted using KMS to protect data and reduce the risk of unauthorized data access.

Solution

When creating a GES graph, use KMS to encrypt the graph instance. For details, see **Creating a Graph Without Using a Template**.

Rule Logic

- If a GES graph is not encrypted using KMS, this graph is noncompliant.
- If a GES graph is encrypted using KMS, this graph is noncompliant.

3.6.45.2 GES Graphs Have LTS Enabled

Rule Details

Table 3-243 Rule details

Parameter	Description
Rule Name	ges-graphs-lts-enable

Parameter	Description
Identifier	ges-graphs-lts-enable
Description	If a GES graph has LTS disabled, this graph is noncompliant.
Tag	ges
Trigger Type	Configuration change
Filter Type	ges.graphs
Configure Rule Parameters	None

Applicable Scenario

If you need to check service logs, enable LTS.

Solution

You can enable LTS for noncompliant GES graphs. If there are no log groups and log streams available, go to LTS console to create one. For details, see **Enable LTS**.

Rule Logic

- If a GES graph has LTS disabled, this graph is noncompliant.
- If a GES graph has LTS enabled, this graph is compliant.

3.6.45.3 GES Graphs Support Cross-AZ HA

Rule Details

Table 3-244 Rule details

Parameter	Description
Rule Name	ges-graphs-multi-az-support
Identifier	ges-graphs-multi-az-support
Description	If a GES graph does not support cross-AZ HA, this graph is noncompliant.
Tag	ges
Trigger Type	Configuration change
Filter Type	ges.graphs
Configure Rule Parameters	None

Applicable Scenario

This rule ensures that your GES graphs have cross-AZ HA enabled. This enables failover to another AZ when there are faults.

Solution

You can enable cross-AZ HA for noncompliant GES graphs. For details, see **Creating a Graph Without Using a Template**.

Rule Logic

- If a GES graph does not support cross-AZ HA, this graph is noncompliant.
- If a GES graph supports cross-AZ HA, this graph is compliant.

3.7 Resource Compliance 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 unexpected 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 an Alarm Rule to Monitor an Event**.

NOTE

Currently, Config only supports Cloud Eye event monitoring in the **AP-Singapore** region.

The following table lists resource compliance events supported by event monitoring.

Table 3-245 Supported resource compliance events

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

For details about resource recorder events supported by event monitoring, see **Table 2-1**.

4 Conformance Packages

4.1 Overview

Functions

A conformance package is a collection of rules. With conformance packages, you can evaluate resource compliance using multiple rules at the same time and centrally query conformance data.

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 deploy these packages to all member accounts that are in the normal state in your organization.

Constraints and Limitation

- Up to 50 conformance packages (including organization conformance packages) and 500 rules can be created in an account.
- The resource recorder must be enabled before you create a conformance package. Config only evaluates resources that are recorded by the resource recorder.
- To deploy an organization conformance package to a member, the member account must be in the normal state, and the resource recorder must be enabled for the member.

Concepts

Sample template

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

Pre-defined conformance package:

A pre-defined conformance package is created using a sample template. To deploy a pre-defined conformance package, you only need to configure a few parameters.

Custom conformance package:

A custom conformance package is created using a custom template. You can include both predefined and custom rules in a custom template. When you deploy a conformance package, you can upload a package template or use a package template stored in an OBS bucket. 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:

- Evaluation results of a conformance package: All rules in the conformance package are used to evaluate resources. If a resource is found to be noncompliant by any of the rules in the package, the evaluation result is noncompliant. If all resources are compliant, the evaluation result is compliant.
- Evaluation results of a rule: Each rule in the conformance package has an evaluation result. If a resource is found to be noncompliant, the result is noncompliant. If all resources are compliant, the result is compliant.
- Compliance score: The percentage of resources that are evaluated as compliant by a conformance 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:

$$\text{Score} = \frac{\sum_{\text{Rules}} \text{Compliant resource count}}{\sum_{\text{Rules}} \text{Total resource count}} \times 100\%$$

Stack:

To create, update, and delete rules in a conformance package, an RFS resource stack is required. Stack is a concept of Resource Formation Service (RFS). For details, see **Basic Concepts**.

Status

Table 4-1 Conformance package deployment states

Value	State	Description
CREATE_SUCCESSFUL	Deployed	A conformance package has been deployed.
CREATE_IN_PROGRESS	Deploying	A conformance package is being deployed.

Value	State	Description
CREATE_FAILED	Abnormal	A conformance package fails to be deployed.
DELETE_IN_PROGRESS	Deleting	A conformance package is being deleted.
DELETE_FAILED	Deletion failed	A conformance package fails to be deleted.
ROLLBACK_SUCCESSFUL	Rolled back	Some rules in a conformance package failed to be created and were rolled back, and created rules were deleted.
ROLLBACK_IN_PROGRESS	Rolling back	Some rules in a conformance package failed to be created and were rolled back, and created rules were being deleted.
ROLLBACK_FAILED	Rollback failed	Some rules in a conformance package failed to be created, and rollback also failed. You can access RFS to check out the reasons.
UPDATE_SUCCESSFUL	Updated	A conformance package is updated.
UPDATE_IN_PROGRESS	Updating	A conformance package is being updated.
UPDATE_FAILED	Update failed	A conformance package fails to be updated.

Authorization

RFS resource stacks need to be authorized to create, delete, and update resources in a conformance package. When you create a conformance package, you need to assign RFS a required agency.

If you decide to not use custom authorization, Config will be automatically assigned an agency that contains required RFS permissions. You can also create a custom agency with IAM. The agency must contain required permissions for RFS to create, modify, and delete rules in a conformance package. For details about how to create an agency, see **Creating an Agency (by a Delegating Party)**.

NOTE

If you want to use a template in your OBS bucket to create a conformance package, configure a proper IAM policy and an OBS bucket policy to ensure that the template can be accessed. For more details, see **Object Storage Service User Guide** and **Resource Formation Service User Guide**.

4.2 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, the first evaluation using rules in the package will be automatically triggered. More evaluations will be triggered based on the specified trigger type of each rule. You can also manually trigger a rule for resource evaluation.

Constraints and Limitation

- Up to 50 conformance packages (including organization conformance packages) and 500 rules can be created in an account.
- To create or modify a conformance package, the resource recorder must be enabled. If the resource recorder is disabled, you can only view or delete conformance packages. For details, see **Configuring the Resource Recorder**.

Procedure

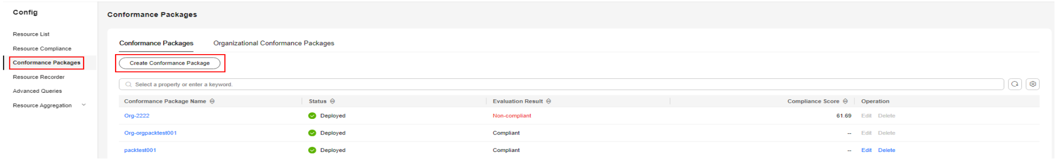
Step 1 Log in to the management console.

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



Conformance Package Name	Status	Evaluation Result	Compliance Score	Operation
Org-2222	Deployed	Non-compliant	61.69	Edit Delete
Org-orgpacktest001	Deployed	Compliant	--	Edit Delete
packtest001	Deployed	Compliant	--	Edit Delete

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

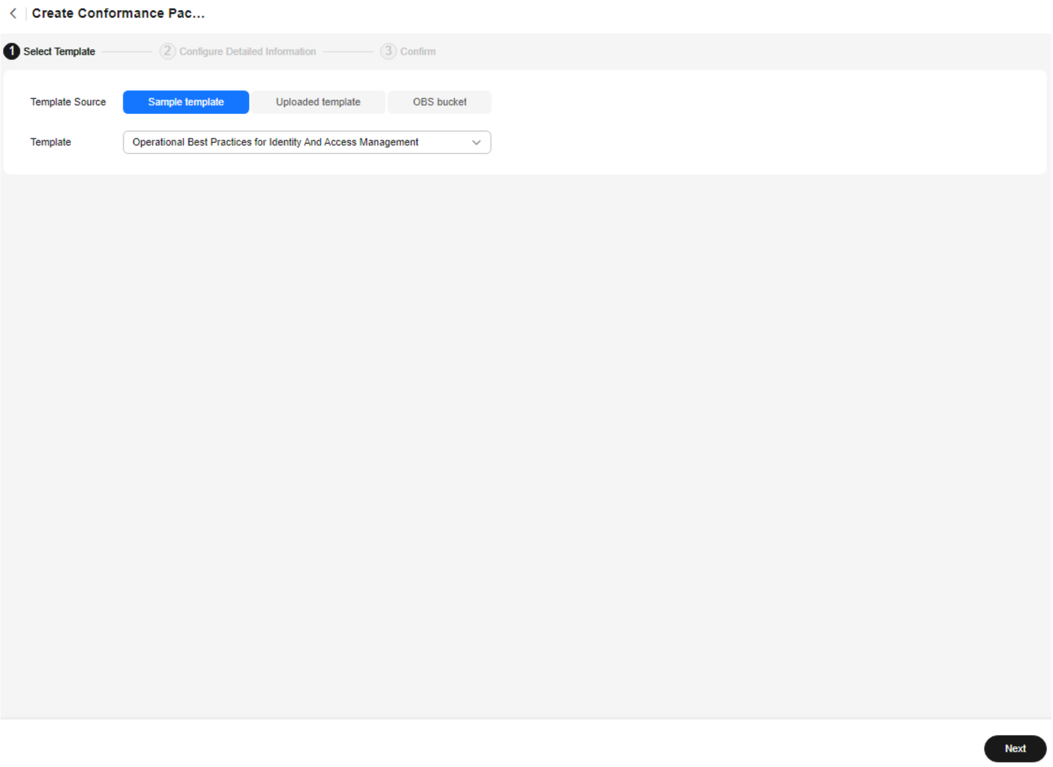
The template must be a JSON file (with the name extension: .tf.json). For details, see **custom conformance packages**.

- OBS bucket: The location of the OBS bucket that stores the custom conformance package template. 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

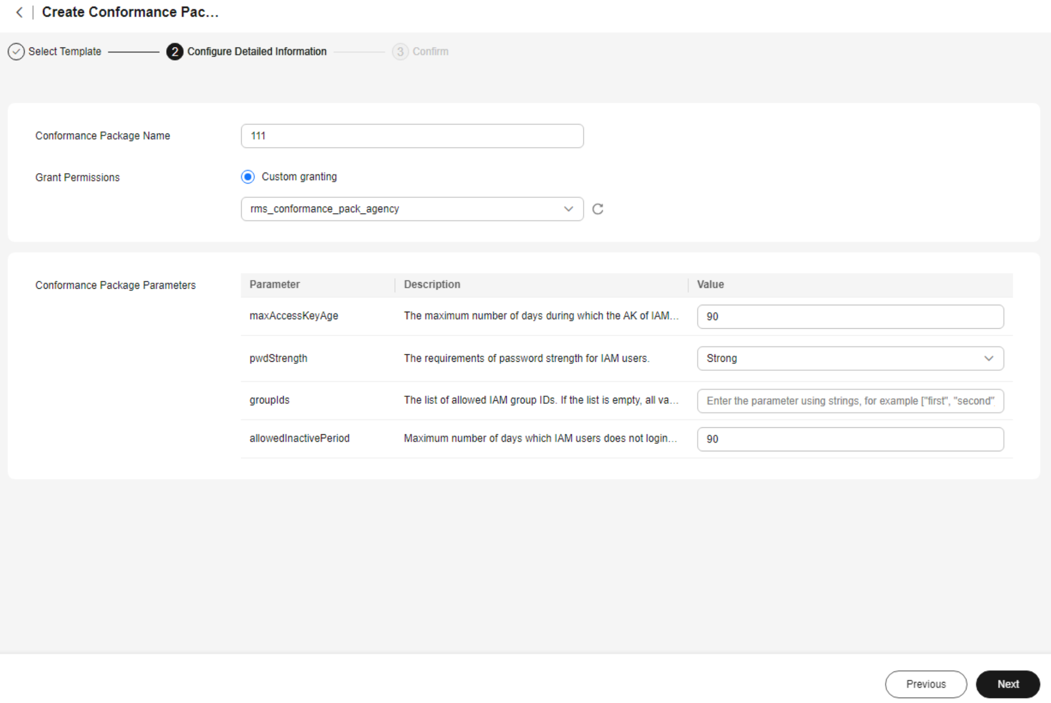


Template Source: Sample template

Template: Operational Best Practices for Identity And Access Management

Step 6 On the **Configure Detailed Information** page, configure required parameters and click **Next**.

Figure 4-4 Detailed information


Create Conformance Pac...

Select Template — 2 Configure Detailed Information — 3 Confirm

Conformance Package Name: 111

Grant Permissions: ● Custom granting

rms_conformance_pack_agency

Conformance Package Parameters

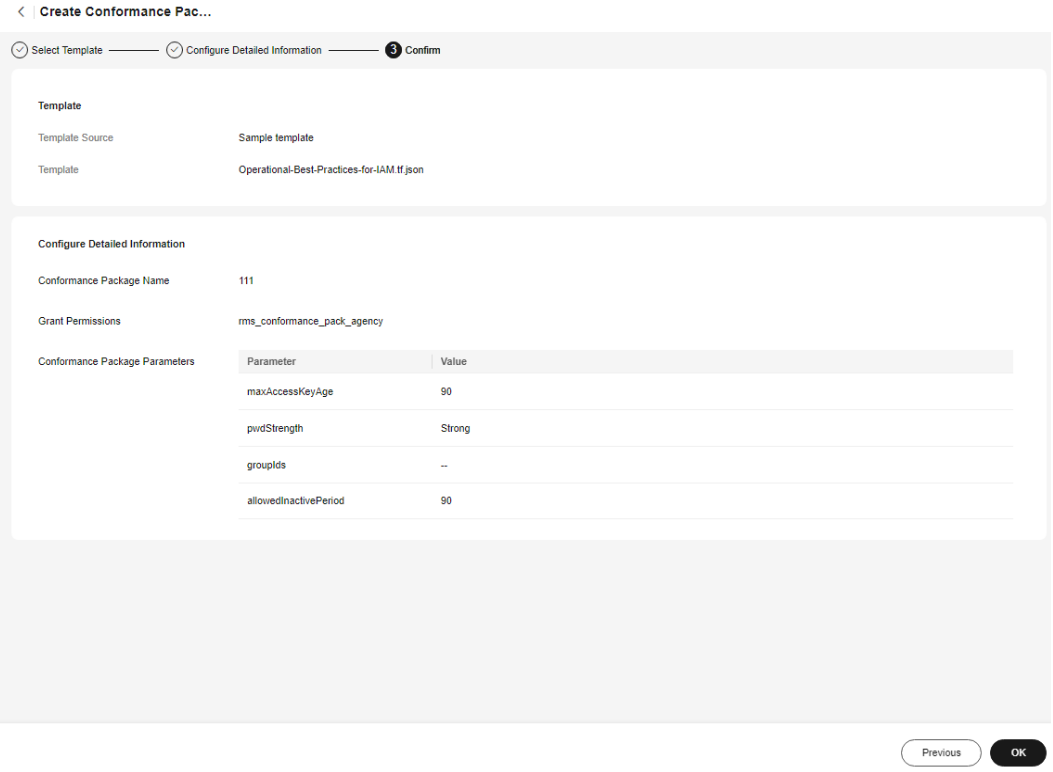
Parameter	Description	Value
maxAccessKeyAge	The maximum number of days during which the AK of IAM...	90
pwdStrength	The requirements of password strength for IAM users.	Strong
groupIds	The list of allowed IAM group IDs. If the list is empty, all va...	Enter the parameter using strings, for example ["first", "second"
allowedInactivePeriod	Maximum number of days which IAM users does not login...	90

Table 4-2 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.
(Optional) Authorization	**Agency authorization** is used. If you decide to not use custom authorization, Config will be automatically assigned an agency that contains required RFS permissions. You can also create a custom agency with IAM. The agency must contain required permissions for RFS to create, modify, and delete rules in a conformance package. 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 **OK**.

Figure 4-5 Confirming configurations



Template

Template Source	Sample template
Template	Operational-Best-Practices-for-IAM.tf.json

Configure Detailed Information

Conformance Package Name	111
Grant Permissions	rms_conformance_pack_agency

Conformance Package Parameters

Parameter	Value
maxAccessKeyAge	90
pwdStrength	Strong
groupIds	--
allowedInactivePeriod	90

NOTE

After a conformance package is created or updated, an evaluation will be automatically triggered.

----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**.

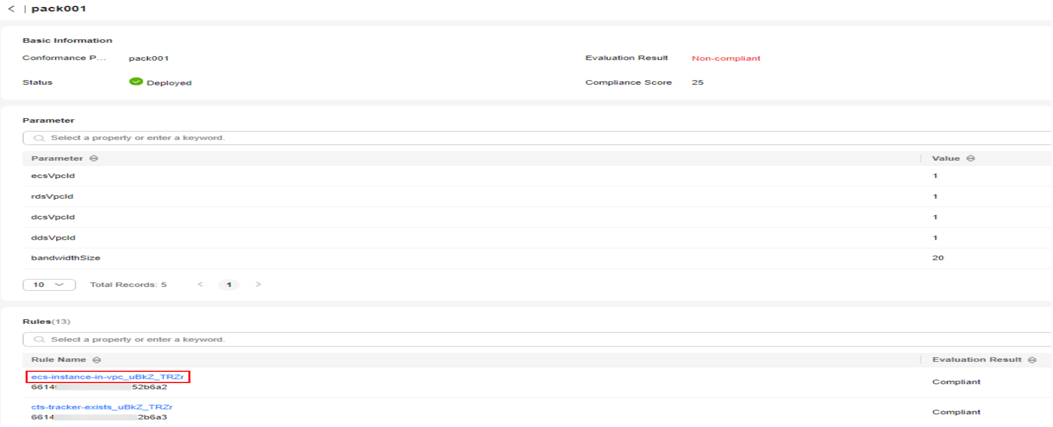
Step 4 View all the conformance packages created and their details, such as evaluation results, compliance scores, and status.

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, configurations, rules included, and the evaluation result of each rule.

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

Figure 4-6 Viewing details of a conformance package



< | pack001

Basic Information

Conformance P... pack001

Evaluation Result Non-compliant

Status Deployed

Compliance Score 25

Parameter

Select a property or enter a keyword.

Parameter	Value
ecsVpcId	1
rdsVpcId	1
dcsVpcId	1
ddsVpcId	1
bandwidthSize	20

10 Total Records: 5 < 1 >

Rules(13)

Select a property or enter a keyword.

Rule Name	Evaluation Result
ecs-instance-in-vpc_uBkZ_TRZr 6614[redacted]52b6a2	Compliant
cts-tracker-exists_uBkZ_TRZr 6614[redacted]2b6a3	Compliant

Table 4-3 Conformance package deployment states

Value	State	Description
CREATE_SUCCESSFUL	Deployed	A conformance package has been deployed.
CREATE_IN_PROGRESS	Deploying	A conformance package is being deployed.
CREATE_FAILED	Abnormal	A conformance package fails to be deployed.
DELETE_IN_PROGRESS	Deleting	A conformance package is being deleted.
DELETE_FAILED	Deletion failed	A conformance package fails to be deleted.
ROLLBACK_SUCCESSFUL	Rolled back	Some rules in a conformance package failed to be created and were rolled back, and created rules were deleted.
ROLLBACK_IN_PROGRESS	Rolling back	Some rules in a conformance package failed to be created and were rolled back, and created rules were being deleted.
ROLLBACK_FAILED	Rollback failed	Some rules in a conformance package failed to be created, and rollback also failed. You can access RFS to check out the reasons.

Value	State	Description
UPDATE_SUCCESSFUL	Updated	A conformance package is updated.
UPDATE_IN_PROGRESS	Updating	A conformance package is being updated.
UPDATE_FAILED	Update failed	A conformance package fails to be updated.

----End

4.2.3 Modifying a Conformance Package

Scenario

This section describes how to modify or update a conformance package.

NOTE

To create or modify a conformance package, the resource recorder must be enabled. If the resource recorder is disabled, you can only view or delete conformance packages. For details, see **Configuring the Resource Recorder**.

Procedure

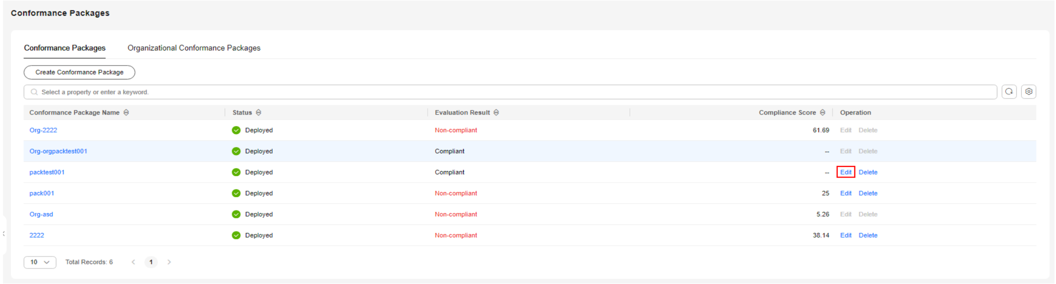
Step 1 Log in to the management console.

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 conformance package and click **Edit** in the **Operation** column to go the **Edit Conformance Package** page.

Figure 4-7 Editing a conformance package



Conformance Packages

Conformance Packages | Organizational Conformance Packages

Create Conformance Package

Select a property or enter a keyword.

Conformance Package Name	Status	Evaluation Result	Compliance Score	Operation
Org-2222	✓ Deployed	Non-compliant	61.69	Edit Delete
Org-orgpacktest001	✓ Deployed	Compliant	--	Edit Delete
packtest001	✓ Deployed	Compliant	--	Edit Delete
pack001	✓ Deployed	Non-compliant	25	Edit Delete
Org-asd	✓ Deployed	Non-compliant	5.26	Edit Delete
2222	✓ Deployed	Non-compliant	38.14	Edit Delete

10 Total Records: 6 < 1 >

Step 5 Click **Next**. Currently, conformance package templates do not support modification.

Step 6 Edit **Conformance Package Name** and **Conformance Package Parameters** and click **Next**.

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

A conformance package will be re-deployed after it is modified.

----End

4.2.4 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**.

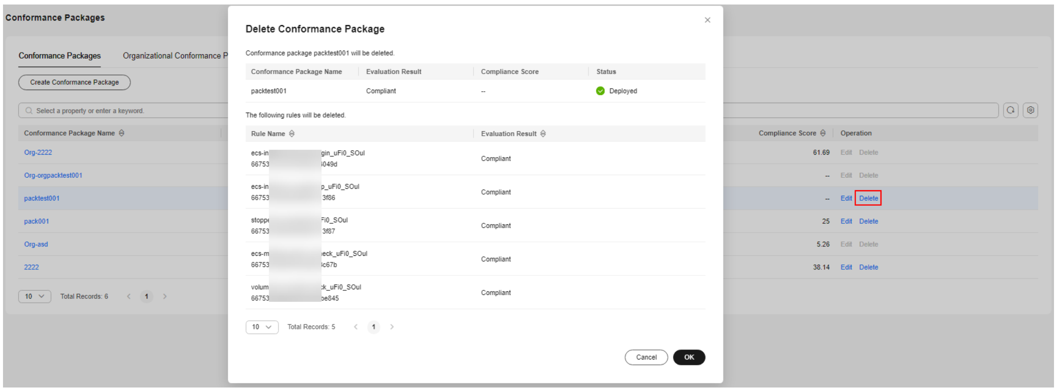
Step 3 On the left navigation pane, choose **Conformance Package**.

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 4-8 Deleting conformance packages



Conformance Packages

Conformance Packages | Organizational Conformance P

Create Conformance Package

Select a property or enter a keyword.

Conformance Package Name	Compliance Score	Operation
Org-2222	61.69	Edit Delete
Org-orgpacktest001	--	Edit Delete
packtest001	--	Edit Delete
pack001	25	Edit Delete
Org-asd	5.26	Edit Delete
2222	38.14	Edit Delete

10 Total Records: 6 < 1 >

Delete Conformance Package

Conformance package packtest001 will be deleted.

Conformance Package Name	Evaluation Result	Compliance Score	Status
packtest001	Compliant	--	✓ Deployed

The following rules will be deleted.

Rule Name	Evaluation Result
ecs-in[redacted]gin_uFi0_SOul 66753 049d	Compliant
ecs-in[redacted]p_uFi0_SOul 66753 3f86	Compliant
stoppe[redacted]Fi0_SOul 66753 3f87	Compliant
ecs-m[redacted]eck_uFi0_SOul 66753 c67b	Compliant
volum[redacted]k_uFi0_SOul 66753 be845	Compliant

10 Total Records: 5 < 1 >

Cancel OK

----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 that are in the normal state 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 with the rules in the package by default. Evaluations will be initiated each time the package is triggered. You can also trigger evaluation with a single rule in the rule list page.

Restrictions and Limitations

- Up to 50 conformance packages (including organization conformance packages) and 500 rules can be created in an account.
- To create or modify an organization conformance package, the resource recorder must be enabled. If the resource recorder is disabled, you can only view or delete organization conformance packages. For details, see **Configuring the Resource Recorder**.
- The **Organization Conformance Package** tab is inaccessible for an account that is not associated with any organizations.
- To deploy an organization conformance package to a member, the member account must be in the normal state, and the resource recorder must be enabled for the member.

Procedure

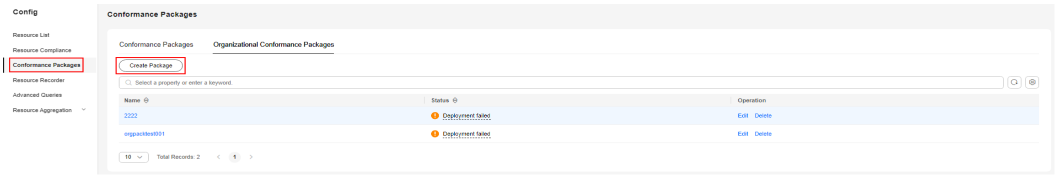
Step 1 Log in to the Config console as an organization administrator or an agency administrator of Config.

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 4-9 Creating an organization conformance package



Name	Status	Operation
2222	Deployment failed	Edit Delete
orgpacktest001	Deployment failed	Edit Delete

10 Total Records: 2 1

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.

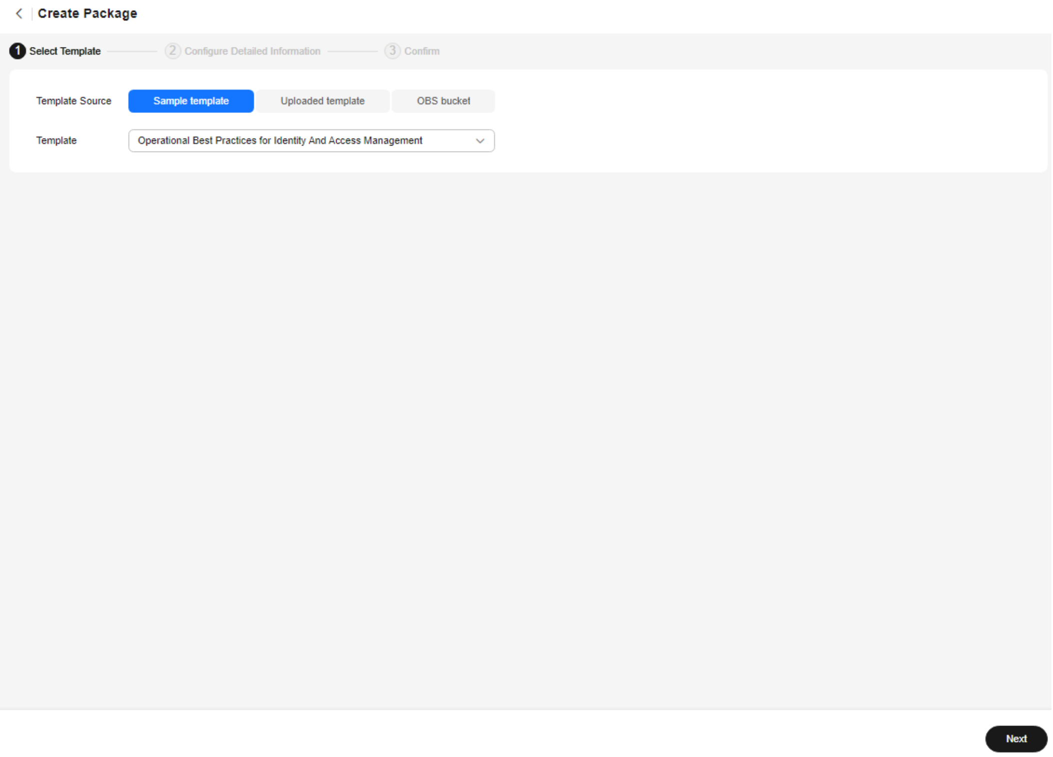
  For details about the rules contained in each sample template, see **conformance package sample template**.
- Local template: Templates uploaded locally. You can create a custom template and upload the template.

  The template must be a JSON file (with the name extension: .tf.json). For details, see **custom conformance packages**.
- OBS bucket: The location of the OBS bucket that stores the custom conformance package template. 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 4-10 Selecting a conformance package template

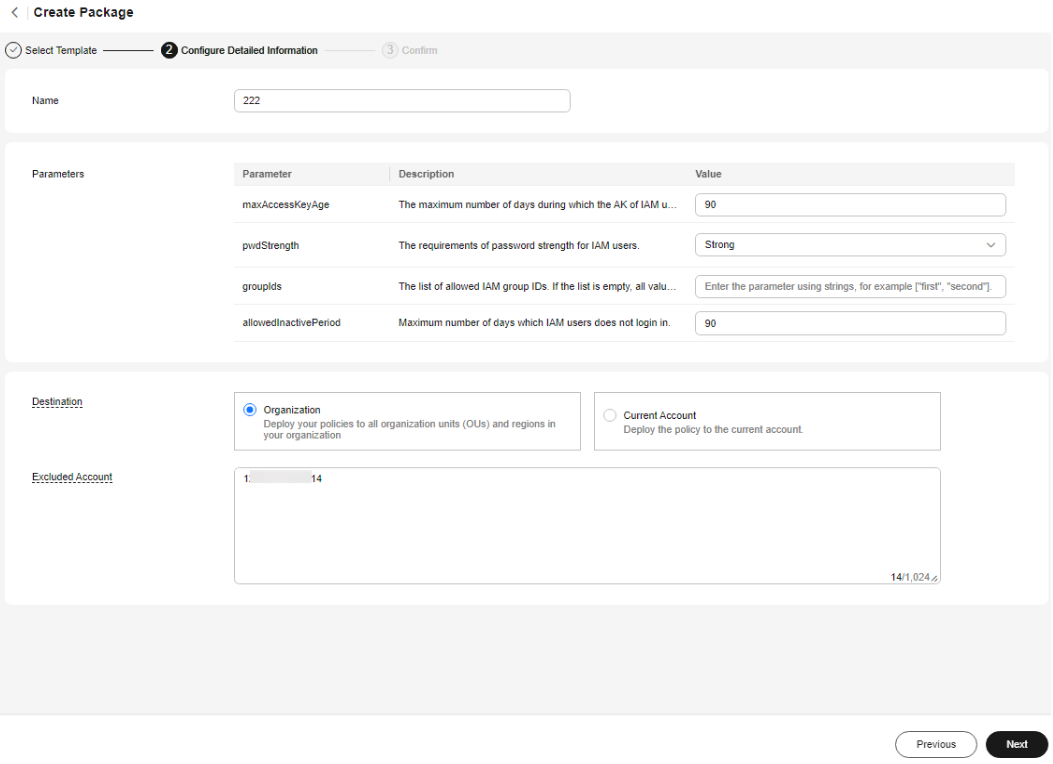


Template Source: Sample template

Template: Operational Best Practices for Identity And Access Management

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

Figure 4-11 Detailed information



Create Package

Select Template — 2 Configure Detailed Information — 3 Confirm

Name: 222

Parameters

Parameter	Description	Value
maxAccessKeyAge	The maximum number of days during which the AK of IAM u...	90
pwdStrength	The requirements of password strength for IAM users.	Strong
groupIds	The list of allowed IAM group IDs. If the list is empty, all valu...	Enter the parameter using strings, for example ["first", "second"].
allowedInactivePeriod	Maximum number of days which IAM users does not login in.	90

Destination

● Organization
Deploy your policies to all organization units (OUs) and regions in your organization

○ Current Account
Deploy the policy to the current account.

Excluded Account: 1[redacted]14

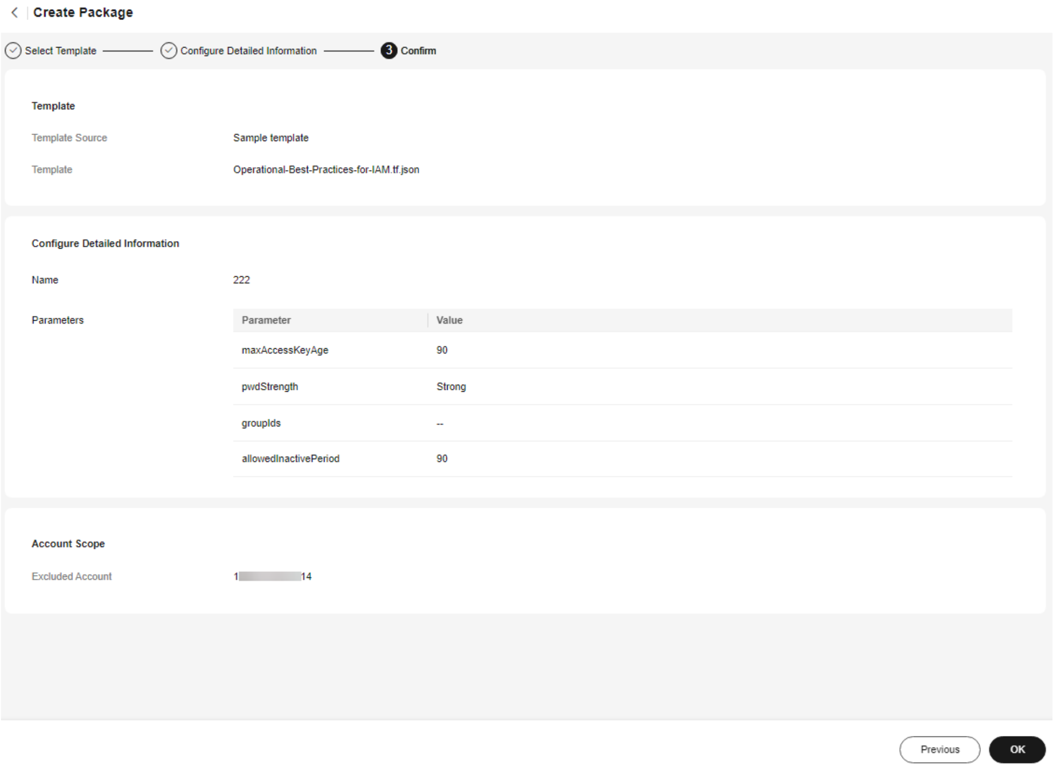
14/1,024

Table 4-4 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 to which organization conformance packages will not be deployed. This parameter is only required when **Destination** is set to **Organization**.

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

Figure 4-12 Confirming configurations



< Create Package

Select Template — Configure Detailed Information — 3 Confirm

Template

Template Source: Sample template

Template: Operational-Best-Practices-for-IAM.tf.json

Configure Detailed Information

Name: 222

Parameters:

Parameter	Value
maxAccessKeyAge	90
pwdStrength	Strong
groupIds	--
allowedInactivePeriod	90

Account Scope

Excluded Account: 1[redacted]14

NOTE

After an organization conformance package is created or updated, an evaluation will be automatically triggered.

----End

4.3.2 Viewing an Organization Conformance Package

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 consists of **Viewing an Organization Conformance Package (for Administrators)**, **Viewing an Organization Conformance Package (for Organization Members)**, and **Deployment Statuses of Organization Rules**.

Viewing an Organization Conformance Package (for Administrators)

Step 1 Log 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**.

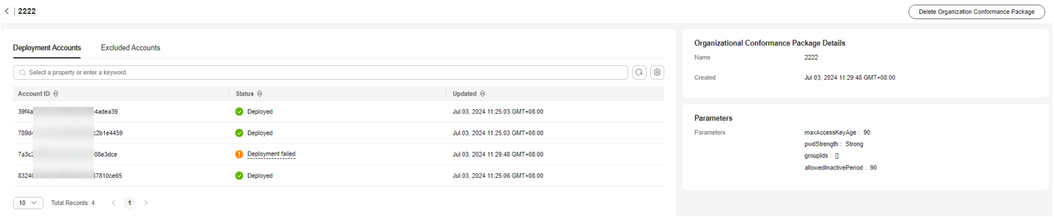
Step 3 On the left navigation pane, choose **Conformance Package**.

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 4-13 Organization details of an organization conformance package


< | 2222
Delete Organization Conformance Package
Deployment Accounts
Excluded Accounts
Select a property or enter a keyword.
10
Total Records: 4
1

Account ID	Status	Updated
39f4a[redacted]4adea39	Deployed	Jul 03, 2024 11:25:03 GMT+08:00
789d[redacted]c2b1e4459	Deployed	Jul 03, 2024 11:25:03 GMT+08:00
7a3c[redacted]08e3dce	Deployment failed	Jul 03, 2024 11:29:48 GMT+08:00
8324[redacted]37810ce65	Deployed	Jul 03, 2024 11:25:06 GMT+08:00

Organizational Conformance Package Details

Name 2222

Created Jul 03, 2024 11:29:48 GMT+08:00

Parameters

Parameters maxAccessKeyAge : 90
pwdStrength : Strong
groupIds : []
allowedInactivePeriod : 90

----End

Viewing an Organization Conformance Package (for Organization Members)

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

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

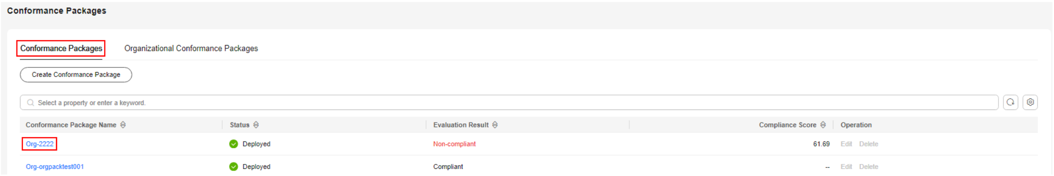
Step 3 On the left navigation pane, choose **Conformance Package**.

Step 4 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, configurations, rules included, and the evaluation result of each rule.

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

Figure 4-14 Viewing an organization conformance package (for organization members)


Conformance Packages
Conformance Packages
Organizational Conformance Packages
Create Conformance Package
Select a property or enter a keyword.

Conformance Package Name	Status	Evaluation Result	Compliance Score	Operation
Org-2222	Deployed	Non-compliant	61.69	Edit Delete
Org-orgpacktest001	Deployed	Compliant	--	Edit Delete

NOTE

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

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

----End

Deployment Statuses of Organization Rules

Table 4-5 Deployment statuses of organization rules

Value	Status	Description
CREATE_IN_PROGRESS	Deploying	An organization conformance package is being created.
UPDATE_IN_PROGRESS	Updating	An organization conformance package is being updated.
DELETE_IN_PROGRESS	Deleting	An organization conformance package is being deleted.
CREATE_FAILED	Abnormal	An organization conformance package fails to be deployed to one or more member accounts.
UPDATE_FAILED	Update failed	An organization conformance package fails to be updated in one or more member accounts.
DELETE_FAILED	Deletion failed	An organization conformance package fails to be deleted in one or more member accounts.
CREATE_SUCCESSFUL	Deployed	An organization conformance package has been deployed to all member accounts.
UPDATE_SUCCESSFUL	Updated	An organization conformance package has been updated in all member accounts.

4.3.3 Modifying an Organization Conformance Package

Scenario

You can modify the name or parameters of an organization conformance package at any time. If you fail to deploy an organization conformance package to some members in your organization, you can include these accounts in the **Excluded Account** area and then redeploy the package.

NOTE

To create or modify an organization conformance package, the resource recorder must be enabled. If the resource recorder is disabled, you can only view or delete organization conformance packages. For details, see **Configuring the Resource Recorder**.

Procedure

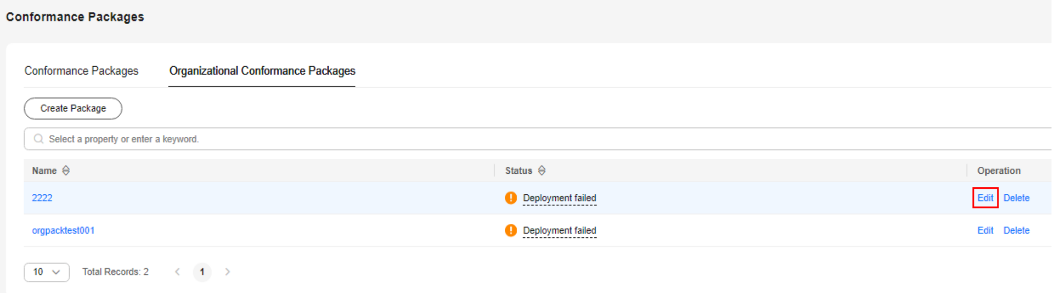
Step 1 Log in to the management console as an organization administrator or a delegated administrator of Config.

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 **Edit** in the **Operation** column.

Figure 4-15 Modifying an organization conformance package



Conformance Packages

Conformance Packages | Organizational Conformance Packages

Create Package

Select a property or enter a keyword.

Name	Status	Operation
2222	Deployment failed	Edit Delete
orgpacktest001	Deployment failed	Edit Delete

10 Total Records: 2 < 1 >

Step 5 In the **Edit Organization Conformance Package** page, click **Next**. Currently, conformance package templates do not support modification.

Step 6 Edit **Conformance Package Name** and **Conformance Package Parameters** and click **Next**.

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

An organization conformance package will be redeployed to specified organization members after it is modified.

----End

4.3.4 Deleting an Organization Conformance Package

Scenario

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

Procedure

Step 1 Log 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**.

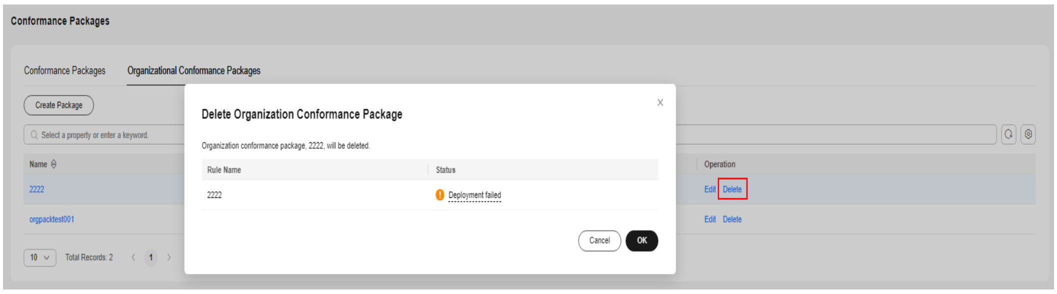
Step 3 On the left navigation pane, choose **Conformance Package**.

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 4-16 Deleting an organization conformance package



Delete Organization Conformance Package

Organization conformance package, 2222, will be deleted.

Rule Name	Status
2222	Deployment failed

----End

4.4 Custom Conformance Packages

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

NOTE

If you want to use a template in your OBS bucket to create a conformance package, configure a proper IAM policy and an OBS bucket policy to ensure that the template can be accessed. For more details, see **Object Storage Service User Guide** and **Resource Formation Service User Guide**.

Template Description

resource: The most important section in a template. Currently, only the **huaweicloud_rms_policy_assignment** resource type is supported. You can add both predefined rules and custom rules in the **resource** section.

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

terraform: The service provider. For details see **Provider**. The following example shows the format of a template:

```
"terraform": {
   "required_providers": {
      "huaweicloud": {
```

```
      "source": "huawei.com/provider/huaweicloud",
      "version": "1.66.2"
    }
  }
}
```

The version must be 1.66.2 or later. For details about the supported versions, see **Supported Provider Versions**.

Example 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": "1.66.2"
      }
    }
  }
}
```

Example 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": "1.66.2"
            }
        }
    }
}
```

4.5 Conformance Package Templates

4.5.1 Overview

Config provides sample templates to help users quickly create a conformance package. Each template contains multiple rules created with predefined policies. For details about predefined policies, see **Built-In 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:

- **Conformance Package for Classified Protection of Cybersecurity Level 3 (2.0)**
- **Conformance Package for the Financial Industry**
- **Conformance Package for Network Security**
- **Conformance Package for Identity and Access Management**
- **Conformance Package for Cloud Eye**
- **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 Enabling Public Access**
- **Conformance Package for Logging and Monitoring**
- **Conformance Package for Architecture Reliability**
- **Conformance Package for Hong Kong Monetary Authority of China Requirements**
- **Conformance Package for ENISA Requirements**
- **Conformance Package for SWIFT CSP**
- **Conformance Package for Germany Cloud Computing Compliance Criteria Catalogue**
- **Conformance Package for PCI DSS**
- **Conformance Package for Healthcare Industry**
- **Best Practices of Network and Data Security**
- **Conformance Package for Landing Zone**
- **Architecture Security Best Practices**
- **Best Practices for Network and Content Delivery Service Operations**

- **Best Practices for Idle Asset Management**
- **Multi-AZ Deployment Best Practices**
- **Resource Stability Best Practices**
- **Best Practices for API Gateway**
- **Best Practices for Cloud Container Engine**
- **Best Practices for Content Delivery Network**
- **Best Practices for FunctionGraph**
- **Best Practices for GaussDB**
- **Best Practices for GeminiDB**
- **Best Practices for MapReduce Service**
- **Best Practices for NIST Requirements**
- **Best Practices for Singapore Financial Industry**
- **Best Practices for Secure Identity and Compliance Operations**
- **Conformance Package for Huawei Cloud Security Configuration Guide (Level 1)**
- **Conformance Package for Huawei Cloud Security Configuration Guide (Level 2)**
- **Best Practices for Static Data Encryption**
- **Best Practices for Data Transmission Encryption**
- **Best Practices for Cloud Backup and Recovery**
- **Best Practices for Cloud Search Service**
- **Best Practices for Distributed Cache Service**
- **Best Practices for Distributed Message Service**
- **Best Practices for Data Warehouse Service**
- **Best Practices for TaurusDB**
- **Best Practices for Object Storage Service**
- **Best Practices for Virtual Private Cloud**
- **Best Practices for Web Application Firewall**

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

This section describes the background, applicable scenarios, and the conformance package to meet requirements by *Classified Protection of Cybersecurity Level 3 (2.0)*.

Background

Level-3 Information Security Protection 2.0 is a set of standards for information security by the Chinese government. It represents an important part of the classified information security protection system of China. This document is intended for information infrastructure sectors, such as the government, finance, telecommunications, and energy. It aims to ensure the security, integrity, and availability of information systems by provide guidance on how to prevent and resolve security threats and risks.

For more details about the basic requirements for classified protection of cybersecurity, see **GB/T 22239-2019**.

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 numbers in the following table are in consistent with the chapter numbers in **GB/T 22239-2019**.

Table 4-6

Guideline No.	Guideline Description	Config Rule	Solution
8.1.2.1	b. Bandwidths should be properly allocated for related networks to meet peak-hour needs.	eip-bandwidth-limit	Allocate sufficient bandwidth to meet peak-hour needs.
8.1.2.1	c. Network shall be divided into different subnets and IP addresses shall be allocated to them. The allocation should facilitate easy management and control.	dcs-redis-in-vpc	Deploy DCS instances within VPCs.
8.1.2.1	c. Network shall be divided into different subnets and IP addresses shall be allocated to them. The allocation should facilitate easy management and control.	ecs-instance-in-vpc	Deploy all ECSs within VPCs.

Guideline No.	Guideline Description	Config Rule	Solution
8.1.2.1	c. Network shall be divided into different subnets and IP addresses shall be allocated to them. The allocation should facilitate easy management and control.	rds-instances-in-vpc	Deploy all RDS instances within VPCs.
8.1.2.1	d. Important subnets shall not be deployed at borders. Reliable technical measures shall be taken to isolate important subnets from other subnets.	dcs-redis-in-vpc	Deploy DCS instances within VPCs.
8.1.2.1	d. Important subnets shall not be deployed at borders. Reliable technical measures shall be taken to isolate important subnets from other subnets.	ecs-instance-in-vpc	Deploy all ECSs within VPCs.
8.1.2.1	d. Important subnets shall not be deployed at borders. Reliable technical measures shall be taken to isolate important subnets from other subnets.	rds-instances-in-vpc	Deploy all RDS instances within VPCs.
8.1.3.1	b. Unauthorized device access to the internal network shall be detected or blocked.	ecs-instance-no-public-ip	Block public access to ECSs to protect sensitive data.

Guideline No.	Guideline Description	Config Rule	Solution
8.1.3.1	b. Unauthorized device access to the internal network shall be detected or blocked.	elb-loadbalancers-no-public-ip	Block public access to elastic load balancers.
8.1.3.1	b. Unauthorized device access to the internal network shall be detected or blocked.	rds-instance-no-public-ip	Block public access to RDS instances. RDS instances may contain sensitive information, and access control is required.
8.1.3.2	a. Access control policies should be configured for network-border or cross-region access. By default, controlled ports only allow specified access.	ecs-instance-no-public-ip	Block public access to ECSs to protect sensitive data.
8.1.3.2	a. Access control policies should be configured for network-border or cross-region access. By default, controlled ports only allow specified access.	elb-loadbalancers-no-public-ip	Block public access to elastic load balancers.
8.1.3.2	a. Access control policies should be configured for network-border or cross-region access. By default, controlled ports only allow specified access.	rds-instance-no-public-ip	Block public access to RDS instances. RDS instances may contain sensitive information, and access control is required.

Guideline No.	Guideline Description	Config Rule	Solution
8.1.3.5	c. Audit records shall be protected and regular backup should be performed to avoid unexpected deletion, modification, or overwriting.	cts-tracker-exists	Ensure that a CTS tracker has been created for your account to record operations on the Huawei Cloud console.
8.1.4.1	d. Two or more authentication methods, such as tokens, passwords, and biometric technologies, shall be used to authenticate user identity. Password authentication must be used.	iam-user-mfa-enabled	Enable MFA for all IAM users. MFA provides an additional layer of protection in addition to the username and password.
8.1.4.7	a. Cryptographic techniques should be used to ensure transmission integrity for important data, including but not limited to authentication data, service data, audit data, configuration data, video data, and personal information.	elb-tls-https-listeners-only	Ensure that load balancer listeners have been configured with the HTTPS protocol. Transmission encryption is helpful for data protection, especially when there is sensitive data.

Guideline No.	Guideline Description	Config Rule	Solution
8.1.4.7	b. Cryptographic techniques should be used to ensure the integrity of important data storage, including but not limited to authentication data, service data, audit data, configuration data, video data, and personal information.	volumes-encrypted-check	Encrypt mounted cloud disks to protect static data.
8.1.4.9	c. Hot redundancy should be provided for critical data processing systems to ensure high availability.	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 a fault occurs, RDS automatically fails over to the standby database so that you can restore databases in a timely manner.

4.5.3 Conformance Package for the Financial Industry

The following table lists the rules and solutions included in this conformance package template.

Table 4-7 Conformance package description

Rule Identifier	Cloud Service	Rule Content
access-keys-rotated	iam	If an IAM user's access key is not rotated within the specified number of days, this user is noncompliant.
as-group-elb-healthcheck-required	as	If an AS group is not using Elastic Load Balancing health check, the result is noncompliant.
css-cluster-https-required	css	If HTTPS is not enabled for a CSS cluster, this cluster is noncompliant.
css-cluster-in-vpc	css	If a CSS cluster is not in any of the specified VPCs, this cluster is noncompliant.
cts-kms-encrypted-check	cts	If a CTS tracker is not encrypted using KMS, this tracker is noncompliant.
cts-lts-enable	cts	If **Transfer to LTS** is not enabled for a CTS tracker, this tracker is noncompliant.
cts-obs-bucket-track	cts	If no CTS trackers are created for the specified OBS bucket, this rule is noncompliant.
cts-support-validate-check	cts	If **Verify Trace File** is not enabled for a CTS tracker, this tacker is noncompliant.
cts-tracker-exists	cts	If there are no CTS trackers in an account, this account is noncompliant.
ecs-instance-in-vpc	ecs, vpc	If an ECS is not within the specified VPC, this ECS is noncompliant.

Rule Identifier	Cloud Service	Rule Content
ecs-instance-no-public-ip	ecs	If an ECS has a public IP attached, this ECS is noncompliant.
eip-unbound-check	vpc	If an EIP has not been attached to any resource, this EIP is noncompliant.
elb-tls-https-listeners-only	elb	If any listener of a load balancer is not configured with HTTPS, this load balancer is noncompliant.
function-graph-concurrency-check	fgs	If the number of concurrent requests of a FunctionGraph function is not within the specified range, this function is noncompliant.
iam-group-has-users-check	iam	If an IAM user group has no user, this user group is noncompliant.
iam-password-policy	iam	If the password of an IAM user does not meet the password strength requirements, this IAM user is noncompliant.
iam-root-access-key-check	iam	If the account root user has an available access key, the account is noncompliant.
iam-user-group-membership-check	iam	If an IAM user is not in any of the specified IAM user groups, this user is noncompliant.
iam-user-last-login-check	iam	If an IAM user does not log in to the system within the specified time range, the result is non-compliant.
iam-user-mfa-enabled	iam	If multi-factor authentication is not enabled for an IAM user, this user is noncompliant.

Rule Identifier	Cloud Service	Rule Content
kms-rotation-enabled	kms	If key rotation is not enabled for a KMS key, this key is noncompliant.
mfa-enabled-for-iam-console-access	iam	If MFA is not enabled for an IAM user who has a console password, this IAM user is noncompliant.
mrs-cluster-in-vpc	mrs	If an MRS cluster is not in the specified VPC, this cluster is noncompliant.
mrs-cluster-kerberos-enabled	mrs	If kerberos is not enabled for an MRS cluster, this cluster is noncompliant.
mrs-cluster-no-public-ip	mrs	If an MRS cluster has an EIP attached, this cluster is noncompliant.
private-nat-gateway-authorized-vpc-only	nat	If a private NAT gateway is not in a specified VPC, this gateway is noncompliant.
rds-instance-multi-az-support	rds	If an RDS instance does not support multi-AZ deployment, this RDS instance is noncompliant.
rds-instance-no-public-ip	rds	If an RDS instance has an EIP attached, this RDS instance is noncompliant.
root-account-mfa-enabled	iam	If multi-factor authentication is not enabled for the root user, the root user is noncompliant.
stopped-ecs-date-diff	ecs	If an ECS has been stopped for longer than the time allowed, and no operations have been performed on it, this ECS is noncompliant.

Rule Identifier	Cloud Service	Rule Content
volume-unused-check	evs	If an EVS disk is not mounted to any cloud server, this disk is noncompliant.
volumes-encrypted-check	ecs, evs	If a mounted EVS disk is not encrypted, this disk is noncompliant.
vpc-acl-unused-check	vpc	If a network ACL is not attached to any subnets, this ACL is noncompliant.
vpc-flow-logs-enabled	vpc	If there is a flow log that has not been enabled for a VPC, this VPC is noncompliant.
vpc-sg-ports-check	vpc	If a security group allows all inbound traffic (with the source address set to **0.0.0.0/0**) and opens all TCP/UDP ports, this security group is noncompliant.
vpn-connections-active	vpnaas	If a VPN is not normally connected, this rule is noncompliant.
waf-instance-policy-not-empty	waf	If a WAF instance does not have a protection policy attached, this instance is noncompliant.

4.5.4 Conformance Package for Network Security

The following table lists the rules and solutions included in this conformance package template.

Table 4-8 Conformance package description

Rule	Cloud Service	Description
access-keys-rotated	iam	If an IAM user's access key is not rotated within the specified number of days, this user is noncompliant.

Rule	Cloud Service	Description
alarm-kms-disable-or-delete-key	ces, kms	If there are no alarm rules configured for disabling or deleting KMS keys, this rule is noncompliant.
alarm-obs-bucket-policy-change	ces, obs	If there are no alarm rules configured for OBS bucket policy changes, this rule is noncompliant.
alarm-vpc-change	ces, vpc	If there are no alarm rules configured for VPC changes, the current account is noncompliant.
css-cluster-https-required	css	If HTTPS is not enabled for a CSS cluster, this cluster is noncompliant.
css-cluster-in-vpc	css	If a CSS cluster is not in the specified VPCs, this cluster is noncompliant.
cts-kms-encrypted-check	cts	If a CTS tracker is not encrypted using KMS, this tracker is noncompliant.
cts-lts-enable	cts	If a CTS tracker does not have trace transfer to LTS enabled, this tracker is noncompliant.
cts-obs-bucket-track	cts	If no trackers are created for the specified OBS bucket, this rule is noncompliant.
cts-support-validate-check	cts	If **Verify Trace File** is not enabled for a CTS tracker, this tacker is noncompliant.
cts-tracker-exists	cts	If there are no trackers or all trackers are disabled in an account, the current account is noncompliant.
ecs-instance-in-vpc	ecs, vpc	If an ECS is not within the specified VPC, this ECS is noncompliant.

Rule	Cloud Service	Description
ecs-instance-no-public-ip	ecs	If an ECS has an EIP attached, this ECS is noncompliant.
eip-unbound-check	vpc	If an EIP has not been attached to any resource, this EIP is noncompliant.
elb-tls-https-listeners-only	elb	If any listener of a load balancer does not have the frontend protocol set to HTTPS, this load balancer is noncompliant.
iam-group-has-users-check	iam	If an IAM user group has no user, this user group is noncompliant.
iam-password-policy	iam	If the password of an IAM user does not meet the password strength requirements, this IAM user is noncompliant.
iam-root-access-key-check	iam	If the account root user has an available access key, the account is noncompliant.
iam-user-console-and-api-access-at-creation	iam	If an IAM user can access the Huawei Cloud console and has AK/SK that was created when the IAM user was created, this user is noncompliant.
iam-user-group-membership-check	iam	If an IAM user is not in any of the specified IAM user groups, this user is noncompliant.
iam-user-last-login-check	iam	If an IAM user does not log in to the system within the specified time range, the result is non-compliant.

Rule	Cloud Service	Description
iam-user-mfa-enabled	iam	If multi-factor authentication is not enabled for an IAM user, this user is noncompliant.
iam-user-single-access-key	iam	If multiple access keys are in the active state for an IAM user, this user is noncompliant.
mfa-enabled-for-iam-console-access	iam	If an IAM user who is allowed to access Huawei Cloud console does not have MFA enabled, this IAM user is noncompliant.
mrs-cluster-kerberos-enabled	mrs	If kerberos is not enabled for an MRS cluster, this cluster is noncompliant.
mrs-cluster-no-public-ip	mrs	If an MRS cluster has an EIP attached, this cluster is noncompliant.
private-nat-gateway-authorized-vpc-only	nat	If a private NAT gateway is not in a specified VPC, this gateway is noncompliant.
rds-instance-multi-az-support	rds	If an RDS instance does not support multi-AZ deployment, this RDS instance is noncompliant.
rds-instance-no-public-ip	rds	If an RDS instance has an EIP attached, this RDS instance is noncompliant.
root-account-mfa-enabled	iam	If the root user does not have MFA enabled, this root user is noncompliant.
stopped-ecs-date-diff	ecs	If an ECS has been stopped for longer than the time allowed, and no operations have been performed on it, this ECS is noncompliant.

Rule	Cloud Service	Description
volume-unused-check	evs	If an EVS disk is not mounted to any cloud server, this disk is noncompliant.
volumes-encrypted-check	ecs, evs	If a mounted EVS disk is not encrypted, this disk is noncompliant.
vpn-connections-active	vpnaas	If a VPN is not normally connected, this rule is noncompliant.
bms-key-pair-security-login	bms	If a BMS does not have key pair login enabled, ths BMS is noncompliant.
cbr-backup-encrypted-check	cbr	If a CBR backup is not encrypted, this backup is noncompliant.
cfw-policy-not-empty	cfw	If a CFW instance does not have a protection policy attached, this instance is noncompliant.
csms-secrets-auto-rotation-enabled	csms	If a CSMS secret does not have automatic rotation enabled, this secret is noncompliant.
csms-secrets-rotation-success-check	csms	If a CSMS secret fails to be rotated, this secret is noncompliant.
csms-secrets-using-cmk	csms	If a CSMS secret has not been configured with one of the specified KMS keys, this secret is noncompliant.

4.5.5 Conformance Package for Identity and Access Management

The following table lists the rules and solutions included in this conformance package template.

Table 4-9 Conformance package description

Rule	Cloud Service	Description
access-keys-rotated	iam	If an IAM user's access key is not rotated within the specified number of days, this user is noncompliant.
iam-group-has-users-check	iam	If an IAM user group has no user, this user group is noncompliant.
iam-password-policy	iam	If the password of an IAM user does not meet the password strength requirements, this IAM user is noncompliant.
iam-root-access-key-check	iam	If the account root user has an available access key, the account is noncompliant.
iam-user-console-and-api-access-at-creation	iam	If an IAM user can access the Huawei Cloud console and has AK/SK that was created when the IAM user was created, this user is noncompliant.
iam-user-group-membership-check	iam	If an IAM user is not in any of the specified IAM user groups, this user is noncompliant.
iam-user-last-login-check	iam	If an IAM user does not log in to the system within the specified time range, the result is non-compliant.
iam-user-mfa-enabled	iam	If multi-factor authentication is not enabled for an IAM user, this user is noncompliant.
iam-user-single-access-key	iam	If multiple access keys are in the active state for an IAM user, this user is noncompliant.

Rule	Cloud Service	Description
mfa-enabled-for-iam-console-access	iam	If MFA is not enabled for an IAM user who has a console password, this IAM user is noncompliant.
root-account-mfa-enabled	iam	If multi-factor authentication is not enabled for the root user, the root user is noncompliant.
iam-policy-in-use	iam	If an IAM policy has not been attached to any IAM users, user groups, or agencies, this policy is noncompliant.
iam-role-in-use	iam	If an IAM role has not been attached to any IAM users, user groups, or agencies, this role is noncompliant.
iam-user-login-protection-enabled	iam	If login protection is not enabled for an IAM user, this user is noncompliant.
iam-user-no-policies-check	iam	If an IAM user has any policies or permissions directly assigned, the IAM user is noncompliant.
iam-user-check-non-admin-group	iam	If a non-root user was added to the **admin** user group, this user is noncompliant.

4.5.6 Conformance Package for Cloud Eye

The following table lists the rules and solutions included in this conformance package template.

Table 4-10 Conformance package description

Rule	Cloud Service	Description
alarm-action-enabled-check	ces	If an alarm rule is not enabled, this rule is noncompliant.
alarm-kms-disable-or-delete-key	ces, kms	If there are no alarm rules configured for disabling or deleting KMS keys, this rule is noncompliant.
alarm-obs-bucket-policy-change	ces, obs	If there are no alarm rules configured for OBS bucket policy changes, this rule is noncompliant.
alarm-vpc-change	ces, vpc	If there are no alarm rules configured for VPC changes, the current account is noncompliant.

4.5.7 Conformance Package for Compute Services

The following table lists the rules and solutions included in this conformance package template.

Table 4-11 Conformance package description

Rule	Cloud Service	Description
as-capacity-rebalancing	as	If the priority policy EQUILIBRIUM_DISTRIBUTE is not used when an AS group scales in or out, the AS group is non-compliant.
as-group-elb-healthcheck-required	as	If an AS group is not using Elastic Load Balancing health check, this rule is noncompliant.
as-multiple-az	as	If an AS group is deployed in a single AZ, this AS group is noncompliant.

Rule	Cloud Service	Description
ecs-instance-key-pair-login	ecs	If key pair authentication is not required for ECS logging, this ECS is noncompliant.
ecs-instance-no-public-ip	ecs	If an ECS has an EIP attached, this ECS is noncompliant.
ecs-multiple-public-ip-check	ecs	If an ECS has multiple EIPs attached, this ECS is noncompliant.
eip-bandwidth-limit	eip	An EIP is non-compliant if its bandwidth is smaller than a specified bandwidth.
function-graph-concurrency-check	fgs	If the number of concurrent requests of a FunctionGraph function is not within the specified range, this function is noncompliant.
function-graph-public-access-prohibited	fgs	If a function can be accessed over a public network, this function is noncompliant.
stopped-ecs-date-diff	ecs	If an ECS has been stopped for longer than the time allowed, and no operations have been performed on it, this ECS is noncompliant.
volume-unused-check	evs	If an EVS disk is not mounted to any cloud server, this disk is noncompliant.
volumes-encrypted-check	ecs, evs	If a mounted EVS disk is not encrypted, this disk is noncompliant.
as-group-ipv6-disabled	as	If an AS group has an IPv6 shared bandwidth attached, this AS group is noncompliant

4.5.8 Conformance Package for ECS

The following table lists the rules and solutions included in this conformance package template.

Table 4-12 Conformance package description

Rule	Cloud Service	Description
ecs-instance-key-pair-login	ecs	If key pair authentication is not required for ECS logging, this ECS is noncompliant.
ecs-instance-no-public-ip	ecs	If an ECS has an EIP attached, this ECS is noncompliant.
ecs-multiple-public-ip-check	ecs	If an ECS has multiple EIPs attached, this ECS is noncompliant.
stopped-ecs-date-diff	ecs	If an ECS has been stopped for longer than the time allowed, and no operations have been performed on it, this ECS is noncompliant.
volumes-encrypted-check	ecs, evs	If a mounted EVS disk is not encrypted, this disk is noncompliant.
ecs-attached-hss-agents-check	ecs	If an ECS does not have an HSS agent installed or the protection mode enabled, this ECS is noncompliant.
ecs-instance-agency-attach-iam-agency	ecs	If an ECS does not have any IAM agencies attached, this ECS is noncompliant.
ecs-last-backup-created	cbr, ecs	If an ECS does not have a backup created within the specified period, this ECS is noncompliant.

4.5.9 Conformance Package for ELB

The following table lists the rules and solutions included in this conformance package template.

Table 4-13 Conformance package description

Rule	Cloud Service	Description
elb-loadbalancers-no-public-ip	elb	If a load balancer has an EIP attached, this load balancer is noncompliant.
elb-predefined-security-policy-https-check	elb	If a specified security policy is not configured for the HTTPS listener of a dedicated load balancer, this dedicated load balancer is noncompliant.
elb-tls-https-listeners-only	elb	If any listener of a load balancer does not have the frontend protocol set to HTTPS, this load balancer is noncompliant.
elb-http-to-https-redirection-check	elb	If an HTTP listener does not have redirecting requests to an HTTPS listener enabled, this HTTP listener is noncompliant.
elb-multiple-az-check	elb	If a load balancer is mapped to only one availability zone (AZ), this load balancer is noncompliant. If a load balancer is mapped to fewer than two AZs, this load balancer is noncompliant.

4.5.10 Conformance Package for Management and Regulatory Services

The following table lists the rules and solutions included in this conformance package template.

Table 4-14 Conformance package description

Rule	Cloud Service	Description
alarm-action-enabled-check	ces	If an alarm rule is not enabled, this rule is noncompliant.
alarm-kms-disable-or-delete-key	ces, kms	If there are no alarm rules configured for disabling or deleting KMS keys, this rule is noncompliant.
alarm-obs-bucket-policy-change	ces, obs	If there are no alarm rules configured for OBS bucket policy changes, this rule is noncompliant.
alarm-vpc-change	ces, vpc	If there are no alarm rules configured for VPC changes, the current account is noncompliant.
cts-kms-encrypted-check	cts	If a CTS tracker is not encrypted using KMS, this tracker is noncompliant.
cts-lts-enable	cts	If **Transfer to LTS** is not enabled for a CTS tracker, this tracker is noncompliant.
cts-support-validate-check	cts	If **Verify Trace File** is not enabled for a CTS tracker, this tacker is noncompliant.
cts-tracker-exists	cts	If there is no CTS tracker in the current account, this rule is noncompliant.
tracker-config-enabled-check	config	If the resource recorder is not enabled, this rule is noncompliant.

4.5.11 Conformance Package for RDS

The following table lists the rules and solutions included in this conformance package template.

Table 4-15 Conformance package description

Rule	Cloud Service	Description
rds-instance-enable-backup	rds	If backup is not enabled for an RDS instance, this instance is noncompliant.
rds-instance-enable-errorLog	rds	If error log collection is not enabled for an RDS instance, this instance is noncompliant.
rds-instance-enable-slowLog	rds	If an RDS instance does not support slow query logs, this instance is noncompliant.
rds-instance-multi-az-support	rds	If an RDS instance does not support multi-AZ deployment, this RDS instance is noncompliant.
rds-instance-no-public-ip	rds	If an RDS instance has an EIP attached, this RDS instance is noncompliant.
rds-instances-enable-kms	rds	If KMS encryption is not enabled for an RDS instance, this instance is noncompliant.
rds-instance-enable-auditLog	rds	If an RDS instance does not have the audit log enabled or has audit logs kept for less than the specified number of days, this instance is noncompliant.
rds-instance-engine-version-check	rds	If the version of an RDS instance engine is earlier than the specified version, this instance is noncompliant.
rds-instance-port-check	rds	If an RDS instance has unallowed ports enabled, this instance is noncompliant.

Rule	Cloud Service	Description
rds-instance-ssl-enable	rds	If SSL is not enabled for an RDS instance, this instance is noncompliant.

4.5.12 Conformance Package for AS

The following table lists the rules and solutions included in this conformance package template.

Table 4-16 Conformance package description

Rule	Cloud Service	Description
as-capacity-rebalancing	as	If the priority policy EQUILIBRIUM_DISTRIBUTE is not used when an AS group scales in or out, the AS group is non-compliant.
as-group-elb-healthcheck-required	as	If an AS group is not using Elastic Load Balancing health check, this rule is noncompliant.
as-multiple-az	as	If an AS group is deployed in a single AZ, this AS group is noncompliant.
as-group-ipv6-disabled	as	If an AS group has an IPv6 shared bandwidth attached, this AS group is noncompliant

4.5.13 Conformance Package for CTS

The following table lists the rules and solutions included in this conformance package template.

Table 4-17 Conformance package description

Rule	Cloud Service	Description
cts-kms-encrypted-check	cts	If a CTS tracker is not encrypted using KMS, this tracker is noncompliant.
cts-lts-enable	cts	If **Transfer to LTS** is not enabled for a CTS tracker, this tracker is noncompliant.
cts-support-validate-check	cts	If **Verify Trace File** is not enabled for a CTS tracker, this tacker is noncompliant.
cts-tracker-exists	cts	If there is no CTS tracker in the current account, this rule is noncompliant.

4.5.14 Conformance Package for AI and Machine Learning

The following table lists the rules and solutions included in this conformance package template.

Table 4-18 Conformance package description

Rule	Cloud Service	Description
cce-cluster-end-of-maintenance-version	cce	If the version of a CCE cluster is no longer supported for maintenance, this cluster is noncompliant.
cce-cluster-oldest-supported-version	cce	If a CCE cluster is running the oldest supported version, this cluster is noncompliant.
cce-endpoint-public-access	cce	If a CCE cluster has an EIP attached, this CCE cluster is noncompliant.
cts-obs-bucket-track	cts	If no trackers are created for the specified OBS bucket, this rule is noncompliant.

Rule	Cloud Service	Description
mrs-cluster-kerberos-enabled	mrs	If kerberos is not enabled for an MRS cluster, this cluster is noncompliant.
mrs-cluster-no-public-ip	mrs	If an MRS cluster has an EIP attached, this cluster is noncompliant.
sfsturbo-encrypted-check	sfsturbo	If KMS encryption is not enabled for an SFS Turbo file system, this file system is noncompliant.

4.5.15 Conformance Package for Autopilot

The following table lists the rules and solutions included in this conformance package template.

Table 4-19 Conformance package description

Rule	Cloud Service	Description
css-cluster-disk-encryption-check	css	If disk encryption is not enabled for a CSS cluster, this cluster is noncompliant.
css-cluster-https-required	css	If HTTPS is not enabled for a CSS cluster, this cluster is noncompliant.
css-cluster-no-public-zone	css	If a CSS cluster can be accessed over a public network, this cluster is noncompliant.
css-cluster-security-mode-enable	css	If a CSS cluster does not support the security mode, this cluster is noncompliant.
cts-kms-encrypted-check	cts	If a CTS tracker is not encrypted using KMS, this tracker is noncompliant.
cts-obs-bucket-track	cts	If no CTS trackers are created for the specified OBS bucket, this rule is noncompliant.

Rule	Cloud Service	Description
cts-support-validate-check	cts	If **Verify Trace File** is not enabled for a CTS tracker, this tacker is noncompliant.
cts-tracker-exists	cts	If there are no CTS trackers in an account, this account is noncompliant.
dcs-redis-no-public-ip	dcs	If a DCS Redis instance has an EIP associated, this instance is noncompliant.
dcs-redis-password-access	dcs	If a DCS Redis instance can be accessed without a password, this instance is noncompliant.
ecs-instance-no-public-ip	ecs	If an ECS has an EIP attached, this ECS is noncompliant.
elb-loadbalancers-no-public-ip	elb	If a load balancer has an EIP attached, this load balancer is noncompliant.
elb-tls-https-listeners-only	elb	If any listener of a load balancer does not have the frontend protocol set to HTTPS, this load balancer is noncompliant.
iam-password-policy	iam	If the password of an IAM user does not meet the password strength requirements, this IAM user is noncompliant.
iam-user-last-login-check	iam	If an IAM user does not log in to the system within the specified time range, the result is non-compliant.
iam-user-mfa-enabled	iam	If multi-factor authentication is not enabled for an IAM user, this user is noncompliant.

Rule	Cloud Service	Description
rds-instance-no-public-ip	rds	If an RDS instance has an EIP attached, this RDS instance is noncompliant.
root-account-mfa-enabled	iam	If multi-factor authentication is not enabled for the root user, the root user is noncompliant.
volumes-encrypted-check	ecs, evs	If a mounted EVS disk is not encrypted, this disk is noncompliant.
vpc-flow-logs-enabled	vpc	If there is a flow log that has not been enabled for a VPC, this VPC is noncompliant.
vpc-sg-ports-check	vpc	If a security group allows all inbound traffic (with the source address set to **0.0.0.0/0**) and opens all TCP/UDP ports, this security group is noncompliant.

4.5.16 Conformance Package for Enabling Public Access

The following table lists the rules and solutions included in this conformance package template.

Table 4-20 Conformance package description

Rule Identifier	Cloud Service	Description
css-cluster-in-vpc	css	If a CSS cluster is not in the specified VPC, this cluster is noncompliant.
drs-data-guard-job-not-public	drs	If the network type of a DR task is set to public network, this DR task is noncompliant.

Rule Identifier	Cloud Service	Description
drs-migration-job-not-public	drs	If the network type of a migration task is set to public network, this migration task is noncompliant.
drs-synchronization-job-not-public	drs	If the network type of a synchronization task is not set to public network, this task is noncompliant.
ecs-instance-in-vpc	ecs, vpc	If an ECS is not within the specified VPC, this ECS is noncompliant.
ecs-instance-no-public-ip	ecs	If an ECS has an EIP attached, this ECS is noncompliant.
function-graph-inside-vpc	fgs	If a function is not in the specified VPC, this function is noncompliant.
function-graph-public-access-prohibited	fgs	If a function can be accessed over a public network, this function is noncompliant.
mrs-cluster-no-public-ip	mrs	If an MRS cluster has an EIP attached, this cluster is noncompliant.
rds-instance-no-public-ip	rds	If an RDS instance has an EIP attached, this RDS instance is noncompliant.

4.5.17 Conformance Package for Logging and Monitoring

The following table lists the rules and solutions included in this conformance package template.

Table 4-21 Conformance package description

Rule Identifier	Cloud Service	Description
alarm-action-enabled-check	ces	If an alarm rule is not enabled, this rule is noncompliant.

Rule Identifier	Cloud Service	Description
apig-instances-execution-logging-enabled	apig	If logging is not enabled for a dedicated APIG gateway, this gateway is considered non-compliant.
as-group-elb-healthcheck-required	as	If an AS group is not using Elastic Load Balancing health check, this rule is noncompliant.
cts-kms-encrypted-check	cts	If a CTS tracker is not encrypted using KMS, this tracker is noncompliant.
cts-lts-enable	cts	If **Transfer to LTS** is not enabled for a CTS tracker, this tracker is noncompliant.
cts-obs-bucket-track	cts	If no CTS trackers are created for the specified OBS bucket, this rule is noncompliant.
cts-support-validate-check	cts	If **Verify Trace File** is not enabled for a CTS tracker, this tacker is noncompliant.
cts-tracker-exists	cts	If there are no CTS trackers in an account, this account is noncompliant.
dws-enable-log-dump	dws	If a DWS cluster does not have log transfer enabled, this cluster is noncompliant.
function-graph-concurrency-check	fgs	If the number of concurrent requests of a FunctionGraph function is not within the specified range, this function is noncompliant.
multi-region-cts-tracker-exists	cts	If there are no CTS trackers in any of the specified regions, this rule is noncompliant.

Rule Identifier	Cloud Service	Description
rds-instance-logging-enabled	rds	If an RDS instance does not have the collection of any types of logs enabled, this instance is noncompliant.
vpc-flow-logs-enabled	vpc	If there is a flow log that has not been enabled for a VPC, this VPC is noncompliant.

4.5.18 Conformance Package for Architecture Reliability

The following table lists the rules and solutions included in this conformance package template.

Table 4-22 Conformance package description

Rule Identifier	Cloud Service	Description
apig-instances-execution-logging-enabled	apig	If logging is not enabled for a dedicated APIG gateway, this gateway is considered non-compliant.
as-group-elb-healthcheck-required	as	If an AS group is not using Elastic Load Balancing health check, this rule is noncompliant.
cts-lts-enable	cts	If **Transfer to LTS** is not enabled for a CTS tracker, this tracker is noncompliant.
cts-obs-bucket-track	cts	If no CTS trackers are created for the specified OBS bucket, this rule is noncompliant.
cts-tracker-exists	cts	If there are no CTS trackers in an account, this account is noncompliant.
dws-enable-kms	dws	If KMS encryption is not enabled for a DWS cluster, this cluster is noncompliant.

Rule Identifier	Cloud Service	Description
ecs-instance-in-vpc	ecs, vpc	If an ECS is not within the specified VPC, this ECS is noncompliant.
function-graph-concurrency-check	fgs	If the number of concurrent requests of a FunctionGraph function is not within the specified range, this function is noncompliant.
gaussdb-nosql-enable-disk-encryption	gaussdb nosql	If a GeminiDB instance does not have disk encryption enabled, this instance is noncompliant.
kms-not-scheduled-for-deletion	kms	If a KMS key is scheduled for deletion, this key is noncompliant.
multi-region-cts-tracker-exists	cts	If there are no trackers in any of the specified regions, this rule is noncompliant.
rds-instance-enable-backup	rds	If backup is not enabled for an RDS instance, this instance is noncompliant.
rds-instance-multi-az-support	rds	If an RDS instance does not support multi-AZ deployment, this RDS instance is noncompliant.
rds-instances-enable-kms	rds	If KMS encryption is not enabled for an RDS instance, this instance is noncompliant.
sfsturbo-encrypted-check	sfsturbo	If KMS encryption is not enabled for an SFS Turbo file system, this file system is noncompliant.
volumes-encrypted-check	ecs, evs	If a mounted EVS disk is not encrypted, this disk is noncompliant.

Rule Identifier	Cloud Service	Description
vpc-flow-logs-enabled	vpc	If there is a flow log that has not been enabled for a VPC, this VPC is noncompliant.
vpn-connections-active	vpnaas	Ensure normal VPN connections.

4.5.19 Conformance Package for Hong Kong Monetary Authority of China Requirements

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

Background

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

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 numbers in the following table are in consistent with the chapter numbers in **HKMA.2022.08.31**.

Table 4-23 The conformance package for 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.
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.

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.	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 numbers in the following table are in consistent with the chapter numbers in **SA-2**.

Table 4-24 Rules for SA-2

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.

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.	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.
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	Use 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

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.	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 4-25 Rules for OR-2

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.

Guideline No.	Guideline Description	Rule	Solution
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.
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 4-26 Rules for TM-G-1

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.
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.

Guideline No.	Guideline Description	Rule	Solution
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.
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.

4.5.20 Conformance Package for ENISA Requirements

This section describes the background, applicable scenarios, and the conformance 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.

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 numbers in the following table are in consistent with the chapter numbers in *cybersecurity-guide-for-smes*.

Table 4-27 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 Regulation 1 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.

Guideline No.	Guideline Description	Rule	Solution
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation 1 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.
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation 1 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.

Guideline No.	Guideline Description	Rule	Solution
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation 1 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.
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation 1 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, so access control is required.

Guideline No.	Guideline Description	Rule	Solution
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation 1 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.
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation 1 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.

Guideline No.	Guideline Description	Rule	Solution
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation 1 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.
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation 1 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 with KMS for CTS trackers.

Guideline No.	Guideline Description	Rule	Solution
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation 1 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.
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation 1 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 Regulation 1 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	You can enable file verification for CTS trackers to prevent log files from being modified or deleted after being stored.
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation 1 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 Regulation 1 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 Regulation 1 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.

Guideline No.	Guideline Description	Rule	Solution
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation 1 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 Regulation 1 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

Guideline No.	Guideline Description	Rule	Solution
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation 1 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
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation 1 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	You can configure security groups to only allow traffic from some IPs to access the SSH port 22 of ECSs to ensure secure remote access to ECSs.

Guideline No.	Guideline Description	Rule	Solution
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation 1 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.
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation 1 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.

Guideline No.	Guideline Description	Rule	Solution
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation 1 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.
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation 1 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.

Guideline No.	Guideline Description	Rule	Solution
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation 1 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 GeminiDB instances.
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	Under the EU General Data Protection Regulation 1 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	You can use security groups to control port connections.

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.	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.
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.

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.	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 Wi-Fi 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 with KMS 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 Wi-Fi 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	You can 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 Wi-Fi 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 Wi-Fi 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 Wi-Fi 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 Wi-Fi 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	HTTPS enables encrypted communication with clusters. If HTTPS is disabled, HTTP is used. This compromises data security, and public access cannot be enabled.

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 Wi-Fi 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 Wi-Fi 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 Wi-Fi 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 Wi-Fi 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 disk encryption with KMS for GeminiDB 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 Wi-Fi 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 Wi-Fi 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 Wi-Fi 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	You can configure security groups to only allow traffic from some IPs to access the SSH port 22 of ECSs to ensure secure remote access to ECSs.

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 SME 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	You can configure security groups to control connections to frequently used ports.
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	You can use security groups to control port connections.

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. - Restrict remote access from suspicious geographical locations or certain IP addresses. - Restrict staff remote access only to the systems and computers they need for their work. - Enforce strong passwords for remote access and where possible enable multi-factor authentication. - 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. - Restrict remote access from suspicious geographical locations or certain IP addresses. - Restrict staff remote access only to the systems and computers they need for their work. - Enforce strong passwords for remote access and where possible enable multi-factor authentication. - 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. - Restrict remote access from suspicious geographical locations or certain IP addresses. - Restrict staff remote access only to the systems and computers they need for their work. - Enforce strong passwords for remote access and where possible enable multi-factor authentication. - 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. - Restrict remote access from suspicious geographical locations or certain IP addresses. - Restrict staff remote access only to the systems and computers they need for their work. - Enforce strong passwords for remote access and where possible enable multi-factor authentication. - 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 APIG 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. - 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. - Enforce strong passwords for remote access and where possible enable multi-factor authentication. - 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. - Restrict remote access from suspicious geographical locations or certain IP addresses. - Restrict staff remote access only to the systems and computers they need for their work. - Enforce strong passwords for remote access and where possible enable multi-factor authentication. - 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. - Restrict remote access from suspicious geographical locations or certain IP addresses. - Restrict staff remote access only to the systems and computers they need for their work. - Enforce strong passwords for remote access and where possible enable multi-factor authentication. - 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 GeminiDB.

4.5.21 Conformance Package for SWIFT CSP

This section describes the background, applicable scenarios, and the conformance 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 4-28 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	You can use security groups to control port connections.
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	You can configure security groups to only allow traffic from some IPs to access the SSH port 22 of ECSs to ensure secure remote access to ECSs.
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	You can configure security groups to control connections to frequently used ports.

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	You can use this rule to identify ECSs that have multiple EIPs attached to reduce network 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.
2.5 A	sfsturbo-encrypted-check	Enable KMS encryption for SFS Turbo file systems.
2.5 A	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, **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	You can 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.

4.5.22 Conformance Package for Germany Cloud Computing Compliance Criteria Catalogue

This section describes the background, applicable scenarios, and the conformance 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 conformance 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 4-29 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	You can configure security groups to control connections to frequently used ports.
COS-03	vpc-sg-restricted-ssh	You can configure security groups to only allow traffic from some IPs to access the SSH port 22 of ECSs to ensure secure remote access to ECSs.
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	You can use security groups to control port connections.
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 RDS instances from public networks to protect sensitive data.
COS-05	vpc-sg-restricted-common-ports	You can configure security groups to control connections to frequently used ports.
COS-05	vpc-sg-restricted-ssh	You can configure security groups to only allow traffic from some IPs to access the SSH port 22 of ECSs to ensure secure remote access to ECSs.
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	You can use security groups to control port connections.
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	HTTPS enables encrypted communication with clusters. If HTTPS is disabled, HTTP is used. This compromises data security, and public access cannot be enabled.
CRY-02	css-cluster-disk-encryption-check	Enable disk encryption for CSS clusters to protect sensitive data.

Guideline No.	Rule	Solution
CRY-02	elb-tls-https-listeners-only	Ensure that your load balancer listeners are configured with the HTTPS protocol.
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, **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.

Guideline No.	Rule	Solution
IDM-01	iam-password-policy	Set thresholds for IAM user password strength.
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.

Guideline No.	Rule	Solution
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.
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 GeminiDB.
OPS-14	cts-support-validate-check	You can 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.

Guideline No.	Rule	Solution
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.
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, **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, **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.

4.5.23 Conformance Package for PCI DSS

This section describes the background, applicable scenarios, and the conformance 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 **Payment Card Industry (PCI) Data Security Standard**.

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 **Payment Card Industry (PCI) Data Security Standard**.

Table 4-30 Rules in the conformance package

Guideline No.	Guideline Description	Rule	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.

Guideline No.	Guideline Description	Rule	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.	drs-data-guard-job-not-public	Block public access to DRS real-time DR tasks.
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.

Guideline No.	Guideline Description	Rule	Solution
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.
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	You can use security groups to control port connections.
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	vpc-sg-restricted-common-ports	You can configure security groups to control connections to frequently used ports.

Guideline No.	Guideline Description	Rule	Solution
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	vpc-sg-restricted-ssh	You can configure security groups to only allow traffic from some IPs to access the SSH port 22 of ECSs to ensure secure remote access to ECSs.
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.

Guideline No.	Guideline Description	Rule	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.	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
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	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	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	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	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	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	You can enable file verification for CTS trackers to prevent log files from being modified or deleted after being stored.

Guideline No.	Guideline Description	Rule	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	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	You can use this rule to identify ECSs that have multiple EIPs attached to reduce network security risks.

Guideline No.	Guideline Description	Rule	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	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.

Guideline No.	Guideline Description	Rule	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-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	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	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	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, **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	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	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 all EVS disks to protect data.

Guideline No.	Guideline Description	Rule	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	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	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	You can configure security groups to control connections to frequently used ports.

Guideline No.	Guideline Description	Rule	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	You can configure security groups to restrict connections to SSH port 23.
2.3	Encrypt all non-console administrative access using strong cryptography.	apig-instances-ssl-enabled	Enable SSL for APIG REST APIs to authenticate API Gateway requests.
2.3	Encrypt all non-console administrative access using strong cryptography.	css-cluster-https-required	HTTPS enables encrypted communication with clusters. If HTTPS is disabled, HTTP is used. This compromises data security, and public access cannot be enabled.
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	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	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	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	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	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	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	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	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	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	HTTPS enables encrypted communication with clusters. If HTTPS is disabled, HTTP is used. This compromises data security, and public access cannot be enabled.

Guideline No.	Guideline Description	Rule	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	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	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	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	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 APIG 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
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, **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	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	You can enable file verification for CTS trackers to prevent log files from being modified or deleted after being stored.
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	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	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	You can use security groups to control port connections.

Guideline No.	Guideline Description	Rule	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	You can configure security groups to control connections to frequently used ports.
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	You can 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	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	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	You can use security groups to control port connections.

Guideline No.	Guideline Description	Rule	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	You can configure security groups to control connections to frequently used ports.
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.
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.

Guideline No.	Guideline Description	Rule	Solution
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	You can use security groups to control port connections.
1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.	vpc-sg-restricted-common-ports	You can configure security groups to control connections to frequently used ports.
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.

Guideline No.	Guideline Description	Rule	Solution
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.
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.

Guideline No.	Guideline Description	Rule	Solution
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	You can use security groups to control port connections.
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.

Guideline No.	Guideline Description	Rule	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.	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.
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.

Guideline No.	Guideline Description	Rule	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.	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.
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	You can use security groups to control port connections.

Guideline No.	Guideline Description	Rule	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-restricted-common-ports	You can configure security groups to control connections to frequently used 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-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 APIG 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.
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.

Guideline No.	Guideline Description	Rule	Solution
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, **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.
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, **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	Solution
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.
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, **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.

Guideline No.	Guideline Description	Rule	Solution
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.
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, **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	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.	cts-tracker-exists	Ensure that a CTS tracker has been created for your account to record operations on the Huawei Cloud console.
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, **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.

Guideline No.	Guideline Description	Rule	Solution
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, **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.
10.2.7	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.

Guideline No.	Guideline Description	Rule	Solution
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, **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.
10.3.1	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.

Guideline No.	Guideline Description	Rule	Solution
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, **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.
10.3.1	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	You can enable file verification for CTS trackers to prevent log files from being modified or deleted after being stored.

Guideline No.	Guideline Description	Rule	Solution
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.
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.

Guideline No.	Guideline Description	Rule	Solution
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.
2.2.2	Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	vpc-sg-ports-check	You can use security groups to control port connections.
2.2.2	Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	vpc-sg-restricted-common-ports	You can configure security groups to control connections to frequently used ports.
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.

Guideline No.	Guideline Description	Rule	Solution
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.
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.

Guideline No.	Guideline Description	Rule	Solution
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.
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.

Guideline No.	Guideline Description	Rule	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-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.
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.

Guideline No.	Guideline Description	Rule	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-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.
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.

Guideline No.	Guideline Description	Rule	Solution
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.
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.

Guideline No.	Guideline Description	Rule	Solution
7.2.1	Establish an access control system 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.
7.2.1	Establish an access control system 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 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	Solution
7.2.1	Establish an access control system 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.
7.2.1	Establish an access control system 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 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	Solution
7.2.1	Establish an access control system 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.
7.2.2	Establish an access control system 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 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.

Guideline No.	Guideline Description	Rule	Solution
7.2.2	Establish an access control system 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.
7.2.2	Establish an access control system 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 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.

Guideline No.	Guideline Description	Rule	Solution
7.2.2	Establish an access control system 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.
7.2.2	Establish an access control system 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.

Guideline No.	Guideline Description	Rule	Solution
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.
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 encryption 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.

Guideline No.	Guideline Description	Rule	Solution
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.
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.

Guideline No.	Guideline Description	Rule	Solution
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 management 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.
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 management 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.

4.5.24 Conformance Package for Healthcare Industry

The following table describes the compliance rules and solutions in the sample template.

Table 4-31 Conformance package description

Rule Identifier	Cloud Service	Description
apig-instances-execution-logging-enabled	apig	If logging is not enabled for a dedicated APIG gateway, this gateway is considered non-compliant.
apig-instances-ssl-enabled	apig	If no SSL certificates are attached to a dedicated APIG gateway, this gateway is considered noncompliant.
as-group-elb-healthcheck-required	as	If an AS group is not using Elastic Load Balancing health check, this rule is noncompliant.
css-cluster-disk-encryption-check	css	If disk encryption is not enabled for a CSS cluster, this cluster is noncompliant.
css-cluster-https-required	css	If HTTPS is not enabled for a CSS cluster, this cluster is noncompliant.
css-cluster-in-vpc	css	If a CSS cluster is not in the specified VPCs, this cluster is noncompliant.
cts-kms-encrypted-check	cts	If a CTS tracker is not encrypted using KMS, this tracker is noncompliant.
cts-lts-enable	cts	If **Transfer to LTS** is not enabled for a CTS tracker, this tracker is noncompliant.
cts-obs-bucket-track	cts	If no CTS trackers are created for the specified OBS bucket, this rule is noncompliant.

Rule Identifier	Cloud Service	Description
cts-support-validate-check	cts	If **Verify Trace File** is not enabled for a CTS tracker, this tacker is noncompliant.
cts-tracker-exists	cts	If there is no tracker in the current account, this rule is noncompliant
drs-data-guard-job-not-public	drs	If the network type of a DR task is set to public network, this DR task is noncompliant.
drs-migration-job-not-public	drs	If the network type of a migration task is set to public network, this migration task is noncompliant.
drs-synchronization-job-not-public	drs	If the network type of a synchronization task is not set to public network, this task is noncompliant.
dws-enable-log-dump	dws	If a DWS cluster does not have log transfer enabled, this cluster is noncompliant.
dws-enable-snapshot	dws	If automated snapshots are not enabled for a DWS cluster, this cluster is noncompliant.
dws-enable-ssl	dws	If SSL is not enabled for a DWS cluster, this cluster is noncompliant.
ecs-instance-in-vpc	ecs, vpc	If an ECS is not within the specified VPC, this ECS is noncompliant.
ecs-instance-no-public-ip	ecs	If an ECS has an EIP attached, this ECS is noncompliant.
eip-unbound-check	vpc	If an EIP has not been attached to any resource, this EIP is noncompliant.

Rule Identifier	Cloud Service	Description
eip-use-in-specified-days	eip	If an EIP is not used within the specified number of days after being created, the EIP is noncompliant.
elb-predefined-security-policy-https-check	elb	If a specified security policy is not configured for the HTTPS listener of a dedicated load balancer, this dedicated load balancer is noncompliant.
elb-tls-https-listeners-only	elb	If any listener of a load balancer does not have the frontend protocol set to HTTPS, this load balancer is noncompliant.
function-graph-public-access-prohibited	fgs	If a function can be accessed over a public network, this function is noncompliant.
gaussdb-nosql-enable-backup	gaussdb nosql	If the backup is not enabled for a GeminiDB instance, this instance is noncompliant.
gaussdb-nosql-enable-disk-encryption	gaussdb nosql	If **Disk Encryption** is disabled for a GeminiDB instance, this instance is noncompliant.
iam-customer-policy-blocked-kms-actions	iam	If there is a blocked action for KMS in an IAM policy, this policy is noncompliant.
iam-password-policy	iam	If the password of an IAM user does not meet the password strength requirements, this IAM user is noncompliant.
iam-policy-no-statements-with-admin-access	iam	If an IAM policy grants administrator permissions (with the **Action** element set to ***:*:***, ***:***, or *****), this policy is noncompliant.

Rule Identifier	Cloud Service	Description
iam-role-has-all-permissions	iam	If an IAM custom policy contains ***:*** in the **allow** section, this policy is noncompliant.
iam-root-access-key-check	iam	If the account root user has an available access key, the account is noncompliant.
iam-user-last-login-check	iam	If an IAM user does not log in to the system within the specified time range, this user is non-compliant.
iam-user-mfa-enabled	iam	If multi-factor authentication is not enabled for an IAM user, this user is noncompliant.
kms-not-scheduled-for-deletion	kms	If a KMS key is scheduled for deletion, this key is noncompliant.
mfa-enabled-for-iam-console-access	iam	If MFA is not enabled for an IAM user who has a console password, this IAM user is noncompliant.
mrs-cluster-kerberos-enabled	mrs	If kerberos is not enabled for an MRS cluster, this cluster is noncompliant.
mrs-cluster-no-public-ip	mrs	If an MRS cluster has an EIP attached, this cluster is noncompliant.
multi-region-cts-tracker-exists	cts	If there are no CTS trackers in any of the specified regions, this rule is noncompliant.
pca-certificate-authority-expiration-check	pca	If the validity period of a private CA is not within the specified period, this CA is noncompliant.

Rule Identifier	Cloud Service	Description
pca-certificate-expiration-check	pca	If the validity period of a certificate is not within the specified range, this certificate is noncompliant.
private-nat-gateway-authorized-vpc-only	nat	If a private NAT gateway is not in a specified VPC, this gateway is noncompliant.
rds-instance-enable-backup	rds	If backup is not enabled for an RDS instance, this instance is noncompliant.
rds-instance-multi-az-support	rds	If an RDS instance does not support multi-AZ deployment, this RDS instance is noncompliant.
rds-instance-no-public-ip	rds	If an RDS instance has an EIP attached, this RDS instance is noncompliant.
rds-instances-enable-kms	rds	If KMS encryption is not enabled for an RDS instance, this instance is noncompliant.
root-account-mfa-enabled	iam	If multi-factor authentication is not enabled for the root user, the root user is noncompliant.
sfsturbo-encrypted-check	sfsturbo	If KMS encryption is not enabled for an SFS Turbo file system, this file system is noncompliant.
stopped-ecs-date-diff	ecs	If an ECS has been stopped for longer than the time allowed, and no operations have been performed on it, this ECS is noncompliant.
volumes-encrypted-check	ecs, evs	If a mounted EVS disk is not encrypted, this disk is noncompliant.

Rule Identifier	Cloud Service	Description
vpc-acl-unused-check	vpc	If a network ACL is not attached to any subnets, this ACL is noncompliant.
vpc-default-sg-closed	vpc	If a default security group allows all inbound or outbound traffic, this security group is noncompliant.
vpc-flow-logs-enabled	vpc	If there is a flow log that has not been enabled for a VPC, this VPC is noncompliant.
vpc-sg-ports-check	vpc	If a security group allows all inbound traffic (with the source address set to **0.0.0.0/0**) and opens all TCP/UDP ports, this security group is noncompliant.
vpc-sg-restricted-common-ports	vpc	If a security group allows all IPv4 addresses (0.0.0.0/0) to access a specified port, this security group is noncompliant.
vpc-sg-restricted-ssh	vpc	If the source address is set to **0.0.0.0/0** and the TCP port 22 is opened, this security group is non-compliant.
vpn-connections-active	vpnaas	If a VPN is not normally connected, this rule is noncompliant.

4.5.25 Best Practices of Network and Data Security

This section describes the best practices of network and data security, their applicable scenarios, and default rules in the conformance package.

Applicable Scenario

This conformance package helps you evaluate network and data security to protect your information assets from network attacks and data leakage.

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 numbers in the following table are in consistent with the chapter numbers in **CIS Control Version 8**.

Table 4-32 Rules for network and data security best practices

Guideline No.	Rule	Cloud Service	Description
1.1	ecs-in-allowed-security-groups	ecs	If an ECS does not have any of the specified security groups attached, this ECS is noncompliant.
1.1	eip-unbound-check	vpc	If an EIP has not been attached to any resource, this EIP is noncompliant.
1.1	eip-use-in-specified-days	eip	If an EIP is not used within the specified number of days after being created, the EIP is noncompliant.
1.1	stopped-ecs-date-diff	ecs	If an ECS has been stopped for longer than the time allowed, and no operations have been performed on it, this ECS is noncompliant.
1.1	vpc-acl-unused-check	vpc	If a network ACL is not attached to any subnets, this ACL is noncompliant.
2.2	cce-cluster-oldest-supported-version	cce	If a CCE cluster is running the oldest supported version, this cluster is noncompliant.
3.3	css-cluster-in-vpc	css	If a CSS cluster is not in the specified VPCs, this cluster is noncompliant.
3.3	drs-data-guard-job-not-public	drs	If the network type of a DR task is set to public network, this DR task is noncompliant.

Guideline No.	Rule	Cloud Service	Description
3.3	drs-migration-job-not-public	drs	If the network type of a migration task is set to public network, this migration task is noncompliant.
3.3	drs-synchronization-job-not-public	drs	If the network type of a synchronization task is not set to public network, this task is noncompliant.
3.3	ecs-instance-in-vpc	ecs, vpc	If an ECS is not within the specified VPC, this ECS is noncompliant.
3.3	ecs-instance-no-public-ip	ecs	If an ECS has an EIP attached, this ECS is noncompliant.
3.3	function-graph-inside-vpc	fgs	If a function is not in the specified VPC, this function is noncompliant.
3.3	function-graph-public-access-prohibited	fgs	If a function can be accessed over a public network, this function is noncompliant.
3.3	iam-customer-policy-blocked-kms-actions	obs, access-analyzer-verified	If an IAM policy allows any blocked actions on KMS keys, this policy is noncompliant.
3.3	iam-group-has-users-check	iam	If an IAM user group has no user, this user group is noncompliant.
3.3	iam-policy-no-statements-with-admin-access	iam	If an IAM policy grants administrator permissions (with the **Action** element set to ***:*:***, ***:***, or *****), this policy is noncompliant.
3.3	iam-role-has-all-permissions	iam	If a custom policy or role allows all actions for a cloud service, this policy or role is noncompliant
3.3	iam-root-access-key-check	iam	If the root user access key is available, this rule is noncompliant.
3.3	iam-user-group-membership-check	iam	If an IAM user is not in any of the specified IAM user groups, this user is noncompliant.

Guideline No.	Rule	Cloud Service	Description
3.3	iam-user-last-login-check	iam	If an IAM user does not log in to the system within the specified time range, this user is non-compliant.
3.3	mrs-cluster-kerberos-enabled	mrs	If kerberos is not enabled for an MRS cluster, this cluster is noncompliant.
3.3	mrs-cluster-no-public-ip	mrs	If an MRS cluster has an EIP attached, this cluster is noncompliant.
3.3	rds-instance-no-public-ip	rds	If an RDS instance has an EIP attached, this RDS instance is noncompliant.
3.3	bms-key-pair-security-login	bms	If a BMS does not have key pair login enabled, ths BMS is noncompliant.
3.1	apig-instances-ssl-enabled	apig	If no SSL certificates are attached to a dedicated APIG gateway, this gateway is considered noncompliant.
3.1	css-cluster-disk-encryption-check	css	If disk encryption is not enabled for a CSS cluster, this cluster is noncompliant.
3.1	css-cluster-https-required	css	If **HTTPS Access** is not enabled for a CSS cluster, this cluster is noncompliant.
3.1	dws-enable-ssl	dws	If SSL is not enabled for a DWS cluster, this cluster is noncompliant.
3.1	elb-tls-https-listeners-only	elb	If any listener of a load balancer does not have the frontend protocol set to HTTPS, this load balancer is noncompliant.
3.11	cts-kms-encrypted-check	cts	If a CTS tracker is not encrypted using KMS, this tracker is noncompliant.
3.11	dws-enable-kms	dws	If KMS encryption is not enabled for a DWS cluster, this cluster is noncompliant.

Guideline No.	Rule	Cloud Service	Description
3.11	gaussdb-nosql-enable-disk-encryption	geminidb	If a GeminiDB instance does not have disk encryption enabled, this instance is noncompliant.
3.11	rds-instances-enable-kms	rds	If KMS encryption is not enabled for an RDS instance, this instance is noncompliant.
3.11	sfsturbo-encrypted-check	sfsturbo	If KMS encryption is not enabled for an SFS Turbo file system, this file system is noncompliant.
3.11	volumes-encrypted-check	evs, ecs	If a mounted EVS disk is not encrypted, this disk is noncompliant.
3.11	cbr-backup-encrypted-check	cbr	If a CBR backup is not encrypted, this backup is noncompliant.
3.14	apig-instances-execution-logging-enabled	apig	If logging is not enabled for a dedicated APIG gateway, this gateway is considered non-compliant.
3.14	cts-lts-enable	cts	If a CTS tracker does not have trace transfer to LTS enabled, this tracker is noncompliant.
3.14	cts-obs-bucket-track	cts	If there are no CTS trackers created for the specified OBS bucket, the current account is noncompliant.
3.14	cts-tracker-exists	cts	If there are no CTS trackers in an account, this account is noncompliant.
3.14	multi-region-cts-tracker-exists	cts	If there are no CTS trackers in any of the specified regions, this rule is noncompliant.
3.14	rds-instance-logging-enabled	rds	If an RDS instance does not have the collection of any types of logs enabled, this instance is noncompliant.
3.14	vpc-flow-logs-enabled	vpc	If flow logs are not enabled for a VPC, this VPC is noncompliant. If not, the VPCs are considered non-compliant.

Guideline No.	Rule	Cloud Service	Description
4.1	access-keys-rotated	iam	If an IAM user's access key is not rotated within the specified number of days, this user is noncompliant.
4.1	evs-use-in-specified-days	evs	If an EVS disk has not been used within the specified time range after being created, this disk is noncompliant.
4.1	stopped-ecs-date-diff	ecs	If an ECS has been stopped for longer than the time allowed, and no operations have been performed on it, this ECS is noncompliant.
4.1	volume-unused-check	evs	If an EVS disk is not mounted to any cloud server, this disk is noncompliant.
4.6	apig-instances-ssl-enabled	apig	If no SSL certificates are attached to a dedicated APIG gateway, this gateway is considered noncompliant.
4.6	css-cluster-https-required	css	If **HTTPS Access** is not enabled for a CSS cluster, this cluster is noncompliant.
4.6	dws-enable-ssl	dws	If SSL is not enabled for a DWS cluster, this cluster is noncompliant.
4.6	elb-tls-https-listeners-only	elb	If any listener of a load balancer is not configured with HTTPS, this load balancer is noncompliant.
4.7	iam-root-access-key-check	iam	If the root user access key is available, this rule is noncompliant.
5.2	iam-password-policy	iam	If the password of an IAM user does not meet the password strength requirements, this IAM user is noncompliant.
5.2	iam-user-mfa-enabled	iam	If multi-factor authentication is not enabled for an IAM user, this user is noncompliant.

Guideline No.	Rule	Cloud Service	Description
5.2	mfa-enabled-for-iam-console-access	iam	If MFA is not enabled for an IAM user who has a console password, this IAM user is noncompliant.
5.2	root-account-mfa-enabled	iam	If multi-factor authentication is not enabled for the root user, the root user is noncompliant.
5.3	iam-user-last-login-check	iam	If an IAM user does not log in to the system within the specified time range, this user is non-compliant.
5.4	iam-policy-no-statements-with-admin-access	iam	If an IAM policy grants administrator permissions (with the **Action** element set to ***:*:***, ***:***, or *****), this policy is noncompliant.
5.4	iam-root-access-key-check	iam	If the root user access key is available, this rule is noncompliant.
6.4	iam-user-mfa-enabled	iam	If multi-factor authentication is not enabled for an IAM user, this user is noncompliant.
6.4	mfa-enabled-for-iam-console-access	iam	If MFA is not enabled for an IAM user who has a console password, this IAM user is noncompliant.
6.4	root-account-mfa-enabled	iam	If multi-factor authentication is not enabled for the root user, the root user is noncompliant.
8.2	apig-instances-execution-logging-enabled	apig	If logging is not enabled for a dedicated APIG gateway, this gateway is considered non-compliant.
8.2	cts-lts-enable	cts	If a CTS tracker does not have trace transfer to LTS enabled, this tracker is noncompliant.
8.2	cts-obs-bucket-track	cts	If there are no CTS trackers created for the specified OBS bucket, the current account is noncompliant.

Guideline No.	Rule	Cloud Service	Description
8.2	cts-tracker-exists	cts	If there are no CTS trackers in an account, this account is noncompliant.
8.2	multi-region-cts-tracker-exists	cts	If there are no CTS trackers in any of the specified regions, this rule is noncompliant.
8.2	rds-instance-logging-enabled	rds	If neither error logs nor slow query logs are collected for an RDS instance, this instance is noncompliant.
8.2	vpc-flow-logs-enabled	vpc	If flow logs are not enabled for a VPC, this VPC is noncompliant. If not, the VPCs are considered non-compliant.
8.5	apig-instances-execution-logging-enabled	apig	If logging is not enabled for a dedicated APIG gateway, this gateway is considered non-compliant.
8.5	cts-lts-enable	cts	If a CTS tracker does not have trace transfer to LTS enabled, this tracker is noncompliant.
8.5	cts-obs-bucket-track	cts	If there are no CTS trackers created for the specified OBS bucket, the current account is noncompliant.
8.5	cts-tracker-exists	cts	If there are no CTS trackers in an account, this account is noncompliant.
8.5	multi-region-cts-tracker-exists	cts	If there are no CTS trackers in any of the specified regions, this rule is noncompliant.
8.5	rds-instance-logging-enabled	rds	If an RDS instance does not have the collection of any types of logs enabled, this instance is noncompliant.
8.5	vpc-flow-logs-enabled	vpc	If flow logs are not enabled for a VPC, this VPC is noncompliant. If not, the VPCs are considered non-compliant.
8.9	cts-lts-enable	cts	If a CTS tracker does not have trace transfer to LTS enabled, this tracker is noncompliant.

Guideline No.	Rule	Cloud Service	Description
11.2	dws-enable-snapshot	dws	If automated snapshots are not enabled for a DWS cluster, this cluster is noncompliant.
11.2	gaussdb-instance-enable-backup	gaussdb	If the backup is not enabled for a GaussDB instance, this instance is noncompliant.
11.2	gaussdb-mysql-instance-enable-backup	taurusdb	If the backup is disabled for a TaurusDB instance, this instance is noncompliant.
11.2	gaussdb-nosql-enable-backup	geminidb	If a GeminiDB instance does not have the backup feature enabled, this instance is noncompliant.
11.2	rds-instance-enable-backup	rds	If backup is not enabled for an RDS instance, this instance is noncompliant.
11.3	rds-instances-enable-kms	rds	If KMS encryption is not enabled for an RDS instance, this instance is noncompliant.
11.3	volumes-encrypted-check	evs, ecs	If a mounted EVS disk is not encrypted, this disk is noncompliant.
11.4	dws-enable-snapshot	dws	If automated snapshots are not enabled for a DWS cluster, this cluster is noncompliant.
11.4	gaussdb-instance-enable-backup	gaussdb	If the backup is not enabled for a GaussDB instance, this instance is noncompliant.
11.4	gaussdb-mysql-instance-enable-backup	taurusdb	If the backup is disabled for a TaurusDB instance, this instance is noncompliant.
11.4	gaussdb-nosql-enable-backup	geminidb	If a GeminiDB instance does not have the backup feature enabled, this instance is noncompliant.
11.4	rds-instance-enable-backup	rds	If backup is not enabled for an RDS instance, this instance is noncompliant.
12.2	css-cluster-in-vpc	css	If a CSS cluster is not in the specified VPCs, this cluster is noncompliant.

Guideline No.	Rule	Cloud Service	Description
12.2	drs-data-guard-job-not-public	drs	If the network type of a DR task is not set to public network, this task is noncompliant.
12.2	drs-migration-job-not-public	drs	If the network type of a migration task is set to public network, this migration task is noncompliant.
12.2	drs-synchronization-job-not-public	drs	If the network type of a synchronization task is not set to public network, this task is noncompliant.
12.2	ecs-instance-in-vpc	ecs, vpc	If an ECS is not within the specified VPC, this ECS is noncompliant.
12.2	ecs-instance-no-public-ip	ecs	If an ECS has an EIP attached, this ECS is noncompliant.
12.2	function-graph-inside-vpc	fgs	If a function is not in the specified VPC, this function is noncompliant.
12.2	function-graph-public-access-prohibited	fgs	If a function can be accessed over a public network, this function is noncompliant.
12.2	mrs-cluster-no-public-ip	mrs	If an MRS cluster has an EIP attached, this cluster is noncompliant.
12.2	pca-certificate-authority-expiration-check	pca	If the validity period of a private CA is not within the specified period, this CA is noncompliant.
12.2	pca-certificate-expiration-check	pca	If the validity period of a certificate is not within the specified range, this certificate is noncompliant.
12.2	rds-instance-multi-az-support	rds	If an RDS instance does not support multi-AZ deployment, this RDS instance is noncompliant.
12.2	rds-instance-no-public-ip	rds	If an RDS instance has an EIP attached, this RDS instance is noncompliant.

Guideline No.	Rule	Cloud Service	Description
12.2	vpc-default-sg-closed	vpc	If a default security group allows all inbound or outbound traffic, this security group is noncompliant.
12.2	vpc-sg-ports-check	vpc	If a security group allows all inbound traffic (with the source address set to **0.0.0.0/0**) and opens all TCP/UDP ports, this security group is noncompliant.
12.2	vpc-sg-restricted-common-ports	vpc	If a security group allows all IPv4 addresses (0.0.0.0/0) to access a specified port, this security group is noncompliant.
12.2	vpc-sg-restricted-ssh	vpc	If the source address is set to **0.0.0.0/0** and the TCP port 22 is opened, this security group is non-compliant.
12.2	vpn-connections-active	vpnaas	If a VPN is not normally connected, this rule is noncompliant.
12.3	apig-instances-ssl-enabled	apig	If no SSL certificates are attached to a dedicated APIG gateway, this gateway is considered noncompliant.
12.3	css-cluster-https-required	css	If HTTPS is not enabled for a CSS cluster, this cluster is noncompliant.
12.3	dws-enable-ssl	dws	If SSL is not enabled for a DWS cluster, this cluster is noncompliant.
12.3	elb-tls-https-listeners-only	elb	If any listener of a load balancer does not have the frontend protocol set to HTTPS, this load balancer is noncompliant.
12.6	apig-instances-ssl-enabled	apig	If no SSL certificates are attached to a dedicated APIG gateway, this gateway is considered noncompliant.

Guideline No.	Rule	Cloud Service	Description
12.6	css-cluster-https-required	css	If HTTPS is not enabled for a CSS cluster, this cluster is noncompliant.
12.6	dws-enable-ssl	dws	If SSL is not enabled for a DWS cluster, this cluster is noncompliant.
12.6	elb-tls-https-listeners-only	elb	If any listener of a load balancer does not have the frontend protocol set to HTTPS, this load balancer is noncompliant.
13.6	vpc-flow-logs-enabled	vpc	If a VPC does not have the flow log enabled, this VPC is noncompliant.

4.5.26 Conformance Package for Landing Zone

This section describes the background and the conformance package for basic scenarios of Landing Zone.

Background

To help customers better manage the cloud, Huawei Cloud provided the Landing Zone solution. This solution integrates years of experience in enterprise governance and digital transformation. Landing Zone gives you a scalable, secure, and compliant cloud environment. If you run a large enterprise with diverse services in the finance sector, Landing Zone is a wise choice for cloud migration and digital transformation. Landing Zone helps enterprises build cloud environments in a number of different ways based on best practices. For instance, there is multi-account organization management, network planning, identity and permissions, data boundaries, security protection, compliance audit, O&M monitoring, and cost management.

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 following table describes the compliance rules and solutions in the sample template.

Table 4-33 Conformance package for Landing Zone

Module	Rule
Design of organization units and accounts	account-part-of-organizations
Design of organization units and accounts	iam-user-group-membership-check
Design of organization units and accounts	iam-group-has-users-check
Identity and permissions	root-account-mfa-enabled
Identity and permissions	mfa-enabled-for-iam-console-access
Identity and permissions	iam-root-access-key-check
Identity and permissions	iam-user-single-access-key
Identity and permissions	iam-password-policy
Identity and permissions	access-keys-rotated
Identity and permissions	iam-user-last-login-check
Identity and permissions	iam-policy-no-statements-with-admin-access
Unified network architecture	eip-unbound-check
Unified network architecture	elb-tls-https-listeners-only
Unified network architecture	vpc-acl-unused-check
Unified network architecture	vpc-sg-restricted-ssh
Unified network architecture	vpc-default-sg-closed
Unified network architecture	vpc-sg-ports-check
Unified network architecture	vpn-connections-active
Unified operations monitoring	alarm-obs-bucket-policy-change
Unified operations monitoring	alarm-vpc-change
Unified operations monitoring	alarm-kms-disable-or-delete-key
Unified compliance audit	cts-lts-enable
Unified compliance audit	cts-support-validate-check
Unified compliance audit	cts-kms-encrypted-check
Unified compliance audit	multi-region-cts-tracker-exists
Unified security management	cce-endpoint-public-access
Unified security management	ecs-instance-no-public-ip

Module	Rule
Unified security management	rds-instance-no-public-ip
Unified security management	pca-certificate-authority-expiration-check
Unified security management	pca-certificate-expiration-check
Unified security management	volumes-encrypted-check
Unified security management	rds-instances-enable-kms
Reliable architecture	rds-instance-enable-backup
Reliable architecture	rds-instance-multi-az-support
Reliable architecture	volume-unused-check

4.5.27 Architecture Security Best Practices

The following table describes the compliance rules and solutions in the sample template.

Table 4-34 Conformance package description

Rule	Cloud Service	Description
access-keys-rotated	iam	If an IAM user's access key is not rotated within the specified number of days, this user is noncompliant.
pca-certificate-authority-expiration-check	pca	If the validity period of a private CA is not within the specified period, this CA is noncompliant.
pca-certificate-expiration-check	pca	If the validity period of a private CA is not within the specified period, this CA is noncompliant.
apig-instances-execution-logging-enabled	apig	If logging is not enabled for a dedicated APIG gateway, this gateway is considered non-compliant.

Rule	Cloud Service	Description
apig-instances-ssl-enabled	apig	If no SSL certificates are attached to an APIG gateway, this gateway is considered noncompliant.
cts-lts-enable	cts	If a CTS tracker does not have trace transfer to LTS enabled, this tracker is noncompliant.
cts-kms-encrypted-check	cts	If a CTS tracker is not encrypted using KMS, this tracker is noncompliant.
cts-support-validate-check	cts	If a CTS tracker does not have trace file verification enabled, this tacker is noncompliant.
cts-obs-bucket-track	cts	If there are no CTS trackers created for the specified OBS bucket, the current account is noncompliant.
ecs-multiple-public-ip-check	ecs	If an ECS has multiple EIPs attached, this ECS is noncompliant.
ecs-instance-no-public-ip	ecs	If an ECS has an EIP attached, this ECS is noncompliant.
stopped-ecs-date-diff	ecs	If an ECS has been stopped for longer than the time allowed, and no operations have been performed on it, this ECS is noncompliant.
evs-use-in-specified-days	evs	If an EVS disk has not been attached to any resources within the specified number of days after being created, this disk is noncompliant.
volume-unused-check	evs	If an EVS disk is not mounted to any cloud server, this disk is noncompliant.

Rule	Cloud Service	Description
cce-cluster-end-of-maintenance-version	cce	If the version of a CCE cluster is no longer supported for maintenance, this cluster is noncompliant.
cce-cluster-oldest-supported-version	cce	If a CCE cluster is running the oldest supported version, this cluster is noncompliant.
sfsturbo-encrypted-check	sfsturbo	If KMS encryption is not enabled for an SFS Turbo file system, this file system is noncompliant.
css-cluster-in-vpc	css	If a CSS cluster is not in the specified VPCs, this cluster is noncompliant.
css-cluster-disk-encryption-check	css	If disk encryption is not enabled for a CSS cluster, this cluster is noncompliant.
elb-tls-https-listeners-only	elb	If any listener of a load balancer does not have the frontend protocol set to HTTPS, this load balancer is noncompliant.
mrs-cluster-kerberos-enabled	mrs	If kerberos is not enabled for an MRS cluster, this cluster is noncompliant.
mrs-cluster-no-public-ip	mrs	If an MRS cluster has an EIP attached, this cluster is noncompliant.
volumes-encrypted-check	ecs, evs	If a mounted EVS disk is not encrypted, this disk is noncompliant.
iam-customer-policy-blocked-kms-actions	iam, access-analyzer-verified	If an IAM policy allows any blocked actions on KMS keys, this policy is noncompliant.
iam-group-has-users-check	iam	If an IAM user group has no user, this user group is noncompliant.

Rule	Cloud Service	Description
iam-password-policy	iam	If the password of an IAM user does not meet the password strength requirements, this IAM user is noncompliant.
iam-policy-no-statements-with-admin-access	iam	If a custom policy or role allows all actions (with the action element set to ***:*:***, ***:***, or *****) for all cloud services, this policy or role is noncompliant.
iam-role-has-all-permissions	iam	If a custom policy or role allows all actions for a cloud service, this policy or role is noncompliant.
iam-root-access-key-check	iam	If the account root user has an available access key, the account is noncompliant.
iam-user-group-membership-check	iam	If an IAM user is not in any of the specified IAM user groups, this user is noncompliant.
iam-user-mfa-enabled	iam	If multi-factor authentication is not enabled for an IAM user, this user is noncompliant.
iam-user-last-login-check	iam	If an IAM user does not log in to the system within the specified time range, this user is non-compliant.
vpc-sg-restricted-ssh	vpc	If a security group allows all inbound traffic (with the source address set to **0.0.0.0/0** or **::/0**) and opens the TCP 22 port, this security group is noncompliant.
ecs-instance-in-vpc	ecs, vpc	If an ECS is not within the specified VPC, this ECS is noncompliant.

Rule	Cloud Service	Description
kms-not-scheduled-for-deletion	kms	If a KMS key is scheduled for deletion, this key is noncompliant.
function-graph-public-access-prohibited	fgs	If a function can be accessed over a public network, this function is noncompliant.
function-graph-inside-vpc	fgs	If a function is not in the specified VPC, this function is noncompliant.
mfa-enabled-for-iam-console-access	iam	If an IAM user who is allowed to access Huawei Cloud console does not have MFA enabled, this IAM user is noncompliant.
css-cluster-https-required	css	If a CSS cluster does not have HTTPS enabled, this cluster is noncompliant.
rds-instance-no-public-ip	rds	If an RDS instance has an EIP attached, this RDS instance is noncompliant.
rds-instance-logging-enabled	rds	If an RDS instance does not have the collection of any types of logs enabled, this instance is noncompliant.
rds-instances-enable-kms	rds	If KMS encryption is not enabled for an RDS instance, this instance is noncompliant.
dws-enable-kms	dws	If KMS encryption is not enabled for a DWS cluster, this cluster is noncompliant.
gaussdb-nosql-enable-disk-encryption	gemini db	If a GeminiDB instance does not have disk encryption enabled, this instance is noncompliant.

Rule	Cloud Service	Description
dws-enable-ssl	dws	If SSL is not enabled for a DWS cluster, this cluster is noncompliant.
vpc-sg-restricted-common-ports	vpc	If a security group allows all IPv4 and IPv6 traffic (with the source address set to **0.0.0.0/0** or **::/0**) to the specified ports, this security group is noncompliant.
root-account-mfa-enabled	iam	If the root user does not have MFA enabled, this root user is noncompliant.
vpc-default-sg-closed	vpc	If a default security group allows all inbound or outbound traffic, this security group is noncompliant.
vpc-flow-logs-enabled	vpc	If a VPC does not have the flow log enabled, this VPC is noncompliant.
vpc-acl-unused-check	vpc	If a network ACL is not attached to any subnets, this ACL is noncompliant.
vpc-sg-ports-check	vpc	If a security group has the source address set to **0.0.0.0/0** or **::/0** and opens all TCP/UDP ports, this security group is noncompliant.
waf-instance-policy-not-empty	waf	If a WAF instance does not have a protection policy attached, this instance is noncompliant.
pca-certificate-authority-root-disable	pca	If private root CAs are not disabled, this rule is noncompliant.

4.5.28 Best Practices for Network and Content Delivery Service Operations

The following table describes the compliance rules and solutions in the sample template.

Table 4-35 Conformance package description

Rule	Cloud Service	Description
apig-instances-execution-logging-enabled	apig	If logging is not enabled for a dedicated APIG gateway, this gateway is considered non-compliant.
apig-instances-ssl-enabled	apig	If no SSL certificates are attached to a dedicated APIG gateway, this gateway is considered noncompliant.
as-group-elb-healthcheck-required	as	If an AS group does not have health check enabled, this AS group is noncompliant.
elb-tls-https-listeners-only	elb	If any listener of a load balancer does not have the frontend protocol set to HTTPS, this load balancer is noncompliant.
vpc-sg-restricted-ssh	vpc	If a security group allows all inbound traffic (with the source address set to **0.0.0.0/0** or **::/0**) and opens the TCP 22 port, this security group is noncompliant.
ecs-instance-in-vpc	ecs, vpc	If an ECS is not within the specified VPC, this ECS is noncompliant.
private-nat-gateway-authorized-vpc-only	nat	If a private NAT gateway is not in a specified VPC, this gateway is noncompliant.

Rule	Cloud Service	Description
vpc-sg-restricted-common-ports	vpc	If a security group allows all IPv4 and IPv6 traffic (with the source address set to **0.0.0.0/0** or **::/0**) to the specified ports, this security group is noncompliant.
vpc-default-sg-closed	vpc	If a default security group allows all inbound or outbound traffic, this security group is noncompliant.
vpc-flow-logs-enabled	vpc	If a VPC does not have the flow log enabled, this VPC is noncompliant.
vpc-acl-unused-check	vpc	If a network ACL is not attached to any subnets, this ACL is noncompliant.
vpc-sg-ports-check	vpc	If a security group has the source address set to **0.0.0.0/0** or **::/0** and opens all TCP/UDP ports, this security group is noncompliant.
vpn-connections-active	vpnaas	If a VPN is not normally connected, this rule is noncompliant.

4.5.29 Best Practices for Idle Asset Management

Background

The best practices for idle asset management are used to check whether cloud resources, such as EIPs, ECSs, and EVS disks, have not been put into use for a long time after being purchased. Idle cloud resources should be detected and managed in a timely manner to prevent resource waste.

Rules

The following table describes the compliance rules and solutions in the sample template.

Table 4-36 Conformance package description

Rule	Cloud Service	Description
stopped-ecs-date-diff	ecs	If an ECS has been stopped for longer than the time allowed, and no operations have been performed on it, this ECS is noncompliant.
eip-use-in-specified-days	vpc	If an EIP has not been attached to any resources within the specified number of days after being created, this EIP is noncompliant.
evs-use-in-specified-days	evs	If an EVS disk has not been attached to any resources within the specified number of days after being created, this disk is noncompliant.
eip-unbound-check	vpc	If an EIP has not been attached to any resource, this EIP is noncompliant.
iam-group-has-users-check	iam	If an IAM user group has no user, this user group is noncompliant.
iam-user-last-login-check	iam	If an IAM user does not log in to the system within the specified time range, this user is non-compliant.
volume-unused-check	evs	If an EVS disk is not mounted to any cloud server, this disk is noncompliant.
vpc-acl-unused-check	vpc	If a network ACL is not attached to any subnets, this ACL is noncompliant.
cce-cluster-end-of-maintenance-version	cce	If the version of a CCE cluster is no longer supported for maintenance, this cluster is noncompliant.

4.5.30 Multi-AZ Deployment Best Practices

The following table describes the compliance rules and solutions in the sample template.

Table 4-37 Conformance package description

Rule	Cloud Service	Description
css-cluster-multiple-az-check	css	If a CSS cluster is not deployed across AZs, the cluster is noncompliant.
gaussdb-nosql-deploy-in-single-az	gemini db	If there is a single-AZ GeminiDB instance, this rule is noncompliant.
as-multiple-az	as	If an AS group is deployed in a single AZ, this AS group is noncompliant.
mrs-cluster-multiAZ-deployment	mrs	If an MRS cluster is deployed in a single AZ, this cluster is noncompliant.
rds-instance-multi-az-support	rds	If an RDS instance does not support multi-AZ deployment, this RDS instance is noncompliant.
dcs-redis-high-tolerance	dcs	If a DCS Redis instance does not have cross-AZ deployment enabled, this instance is noncompliant.
elb-multiple-az-check	elb	If a load balancer is mapped to only one AZ, this load balancer is noncompliant. If a load balancer is mapped to fewer than two AZs, this load balancer is noncompliant.
gaussdb-instance-multiple-az-check	gaussdb	If a GaussDB instance does not support cross-AZ deployment, this instance is noncompliant.

Rule	Cloud Service	Description
gaussdb-mysql-instance-multiple-az-check	taurus db	If a TaurusDB instance does not support cross-AZ deployment, this instance is noncompliant.

4.5.31 Resource Stability Best Practices

The following table describes the compliance rules and solutions in the sample template.

Table 4-38 Conformance package description

Rule	Cloud Service	Description
css-cluster-multiple-az-check	css	If a CSS cluster is not deployed across AZs, the cluster is noncompliant.
gaussdb-nosql-deploy-in-single-az	gemini db	If there is a single-AZ GeminiDB instance, this rule is noncompliant.
as-multiple-az	as	If an AS group is deployed in a single AZ, this AS group is noncompliant.
mrs-cluster-multiAZ-deployment	mrs	If an MRS cluster is deployed in a single AZ, this cluster is noncompliant.
rds-instance-multi-az-support	rds	If an RDS instance does not support multi-AZ deployment, this RDS instance is noncompliant.
dcs-redis-high-tolerance	dcs	If a DCS Redis instance does not have cross-AZ deployment enabled, this instance is noncompliant.
allowed-rds-flavors	rds	If the flavor of an RDS instance is not within the specified scope, this cluster is noncompliant.

Rule	Cloud Service	Description
allowed-images-by-name	ecs	If the name of an ECS's image does not match any of the specified image names, this ECS is noncompliant.
allowed-images-by-id	ecs, ims	If the ID of an ECS's image does not match any of the specified image IDs, this ECS is noncompliant.
function-graph-concurrency-check	fgs	If the number of concurrent requests allowed by a FunctionGraph function exceeds the specified limit, this function is noncompliant.
function-graph-settings-check	fgs	If the runtime, timeout, or memory limit of a function is not within the specified ranges, this function is noncompliant.
dds-instance-hamode	dds	If a DDS instance is inconsistent with the specified type, the instance is noncompliant.
allowed-cce-flavors	cce	If the flavor of a CCE cluster does not match any of the specified flavors, this cluster is noncompliant.
allowed-ecs-flavors	ecs	If an ECS's flavor is not one of the specified flavors, this ECS is noncompliant.

4.5.32 Best Practices for API Gateway

The following table describes the compliance rules and solutions in the sample template.

Table 4-39 Conformance package description

Rule	Cloud Service	Description
apig-instances-authorization-type-configured	apig	If a dedicated APIG gateway does not have any types of API authentication configured, this gateway is non-compliant.
apig-instances-execution-logging-enabled	apig	If logging is not enabled for a dedicated APIG gateway, this gateway is considered non-compliant.
apig-instances-ssl-enabled	apig	If no SSL certificates are attached to a dedicated APIG gateway, this gateway is considered noncompliant.

4.5.33 Best Practices for Cloud Container Engine

The following table describes the compliance rules and solutions in the sample template.

Table 4-40 Conformance package description

Rule	Cloud Service	Description
allowed-cce-flavors	cce	If the flavor of a CCE cluster does not match any of the specified flavors, this cluster is noncompliant.
cce-cluster-end-of-maintenance-version	cce	If the version of a CCE cluster is no longer supported for maintenance, this cluster is noncompliant.
cce-cluster-oldest-supported-version	cce	If a CCE cluster is running the oldest supported version, this cluster is noncompliant.
cce-endpoint-public-access	cce	If a CCE cluster has an EIP attached, this CCE cluster is noncompliant.

4.5.34 Best Practices for Content Delivery Network

The following table describes the compliance rules and solutions in the sample template.

Table 4-41 Conformance package description

Rule	Cloud Service	Description
cdn-enable-https-certificate	cdn	If a domain does not have an HTTPS certificate configured, this domain is noncompliant.
cdn-origin-protocol-no-http	cdn	If a domain does not have HTTPS configured for communication between CDN and origins, this domain is noncompliant.
cdn-security-policy-check	cdn	If a domain uses a TLS version earlier than version 1.2, this domain is noncompliant.
cdn-use-my-certificate	cdn	If a domain has its **Certificate Source** set to **My certificate**, this domain is noncompliant.

4.5.35 Best Practices for FunctionGraph

The following table describes the compliance rules and solutions in the sample template.

Table 4-42 Conformance package description

Rule	Cloud Service	Description
function-graph-concurrency-check	fgs	If the number of concurrent requests of a FunctionGraph function is not within the specified range, this function is noncompliant.

Rule	Cloud Service	Description
function-graph-inside-vpc	fgs	If a function is not in the specified VPC, this function is noncompliant.
function-graph-public-access-prohibited	fgs	If a function can be accessed over a public network, this function is noncompliant.
function-graph-settings-check	fgs	If the runtime, timeout, or memory limit of a function is not within the specified ranges, this function is noncompliant.
function-graph-logging-enabled	fgs	If a function does not have log collection enabled, this function is noncompliant.

4.5.36 Best Practices for GaussDB

The following table describes the compliance rules and solutions in the sample template.

Table 4-43 Conformance package description

Rule	Cloud Service	Description
gaussdb-instance-enable-auditLog	gaussdb	If a GaussDB instance does not have audit log collection enabled, this instance is noncompliant.
gaussdb-instance-enable-backup	gaussdb	If a GaussDB instance does not have the backup enabled, this instance is noncompliant.
gaussdb-instance-enable-errorLog	gaussdb	If a GaussDB instance does not have error log collection enabled, this instance is noncompliant.

Rule	Cloud Service	Description
gaussdb-instance-enable-slowLog	gaussdb	If a GaussDB instance does not have slow query log collection enabled, this instance is noncompliant.
gaussdb-instance-in-vpc	gaussdb	If a GaussDB instance is not in the specified VPC, this instance is noncompliant.
gaussdb-instance-multiple-az-check	gaussdb	If a GaussDB instance does not support cross-AZ deployment, this instance is noncompliant.
gaussdb-instance-no-public-ip-check	gaussdb	If a GaussDB instance has an EIP attached, this instance is noncompliant.
gaussdb-instance-ssl-enable	gaussdb	If a GaussDB instance does not have SSL enabled, this instance is noncompliant.

4.5.37 Best Practices for GeminiDB

The following table describes the compliance rules and solutions in the sample template.

Table 4-44 Conformance package description

Rule	Cloud Service	Description
gaussdb-nosql-deploy-in-single-az	gemini db	If there is a single-AZ GeminiDB instance, this rule is noncompliant.
gaussdb-nosql-enable-backup	gemini db	If a GeminiDB instance does not have the backup feature enabled, this instance is noncompliant.

Rule	Cloud Service	Description
gaussdb-nosql-enable-disk-encryption	gemini db	If a GeminiDB instance does not have disk encryption enabled, this instance is noncompliant.
gaussdb-nosql-enable-error-log	gemini db	If a GeminiDB instance does not have error log collection enabled, this instance is noncompliant.
gaussdb-nosql-support-slow-log	gemini db	If a GeminiDB instance does not have the slow query log collection enabled, this instance is noncompliant.

4.5.38 Best Practices for MapReduce Service

The following table describes the compliance rules and solutions in the sample template.

Table 4-45 Conformance package description

Rule	Cloud Service	Description
mrs-cluster-in-allowed-security-groups	mrs	If an MRS cluster does not have a specified security group attached, the cluster is noncompliant.
mrs-cluster-in-vpc	mrs	If an MRS cluster is not in the specified VPC, this cluster is noncompliant.
mrs-cluster-kerberos-enabled	mrs	If kerberos is not enabled for an MRS cluster, this cluster is noncompliant.
mrs-cluster-multiAZ-deployment	mrs	If an MRS cluster does not support multi-AZ deployment, this cluster is noncompliant.
mrs-cluster-no-public-ip	mrs	If an MRS cluster has an EIP attached, this cluster is noncompliant.

Rule	Cloud Service	Description
mrs-cluster-encrypt-enable	mrs	If KMS encryption is not enabled for an MRS cluster, this cluster is noncompliant.

4.5.39 Best Practices for NIST Requirements

Applicable Scenario

Config provides a conformance package to help you check if your resources on Huawei Cloud meet some of the National Institute of Standards and Technology (NIST) requirements.

Rules

The following table lists the rules and solutions included in this conformance package template.

Table 4-46 Conformance package description

Rule	Cloud Service	Description
access-keys-rotated	iam	If an IAM user's access key is not rotated within the specified number of days, this user is noncompliant.
apig-instances-execution-logging-enabled	apig	If logging is not enabled for a dedicated APIG gateway, this gateway is considered non-compliant.
apig-instances-ssl-enabled	apig	If no SSL certificates are attached to a dedicated APIG gateway, this gateway is considered noncompliant.
as-group-elb-healthcheck-required	as	If an AS group does not have health check enabled, this AS group is noncompliant.
css-cluster-disk-encryption-check	css	If disk encryption is not enabled for a CSS cluster, this cluster is noncompliant.

Rule	Cloud Service	Description
css-cluster-in-vpc	css	If a CSS cluster is not in the specified VPCs, this cluster is noncompliant.
cts-kms-encrypted-check	cts	If a CTS tracker does not have KMS encryption enabled, this tracker is noncompliant.
cts-lts-enable	cts	If a CTS tracker does not have trace transfer to LTS enabled, this tracker is noncompliant.
cts-obs-bucket-track	cts	If there are no CTS trackers created for the specified OBS bucket, the current account is noncompliant.
cts-support-validate-check	cts	If a CTS tracker does not have trace file verification enabled, this tacker is noncompliant.
cts-tracker-exists	cts	If there are no trackers or all trackers are disabled in an account, the current account is noncompliant.
drs-data-guard-job-not-public	drs	If the network type of a DR task is set to public network, this DR task is noncompliant.
drs-migration-job-not-public	drs	If the network type of a migration task is set to public network, this migration task is noncompliant.
drs-synchronization-job-not-public	drs	If the network type of a synchronization task is not set to public network, this synchronization task is noncompliant.
dws-enable-kms	dws	If KMS encryption is not enabled for a DWS cluster, this cluster is noncompliant.

Rule	Cloud Service	Description
dws-enable-snapshot	dws	If automated snapshots are not enabled for a DWS cluster, this cluster is noncompliant.
dws-enable-ssl	dws	If SSL is not enabled for a DWS cluster, this cluster is noncompliant.
ecs-instance-in-vpc	ecs, vpc	If an ECS is not within the specified VPC, this ECS is noncompliant.
ecs-instance-no-public-ip	ecs	If an ECS has an EIP attached, this ECS is noncompliant.
eip-unbound-check	vpc	If an EIP has not been attached to any resource, this EIP is noncompliant.
eip-use-in-specified-days	vpc	If an EIP has not been attached to any resources within the specified number of days after being created, this EIP is noncompliant.
elb-tls-https-listeners-only	elb	If any listener of a load balancer does not have the frontend protocol set to HTTPS, this load balancer is noncompliant.
evs-use-in-specified-days	evs	If an EVS disk has not been attached to any resources within the specified number of days after being created, this disk is noncompliant.
function-graph-inside-vpc	fgs	If a function is not in the specified VPC, this function is noncompliant.
function-graph-public-access-prohibited	fgs	If a function can be accessed over a public network, this function is noncompliant.

Rule	Cloud Service	Description
gaussdb-nosql-enable-backup	gemini db	If a GeminiDB instance does not have the backup enabled, this instance is noncompliant.
iam-customer-policy-blocked-kms-actions	iam, access-analyzer-verified	If an IAM policy allows any blocked actions on KMS keys, this policy is noncompliant.
iam-group-has-users-check	iam	If an IAM user group has no user, this user group is noncompliant.
iam-password-policy	iam	If the password of an IAM user does not meet the password strength requirements, this IAM user is noncompliant.
iam-policy-no-statements-with-admin-access	iam	If a custom policy or role allows all actions (with the action element set to *:*:*, *:*, or *) for all cloud services, this policy or role is noncompliant.
iam-role-has-all-permissions	iam	If a custom policy or role allows all actions for a cloud service, this policy or role is noncompliant.
iam-root-access-key-check	iam	If the account root user has an available access key, the account is noncompliant.
iam-user-group-membership-check	iam	If an IAM user is not in any of the specified IAM user groups, this user is noncompliant.
iam-user-mfa-enabled	iam	If multi-factor authentication is not enabled for an IAM user, this user is noncompliant.
kms-not-scheduled-for-deletion	kms	If a KMS key is scheduled for deletion, this key is noncompliant.

Rule	Cloud Service	Description
kms-rotation-enabled	kms	If key rotation is not enabled for a KMS key, this key is noncompliant.
mfa-enabled-for-iam-console-access	iam	If an IAM user who is allowed to access Huawei Cloud console does not have MFA enabled, this IAM user is noncompliant.
mrs-cluster-kerberos-enabled	mrs	If an MRS cluster does not have Kerberos authentication enabled, this cluster is noncompliant.
mrs-cluster-no-public-ip	mrs	If an MRS cluster has an EIP attached, this cluster is noncompliant.
multi-region-cts-tracker-exists	cts	If there are no enabled CTS trackers in any of the specified regions, the current account is noncompliant.
private-nat-gateway-authorized-vpc-only	nat	If a private NAT gateway is not in a specified VPC, this gateway is noncompliant.
rds-instance-enable-backup	rds	If backup is not enabled for an RDS instance, this instance is noncompliant.
rds-instance-multi-az-support	rds	If an RDS instance does not support multi-AZ deployment, this RDS instance is noncompliant.
rds-instance-no-public-ip	rds	If an RDS instance has an EIP attached, this RDS instance is noncompliant.
root-account-mfa-enabled	iam	If the root user does not have MFA enabled, this root user is noncompliant.

Rule	Cloud Service	Description
sfsturbo-encrypted-check	sfsturbo	If KMS encryption is not enabled for an SFS Turbo file system, this file system is noncompliant.
stopped-ecs-date-diff	ecs	If an ECS has been stopped for longer than the time allowed, and no operations have been performed on it, this ECS is noncompliant.
volume-unused-check	evs	If an EVS disk is not mounted to any cloud server, this disk is noncompliant.
volumes-encrypted-check	ecs, evs	If a mounted EVS disk is not encrypted, this disk is noncompliant.
vpc-acl-unused-check	vpc	If a network ACL is not attached to any subnets, this ACL is noncompliant.
vpc-default-sg-closed	vpc	If a default security group allows all inbound or outbound traffic, this security group is noncompliant.
vpc-sg-ports-check	vpc	If a security group has the source address set to **0.0.0.0/0** or **::/0** and opens all TCP/UDP ports, this security group is noncompliant.
vpc-sg-restricted-common-ports	vpc	If a security group allows all inbound traffic from any IPv4 address (0.0.0.0/0) or IPv6 address to a specified port, this security group is noncompliant.
vpc-sg-restricted-ssh	vpc	If a security group allows all inbound traffic (with the source address set to **0.0.0.0/0** or **::/0**) and opens the TCP 22 port, this security group is noncompliant.

Rule	Cloud Service	Description
vpn-connections-active	vpnaas	If a VPN is not normally connected, this rule is noncompliant.

4.5.40 Best Practices for Singapore Financial Industry

Applicable Scenario

The Monetary Authority of Singapore has developed the MAS guidelines to regulate the practices of financial institutions. For more information about the guidelines, see **Technology Risk Management Guidelines**.

Rules

The following table lists the rules and solutions included in this conformance package template.

Table 4-47 Conformance package description

Rule	Cloud Service	Description
access-keys-rotated	iam	If an IAM user's access key is not rotated within the specified number of days, this user is noncompliant.
account-part-of-organizations	organizations	If an account has not been added to any organizations or to a specified organization, this account is noncompliant.
pca-certificate-authority-expiration-check	pca	If the validity period of a private CA is not within the specified period, this CA is noncompliant.
pca-certificate-expiration-check	pca	If the validity period of a private certificate is not within the specified period, this certificate is noncompliant.

Rule	Cloud Service	Description
elb-http-to-https-redirection-check	elb	If an HTTP listener does not have redirecting requests to an HTTPS listener enabled, this HTTP listener is noncompliant.
apig-instances-execution-logging-enabled	apig	If logging is not enabled for a dedicated APIG gateway, this gateway is considered non-compliant.
apig-instances-ssl-enabled	apig	If no SSL certificates are attached to a dedicated APIG gateway, this gateway is considered noncompliant.
as-group-elb-healthcheck-required	as	If an AS group does not have health check enabled, this AS group is noncompliant.
as-group-ipv6-disabled	as	If an AS group has an IPv6 shared bandwidth attached, this AS group is noncompliant
cts-lts-enable	cts	If a CTS tracker does not have trace transfer to LTS enabled, this tracker is noncompliant.
cts-tracker-exists	cts	If there are no trackers or all trackers are disabled in an account, this account is noncompliant.
cts-kms-encrypted-check	cts	If a CTS tracker does not have KMS encryption enabled, this tracker is noncompliant.
cts-support-validate-check	cts	If a CTS tracker does not have trace file verification enabled, this tacker is noncompliant.

Rule	Cloud Service	Description
cts-obs-bucket-track	cts	If no CTS trackers are created for the specified OBS bucket, this rule is noncompliant.
cts-tracker-enabled-security	cts	If there is no tracker that complies with security best practices, this rule is noncompliant.
kms-rotation-enabled	kms	If key rotation is not enabled for a KMS key, this key is noncompliant.
cloudbuildserver-encryption-parameter-check	codeartsbuild	If encryption is not enabled for custom parameters of a CodeArts build project, this project is noncompliant.
rds-instance-enable-backup	rds	If backup is not enabled for an RDS instance, this instance is noncompliant.
drs-data-guard-job-not-public	drs	If the network type of a DR task is set to public network, this DR task is noncompliant.
drs-migration-job-not-public	drs	If the network type of a migration task is set to public network, this migration task is noncompliant.
drs-synchronization-job-not-public	drs	If the network type of a synchronization task is not set to public network, this synchronization task is noncompliant.
volumes-encrypted-check-by-default	evs	If an EVS disk is not encrypted, this EVS disk is noncompliant.
ecs-instance-no-public-ip	ecs	If an ECS has an EIP attached, this ECS is noncompliant.

Rule	Cloud Service	Description
ecs-instance-agency-attach-iam-agency	ecs	If an ECS does not have any IAM agencies attached, this ECS is noncompliant.
sfsturbo-encrypted-check	sfsturbo	If KMS encryption is not enabled for an SFS Turbo file system, this file system is noncompliant.
css-cluster-in-vpc	css	If a CSS cluster is not in the specified VPCs, this cluster is noncompliant.
css-cluster-disk-encryption-check	css	If disk encryption is not enabled for a CSS cluster, this cluster is noncompliant.
elb-multiple-az-check	elb	If a load balancer is mapped to only one availability zone (AZ), this load balancer is noncompliant. If a load balancer is mapped to fewer than two AZs, this load balancer is noncompliant.
elb-tls-https-listeners-only	elb	If any listener of a load balancer does not have the frontend protocol set to HTTPS, this load balancer is noncompliant.
mrs-cluster-kerberos-enabled	mrs	If an MRS cluster does not have Kerberos authentication enabled, this cluster is noncompliant.
mrs-cluster-no-public-ip	mrs	If an MRS cluster has an EIP attached, this cluster is noncompliant.
volumes-encrypted-check	ecs, evs	If a mounted EVS disk is not encrypted, this disk is noncompliant.

Rule	Cloud Service	Description
iam-customer-policy-blocked-kms-actions	iam, access-analyzer-verified	If an IAM policy allows any blocked actions on KMS keys, this policy is noncompliant.
iam-group-has-users-check	iam	If an IAM user group has no user, this user group is noncompliant.
iam-password-policy	iam	If the password of an IAM user does not meet the password strength requirements, this IAM user is noncompliant.
iam-policy-no-statements-with-admin-access	iam	If a custom policy or role allows all actions (with the action element set to *:*:*, *:*, or *) for all cloud services, this policy or role is noncompliant.
iam-role-has-all-permissions	iam	If a custom policy or role allows all actions for a cloud service, this policy or role is noncompliant.
iam-root-access-key-check	iam	If the account root user has an available access key, the account is noncompliant.
iam-user-group-membership-check	iam	If an IAM user is not in any of the specified IAM user groups, this user is noncompliant.
iam-user-mfa-enabled	iam	If multi-factor authentication is not enabled for an IAM user, this user is noncompliant.
iam-user-last-login-check	iam	If an IAM user does not log in to the system within the specified period, this user is non-compliant.

Rule	Cloud Service	Description
vpc-sg-restricted-ssh	vpc	If a security group allows all inbound traffic (with the source address set to **0.0.0.0/0** or **::/0**) and opens the TCP 22 port, this security group is noncompliant.
ecs-instance-in-vpc	ecs, vpc	If an ECS is not within the specified VPC, this ECS is noncompliant.
kms-not-scheduled-for-deletion	kms	If a KMS key is scheduled for deletion, this key is noncompliant.
function-graph-public-access-prohibited	fgs	If a function can be accessed over a public network, this function is noncompliant.
function-graph-inside-vpc	fgs	If a function is not in the specified VPC, this function is noncompliant.
mfa-enabled-for-iam-console-access	iam	If an IAM user who is allowed to access Huawei Cloud console does not have MFA enabled, this IAM user is noncompliant.
css-cluster-https-required	css	If a CSS cluster does not have HTTPS enabled, this cluster is noncompliant.
rds-instance-no-public-ip	rds	If an RDS instance has an EIP attached, this RDS instance is noncompliant.
rds-instance-logging-enabled	rds	If an RDS instance does not have the collection of any types of logs enabled, this instance is noncompliant.
rds-instance-multi-az-support	rds	If an RDS instance does not support multi-AZ deployment, this RDS instance is noncompliant.

Rule	Cloud Service	Description
rds-instances-enable-kms	rds	If KMS encryption is not enabled for an RDS instance, this instance is noncompliant.
dws-enable-snapshot	dws	If automated snapshots are not enabled for a DWS cluster, this cluster is noncompliant.
gaussdb-instance-enable-backup	gaussdb	If a GaussDB instance does not have the backup enabled, this instance is noncompliant.
gaussdb-mysql-instance-enable-backup	taurusdb	If a TaurusDB instance does not have the backup enabled, this instance is noncompliant.
gaussdb-nosql-enable-backup	gemini db	If a GeminiDB instance does not have the backup enabled, this instance is noncompliant.
dws-enable-kms	dws	If KMS encryption is not enabled for a DWS cluster, this cluster is noncompliant.
gaussdb-nosql-enable-disk-encryption	gemini db	If a GeminiDB instance does not have disk encryption enabled, this instance is noncompliant.
dws-maintain-window-check	dws	If the O&M time window of a DWS cluster is not consistent with the specified time window, this cluster is noncompliant.
dws-clusters-no-public-ip	dws	If a DWS cluster has an EIP attached, this cluster is noncompliant.
dws-enable-ssl	dws	If SSL is not enabled for a DWS cluster, this cluster is noncompliant.

Rule	Cloud Service	Description
vpc-sg-restricted-common-ports	vpc	If a security group allows all IPv4 and IPv6 traffic (with the source address set to **0.0.0.0/0** or **::/0**) to the specified ports, this security group is noncompliant.
root-account-mfa-enabled	iam	If the root user does not have MFA enabled, this root user is noncompliant.
csms-secrets-rotation-success-check	csms	If a CSMS secret fails to be rotated, this secret is noncompliant.
vpc-default-sg-closed	vpc	If a default security group allows all inbound or outbound traffic, this security group is noncompliant.
vpc-flow-logs-enabled	vpc	If a VPC does not have the flow log enabled, this VPC is noncompliant.
vpc-sg-ports-check	vpc	If a security group has the source address set to **0.0.0.0/0** or **::/0** and opens all TCP/UDP ports, this security group is noncompliant.
vpn-connections-active	vpnaas	If a VPN is not normally connected, this rule is noncompliant.

4.5.41 Best Practices for Secure Identity and Compliance Operations

The following table describes the compliance rules and solutions in the sample template.

Table 4-48 Conformance package description

Rule	Cloud Service	Description
access-keys-rotated	iam	If an IAM user's access key is not rotated within the specified number of days, this user is noncompliant.
pca-certificate-authority-expiration-check	pca	If the validity period of a private CA is not within the specified period, this CA is noncompliant.
pca-certificate-expiration-check	pca	If the validity period of a private certificate is not within the specified range, this certificate is noncompliant.
apig-instances-execution-logging-enabled	apig	If logging is not enabled for a dedicated APIG gateway, this gateway is considered non-compliant.
cts-lts-enable	cts	If a CTS tracker does not have trace transfer to LTS enabled, this tracker is noncompliant.
cts-tracker-exists	cts	If there are no trackers or all trackers are disabled in an account, this account is noncompliant.
cts-kms-encrypted-check	cts	If a CTS tracker does not have KMS encryption enabled, this tracker is noncompliant.
cts-support-validate-check	cts	If a CTS tracker does not have trace file verification enabled, this tacker is noncompliant.
kms-rotation-enabled	kms	If key rotation is not enabled for a KMS key, this key is noncompliant.
iam-customer-policy-blocked-kms-actions	iam, access-analyzer-verified	If an IAM policy allows any blocked actions on KMS keys, this policy is noncompliant.

Rule	Cloud Service	Description
iam-group-has-users-check	iam	If an IAM user group has no user, this user group is noncompliant.
iam-password-policy	iam	If the password of an IAM user does not meet the password strength requirements, this IAM user is noncompliant.
iam-policy-no-statements-with-admin-access	iam	If a custom policy or role allows all actions (with the action element set to *:*:*, *:*, or *) for all cloud services, this policy or role is noncompliant.
iam-role-has-all-permissions	iam	If a custom policy or role allows all actions for a cloud service, this policy or role is noncompliant.
iam-root-access-key-check	iam	If the account root user has an available access key, the account is noncompliant.
iam-user-group-membership-check	iam	If an IAM user is not in any of the specified IAM user groups, this user is noncompliant.
iam-user-mfa-enabled	iam	If multi-factor authentication is not enabled for an IAM user, this user is noncompliant.
iam-user-last-login-check	iam	If an IAM user does not log in to the system within the specified period, this user is non-compliant.
vpc-sg-restricted-ssh	vpc	If a security group allows all inbound traffic (with the source address set to **0.0.0.0/0** or **::/0**) and opens the TCP 22 port, this security group is noncompliant.

Rule	Cloud Service	Description
kms-not-scheduled-for-deletion	kms	If a KMS key is scheduled for deletion, this key is noncompliant.
mfa-enabled-for-iam-console-access	iam	If an IAM user who is allowed to access Huawei Cloud console does not have MFA enabled, this IAM user is noncompliant.
rds-instance-logging-enabled	rds	If an RDS instance does not have the collection of any types of logs enabled, this instance is noncompliant.
vpc-sg-restricted-common-ports	vpc	If a security group allows all IPv4 and IPv6 traffic (with the source address set to **0.0.0.0/0** or **::/0**) to the specified ports, this security group is noncompliant.
root-account-mfa-enabled	iam	If the root user does not have MFA enabled, this root user is noncompliant.
vpc-default-sg-closed	vpc	If a default security group allows all inbound or outbound traffic, this security group is noncompliant.
vpc-sg-ports-check	vpc	If a security group has the source address set to **0.0.0.0/0** or **::/0** and opens all TCP/UDP ports, this security group is noncompliant.

4.5.42 Conformance Package for Huawei Cloud Security Configuration Guide (Level 1)

This section describes the background, applicable scenarios, and the conformance package to meet requirements of Huawei Cloud Security Configuration Guide at level 1.

Applicable Scenario

Huawei Cloud Security Configuration Guide provides you with baseline configuration guidance for important cloud services. For more details, see **Security**.

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 **Huawei Cloud Security Configuration Guide**.

Table 4-49 Rules in the conformance package

Guideline No.	Guideline Description	Rule	Cloud Service	Description
C.CS.FOUNDATION.G_1.R_1	Ensuring that AK/SK are disabled for Administrator Account	iam-root-access-key-check	iam	If the account root user has an available access key, the account is noncompliant.
C.CS.FOUNDATION.G_1.R_2	Enabling MFA for the administrator account	root-account-mfa-enabled	iam	If the root user does not have MFA enabled, this root user is noncompliant.
C.CS.FOUNDATION.G_1.R_14	Ensuring that no iam policy is created to allow the ***:*** permissions	iam-policy-no-statements-with-admin-access	iam	If a custom policy or role allows all actions (with the action element set to ***:*:***, ***:***, or *****) for all cloud services, this policy or role is noncompliant.
C.CS.FOUNDATION.G_2.R_1	Enabling CTS	multi-region-cts-tracker-exists	cts	If there are no enabled CTS trackers in any of the specified regions, the current account is noncompliant.
C.CS.FOUNDATION.G_2.R_15	Enabling log file integrity verification	cts-support-validate-check	cts	If a CTS tracker does not have trace file verification enabled, this tacker is noncompliant.

Guideline No.	Guideline Description	Rule	Cloud Service	Description
C.CS.FOUNDATION.G_3_3.R_1	Disabling the kubernetes cluster versions that has reached EOS	cce-cluster-end-of-maintenance-version	cce	If the version of a CCE cluster is no longer supported for maintenance, this cluster is noncompliant.
C.CS.FOUNDATION.G_3_3.R_6	Preventing cluster nodes from being exposed to public networks	cce-endpoint-public-access	cce	If a CCE cluster has an EIP attached, this CCE cluster is noncompliant.
C.CS.FOUNDATION.G_4.R_1	Disabling internet access over SSH	vpc-sg-restricted-ssh	vpc	If a security group allows all inbound traffic (with the source address set to **0.0.0.0/0** or **::/0**) and opens the TCP 22 port, this security group is noncompliant.
C.CS.FOUNDATION.G_4.R_4	Disabling access to remote management ports and high-risk ports over the source IP address 0.0.0.0/0 for security groups	vpc-sg-restricted-common-ports	vpc	If a security group allows all IPv4 and IPv6 traffic (with the source address set to **0.0.0.0/0** or **::/0**) to the specified ports, this security group is noncompliant.
C.CS.FOUNDATION.G_5_1.R_2	Disabling anonymous access	obs-bucket-policy-not-more-permissive	obs	If an OBS bucket has a policy that allows more permissions than the specified policy, this bucket is noncompliant.

Guideline No.	Guideline Description	Rule	Cloud Service	Description
C.CS.FOUNDATION.G_5_1.R_5	Using bucket policies to restrict access to obs buckets using HTTPS	obs-bucket-ssl-requests-only	obs	If an OBS bucket allows HTTP requests, this bucket is noncompliant.
C.CS.FOUNDATION.G_6_1.R_1	Enabling encrypted communication	rds-instance-ssl-enable	rds	If SSL is not enabled for an RDS instance, this instance is noncompliant.
C.CS.FOUNDATION.G_6_1.R_5	Do not bind an eip to access rds for mysql through internet	rds-instance-no-public-ip	rds	If an RDS instance has an EIP attached, this RDS instance is noncompliant.
C.CS.FOUNDATION.G_6_2.R_1	Enabling encrypted communication	dds-instance-enable-ssl	dds	If SSL is not enabled for a DDS instance, this instance is noncompliant.
C.CS.FOUNDATION.G_6_2.R_7	Do not use the default port	dds-instance-port-check	dds	If a DDS instance has unallowed ports enabled, this instance is noncompliant.
C.CS.FOUNDATION.G_6_2.R_8	Patch upgrade	dds-instance-engine-version-check	dds	If the version of a DDS instance is earlier than the specified version, this instance is noncompliant.
C.CS.FOUNDATION.G_6_3.R_2	Enabling the backup function and configuring a backup policy	rds-instance-enable-backup	rds	If backup is not enabled for an RDS instance, this instance is noncompliant.
C.CS.FOUNDATION.G_6_3.R_4	Do not use the default port	rds-instance-port-check	rds	If an RDS instance has unallowed ports enabled, this instance is noncompliant.

Guideline No.	Guideline Description	Rule	Cloud Service	Description
C.CS.FOUNDATION.G_6_3.R_8	Update the database version to the latest version	rds-instance-engine-version-check	rds	If the version of an RDS instance engine is earlier than the specified version, this instance is noncompliant.
C.CS.FOUNDATION.G_7_2.R_1	Enabling kerberos authentication	mrs-cluster-kerberos-enabled	mrs	If an MRS cluster does not have Kerberos authentication enabled, this cluster is noncompliant.
C.CS.FOUNDATION.G_7_2.R_3	EIP security group management and control	mrs-cluster-no-public-ip	mrs	If an MRS cluster has an EIP attached, this cluster is noncompliant.
C.CS.FOUNDATION.G_7_2.R_3	EIP security group management and control	mrs-cluster-in-vpc	mrs	If an MRS cluster is not in the specified VPC, this cluster is noncompliant.
C.CS.FOUNDATION.G_7_3.R_6	Enabling SSL encrypted transmission	dws-enable-ssl	dws	If SSL is not enabled for a DWS cluster, this cluster is noncompliant.
C.CS.FOUNDATION.G_8.R_1	Enabling WAF	waf-instance-enable-protect	waf	If domain name protection is not enabled for a WAF instance, this instance is noncompliant.
C.CS.FOUNDATION.G_8.R_2	Configuring a geolocation access rule in WAF	waf-policy-enable-geoip	waf	If there is a WAF protection policy that does not have geolocation access control configured or enabled, the current account is noncompliant.
C.CS.FOUNDATION.G_8.R_5	Enabling WAF basic web protection block mode	waf-instance-enable-block-policy	waf	If a WAF instance does not have a block policy associated, this instance is noncompliant.

Guideline No.	Guideline Description	Rule	Cloud Service	Description
C.CS.FOUNDATION.G_8.R_7	Enabling HSS (basic/professional/enterprise/premium edition)	ecs-attached-hss-agents-check	ecs	If an ECS does not have an HSS agent installed or the protection mode enabled, this ECS is noncompliant.

4.5.43 Conformance Package for Huawei Cloud Security Configuration Guide (Level 2)

This section describes the background, applicable scenarios, and the conformance package to meet requirements of Huawei Cloud Security Configuration Guide at level 2.

Applicable Scenario

Huawei Cloud Security Configuration Guide provides you with baseline configuration guidance for important cloud services. For more details, see **Security**.

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 **Huawei Cloud Security Configuration Guide**.

Table 4-50 Rules in the conformance package

Guideline No.	Guideline Description	Rule	Cloud Service	Description
C.CS.FOUNDATION.G_1.R_3	Ensuring that no IAM users created in admin user group	iam-user-check-non-admin-group	iam	If a non-root user was added to the **admin** user group, this user is noncompliant.

Guideline No.	Guideline Description	Rule	Cloud Service	Description
C.CS.FOUNDATION.G_1.R_9	Enabling login protection	iam-user-login-protection-enabled	iam	If login protection is not enabled for an IAM user, this user is noncompliant.
C.CS.FOUNDATION.G_1.R_12	Avoiding setting access keys for users with console passwords when setting initial iam users	iam-user-console-and-api-access-at-creation	iam	If an IAM user can access the Huawei Cloud console and has AK/SK that was created when the IAM user was created, this user is noncompliant.
C.CS.FOUNDATION.G_1.R_13	Ensuring that only one active access key is available for an IAM user	iam-user-single-access-key	iam	If multiple access keys are in the active state for an IAM user, this user is noncompliant.
C.CS.FOUNDATION.G_2.R_5	Enabling VPC flow logs	vpc-flow-logs-enabled	vpc	If a VPC does not have the flow log enabled, this VPC is noncompliant.
C.CS.FOUNDATION.G_2.R_11	Enabling FunctionGraph logging	function-graph-logging-enabled	fgs	If a function does not have log collection enabled, this function is noncompliant.
C.CS.FOUNDATION.G_2.R_16	Enabling encrypted storage of log files	cts-kms-encrypted-check	cts	If a CTS tracker does not have KMS encryption enabled, this tracker is noncompliant.
C.CS.FOUNDATION.G_3_1.R_1	Using a key pair to securely log in to an ECS	ecs-instance-key-pair-login	ecs	If key pair authentication is not required for ECS logging, this ECS is noncompliant.
C.CS.FOUNDATION.G_3_1.R_4	Enabling encryption for private images	ims-images-enable-encryption	ims	If a private image does not have encryption enabled, this image is noncompliant.

Guideline No.	Guideline Description	Rule	Cloud Service	Description
C.CS.FOUNDATION.G_3_2.R_1	Using a key pair to securely log in to BMS	bms-key-pair-security-login	bms	If a BMS does not have key pair login enabled, this BMS is noncompliant.
C.CS.FOUNDATION.G_5_1.R_4	Controlling permissions of OBS resources using both VPC endpoint and OBS bucket policies	obs-bucket-policy-grantee-check	obs	If an OBS bucket has a policy that allows access from an object that is not one of the specified ones, this bucket is noncompliant.
C.CS.FOUNDATION.G_5_2.R_1	Ensuring that EVS encryption is enabled	volumes-encrypted-check	ecs, evs	If a mounted EVS disk is not encrypted, this disk is noncompliant.
C.CS.FOUNDATION.G_5_3.R_1	Ensuring that the SFS Turbo file system encryption is enabled	sfsturbo-encrypted-check	sfsturbo	If KMS encryption is not enabled for an SFS Turbo file system, this file system is noncompliant.
C.CS.FOUNDATION.G_5_4.R_1	Selecting an encryption disk for EVS that carries the backup data	cbr-backup-encrypted-check	cbr	If a CBR backup is not encrypted, this backup is noncompliant.
C.CS.FOUNDATION.G_5_4.R_4	Enabling forcible backup	ecs-protected-by-cbr	cbr, ecs	If an ECS does not have a backup vault attached, this ECS is noncompliant.
C.CS.FOUNDATION.G_5_4.R_4	Enabling forcible backup	evs-protected-by-cbr	cbr, evs	If an EVS disk does not have a backup vault attached, this disk is noncompliant.
C.CS.FOUNDATION.G_5_4.R_4	Enabling forcible backup	sfsturbo-protected-by-cbr	cbr, sfsturbo	Checks whether an SFS Turbo system has a backup vault attached. If no, the system is considered non-compliant.

Guideline No.	Guideline Description	Rule	Cloud Service	Description
C.CS.FOUNDATION.G_6_1.R_7	Enabling the database audit logs	rds-instance-enable-auditLog	rds	If an RDS instance does not have the audit log enabled or has audit logs kept for less than the specified number of days, this instance is noncompliant.
C.CS.FOUNDATION.G_6_4.R_5	Enabling the database audit logs	gaussdb-instance-enable-auditLog	gaussdb	If a GaussDB instance does not have audit log collection enabled, this instance is noncompliant.
C.CS.FOUNDATION.G_6_4.R_5	Enabling the database audit logs	gaussdb-mysql-instance-enable-auditlog	taurusdb	If a TaurusDB instance does not have audit log collection enabled, this instance is noncompliant.
C.CS.FOUNDATION.G_6_4.R_7	Enabling the backup function and configuring a backup policy	gaussdb-instance-enable-backup	gaussdb	If a GaussDB instance does not have the backup enabled, this instance is noncompliant.
C.CS.FOUNDATION.G_7_3.R_1	Enabling cluster data encryption	dws-enable-kms	dws	If KMS encryption is not enabled for a DWS cluster, this cluster is noncompliant.
C.CS.FOUNDATION.G_7_3.R_4	Enabling Audit Log Dumping for a DWS Database	dws-enable-log-dump	dws	If a DWS cluster does not have log transfer enabled, this cluster is noncompliant.

4.5.44 Best Practices for Static Data Encryption

The following table lists the rules and solutions included in this conformance package template.

Table 4-51 Conformance package description

Rule	Cloud Service	Description
cbr-backup-encrypted-check	cbr	If a CBR backup is not encrypted, this backup is noncompliant.
css-cluster-disk-encryption-check	css	If disk encryption is not enabled for a CSS cluster, this cluster is noncompliant.
cts-kms-encrypted-check	cts	If a CTS tracker does not have KMS encryption enabled, this tracker is noncompliant.
dws-enable-kms	dws	If KMS encryption is not enabled for a DWS cluster, this cluster is noncompliant.
gaussdb-nosql-enable-disk-encryption	gemini db	If a GeminiDB instance does not have disk encryption enabled, this instance is noncompliant.
ims-images-enable-encryption	ims	If a private image does not have encryption enabled, this image is noncompliant.
kms-rotation-enabled	kms	If key rotation is not enabled for a KMS key, this key is noncompliant.
mrs-cluster-encrypt-enable	mrs	If KMS encryption is not enabled for an MRS cluster, this cluster is noncompliant.
rds-instances-enable-kms	rds	If KMS encryption is not enabled for an RDS instance, this instance is noncompliant.
sfsturbo-encrypted-check	sfsturbo	If KMS encryption is not enabled for an SFS Turbo file system, this file system is noncompliant.
volumes-encrypted-check	ecs, evs	If a mounted EVS disk is not encrypted, this disk is noncompliant.

4.5.45 Best Practices for Data Transmission Encryption

The following table lists the rules and solutions included in this conformance package template.

Table 4-52 Conformance package description

Rule	Cloud Service	Description
apig-instances-ssl-enabled	apig	If no SSL certificates are attached to a dedicated APIG gateway, this gateway is considered noncompliant.
cdn-enable-https-certificate	cdn	If a domain does not have an HTTPS certificate configured, this domain is noncompliant.
cdn-origin-protocol-no-http	cdn	If a domain does not have HTTPS configured for communication between CDN and origins, this domain is noncompliant.
css-cluster-https-required	css	If a CSS cluster does not have HTTPS enabled, this cluster is noncompliant.
css-cluster-security-mode-enable	css	If a CSS cluster does not support the security mode, this cluster is noncompliant.
dcs-memcached-enable-ssl	dcs	If a DCS Memcached instance can be accessed through public networks but does not support SSL, this instance is noncompliant.
dcs-redis-enable-ssl	dcs	If a DCS Redis instance can be accessed over public networks but does not support SSL, this instance is noncompliant.

Rule	Cloud Service	Description
dds-instance-enable-ssl	dds	If SSL is not enabled for a DDS instance, this instance is noncompliant.
dms-kafka-not-enable-private-ssl	dms	If a DMS Kafka instance does not enable SSL for private access, this instance is noncompliant.
dms-kafka-not-enable-public-ssl	dms	If a DMS Kafka instance does not enable SSL for public access, this instance is noncompliant.
dms-rabbitmq-not-enable-ssl	dms	If a DMS RabbitMQ instance does not have SSL enabled, this instance is noncompliant.
dms-rocketmq-not-enable-ssl	dms	If a DMS RocketMQ instance does not have SSL enabled, this instance is noncompliant.
dws-enable-ssl	dws	If SSL is not enabled for a DWS cluster, this cluster is noncompliant.
elb-http-to-https-redirection-check	elb	If an HTTP listener does not have redirecting requests to an HTTPS listener enabled, this HTTP listener is noncompliant.
elb-tls-https-listeners-only	elb	If any listener of a load balancer does not have the frontend protocol set to HTTPS, this load balancer is noncompliant.
gaussdb-instance-ssl-enable	gaussdb	If a GaussDB instance does not have SSL enabled, this instance is noncompliant.

Rule	Cloud Service	Description
gaussdb-mysql-instance-ssl-enable	taurusdb	If a TaurusDB instance does not have SSL enabled, this instance is noncompliant.
obs-bucket-ssl-requests-only	obs	If an OBS bucket allows HTTP requests, this bucket is noncompliant.
rds-instance-ssl-enable	rds	If SSL is not enabled for an RDS instance, this instance is noncompliant.

4.5.46 Best Practices for Cloud Backup and Recovery

The following table lists the rules and solutions included in this conformance package template.

Table 4-53 Conformance package description

Rule	Cloud Service	Description
cbr-backup-encrypted-check	cbr	If a CBR backup is unencrypted, this backup is noncompliant.
cbr-policy-minimum-frequency-check	cbr	If the execution frequency of a backup policy is lower within the specified frequency, this policy is noncompliant.
cbr-vault-minimum-retention-check	cbr	If a CBR vault has no policies attached or has a policy that is retained for less than the specified period (in days), this vault is noncompliant.
ecs-protected-by-cbr	cbr, ecs	If an ECS does not have a backup vault attached, this ECS is noncompliant.
evs-protected-by-cbr	cbr, evs	If an EVS disk does not have a backup vault attached, this disk is noncompliant.

Rule	Cloud Service	Description
sfsturbo-protected-by-cbr	cbr, sfsturbo	If an SFS Turbo file system does not have a backup vault attached, this file system is noncompliant.
ecs-last-backup-created	cbr, ecs	If an ECS does not have a backup created within the specified period, this ECS is noncompliant.
evs-last-backup-created	cbr, evs	If an EVS disk does not have a backup created within the specified period, this disk is noncompliant.
sfsturbo-last-backup-created	cbr, sfsturbo	If an SFS Turbo system does not have a backup created within the specified period, this system is noncompliant.

4.5.47 Best Practices for Cloud Search Service

The following table lists the rules and solutions included in this conformance package template.

Table 4-54 Conformance package description

Rule	Cloud Service	Description
css-cluster-backup-available	css	If the snapshot function is not enabled for a CSS cluster, this cluster is noncompliant.
css-cluster-disk-encryption-check	css	If disk encryption is not enabled for a CSS cluster, this cluster is noncompliant.
css-cluster-https-required	css	If a CSS cluster does not have HTTPS enabled, this cluster is noncompliant.
css-cluster-not-enable-white-list	css	If a CSS cluster does not have access control enabled, this cluster is noncompliant.

Rule	Cloud Service	Description
css-cluster-kibana-not-enable-white-list	css	If a CSS cluster does not have Kibana access control enabled, this cluster is noncompliant.
css-cluster-multiple-az-check	css	If a CSS cluster is not deployed across AZs, the cluster is noncompliant.
css-cluster-no-public-zone	css	If a CSS cluster can be accessed over a public network, this cluster is noncompliant.
css-cluster-security-mode-enable	css	If a CSS cluster does not support the security mode, this cluster is noncompliant.
css-cluster-slowLog-enable	css	If a CSS cluster has slow query log disabled, this cluster is noncompliant.

4.5.48 Best Practices for Distributed Cache Service

The following table lists the rules and solutions included in this conformance package template.

Table 4-55 Conformance package description

Rule	Cloud Service	Description
dcs-redis-enable-ssl	dcs	If a DCS Redis instance can be accessed over public networks but does not support SSL, this instance is noncompliant.
dcs-redis-high-tolerance	dcs	If a DCS Redis instance does not have cross-AZ deployment enabled, this instance is noncompliant.
dcs-redis-no-public-ip	dcs	If a DCS Redis instance has an EIP associated, this instance is noncompliant.

Rule	Cloud Service	Description
dcs-redis-password-access	dcs	If a DCS Redis instance can be accessed without a password, this instance is noncompliant.

4.5.49 Best Practices for Distributed Message Service

The following table lists the rules and solutions included in this conformance package template.

Table 4-56 Conformance package description

Rule	Cloud Service	Description
dms-kafka-not-enable-private-ssl	dms	If a DMS Kafka instance does not enable SSL for private access, this instance is noncompliant.
dms-kafka-not-enable-public-ssl	dms	If a DMS Kafka instance does not enable SSL for public access, this instance is noncompliant.
dms-kafka-public-access-enabled-check	dms	If a DMS Kafka instance can be accessed over a public network, this instance is noncompliant.
dms-rabbitmq-not-enable-ssl	dms	If a DMS RabbitMQ instance does not have SSL enabled, this instance is noncompliant.
dms-rocketmq-not-enable-ssl	dms	If a DMS RocketMQ instance does not have SSL enabled, this instance is noncompliant.
dms-rabbitmq-public-access-enabled-check	dms	If a DMS RabbitMQ instance has public access enabled, this instance is noncompliant.

Rule	Cloud Service	Description
dms-reliability-public-access-enabled-check	dms	If a DMS RocketMQ instance allows public access, the RocketMQ instance is noncompliant.

4.5.50 Best Practices for Data Warehouse Service

The following table lists the rules and solutions included in this conformance package template.

Table 4-57 Conformance package description

Rule	Cloud Service	Description
dws-clusters-no-public-ip	dws	If a DWS cluster has an EIP attached, this cluster is noncompliant.
dws-enable-kms	dws	If KMS encryption is not enabled for a DWS cluster, this cluster is noncompliant.
dws-enable-ssl	dws	If SSL is not enabled for a DWS cluster, this cluster is noncompliant.
dws-enable-log-dump	dws	If a DWS cluster does not have log transfer enabled, this cluster is noncompliant.
dws-enable-snapshot	dws	If automated snapshots are not enabled for a DWS cluster, this cluster is noncompliant.
dws-maintain-window-check	dws	If the O&M time window of a DWS cluster is not consistent with the specified time window, this cluster is noncompliant.

4.5.51 Best Practices for TaurusDB

The following table lists the rules and solutions included in this conformance package template.

Table 4-58 Conformance package description

Rule	Cloud Service	Description
gaussdb-mysql-instance-enable-auditlog	taurusdb	If a TaurusDB instance does not have audit log collection enabled, this instance is noncompliant.
gaussdb-mysql-instance-enable-backup	taurusdb	If a TaurusDB instance does not have the backup enabled, this instance is noncompliant.
gaussdb-mysql-instance-enable-errorlog	taurusdb	If a TaurusDB instance does not have error log collection enabled, this instance is noncompliant.
gaussdb-mysql-instance-enable-slowlog	taurusdb	If a TaurusDB instance does not have the slow query log enabled, this instance is noncompliant.
gaussdb-mysql-instance-multiple-az-check	taurusdb	If a TaurusDB instance does not allow cross-AZ deployment, this instance is noncompliant.
gaussdb-mysql-instance-no-public-ip-check	taurusdb	If a TaurusDB instance has an EIP associated, this instance is noncompliant.
gaussdb-mysql-instance-ssl-enable	taurusdb	If a TaurusDB instance does not have SSL enabled, this instance is noncompliant.

4.5.52 Best Practices for Object Storage Service

The following table lists the rules and solutions included in this conformance package template.

Table 4-59 Conformance package description

Rule	Cloud Service	Description
obs-bucket-public-read-policy-check	obs	If an OBS bucket allows public read access, this bucket is noncompliant.
obs-bucket-public-write-policy-check	obs	If an OBS bucket allows public read access, this bucket is noncompliant.
obs-bucket-ssl-requests-only	obs	If an OBS bucket allows HTTP requests, this bucket is noncompliant.

4.5.53 Best Practices for Virtual Private Cloud

The following table lists the rules and solutions included in this conformance package template.

Table 4-60 Conformance package description

Rule	Cloud Service	Description
vpc-default-sg-closed	vpc	If a default security group allows all inbound or outbound traffic, this security group is noncompliant.
vpc-sg-attached-ports	vpc	This rule checks if a security group is associated with any elastic network interface. If a security group is not attached to any elastic network interface, this security group is noncompliant.
vpc-sg-ports-check	vpc	If a security group has the source address set to **0.0.0.0/0** or **::/0** and opens all TCP/UDP ports, this security group is noncompliant.

Rule	Cloud Service	Description
vpc-sg-restricted-ssh	vpc	If a security group allows all inbound traffic (with the source address set to **0.0.0.0/0** or **::/0**) and opens the TCP 22 port, this security group is noncompliant.
vpc-sg-by-white-list-ports-check	vpc	If a security group allows traffic to a non-whitelisted port, this security group is noncompliant.

4.5.54 Best Practices for Web Application Firewall

The following table lists the rules and solutions included in this conformance package template.

Table 4-61 Conformance package description

Rule	Cloud Service	Description
waf-instance-enable-block-policy	waf	If a WAF instance does not have a block policy associated, this instance is noncompliant.
waf-instance-enable-protect	waf	If domain name protection is not enabled for a WAF instance, this instance is noncompliant.
waf-instance-policy-not-empty	waf	If a WAF instance does not have a protection policy attached, this instance is noncompliant.
waf-policy-enable-geoip	waf	If there is a WAF protection policy that does not have geolocation access control configured or enabled, the current account is noncompliant.

Rule	Cloud Service	Description
waf-policy-not-empty	waf	If no rules are added for a WAF protection policy, this policy is noncompliant.

5 Advanced Queries

5.1 Overview

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

You can conveniently use ResourceQL and a query editor to search for and view your resources.

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 check if the configurations (public IPs attached or disks encrypted) of your resources meet security requirements.
- Optimize costs. For example, you can list all EVS disks that have not been attached to any ECS to avoid unnecessary expenditures.

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.

5.2 Restrictions

To prevent a single user from occupying resources for queries for too long, the following constraints are set on advanced queries:

- If the execution duration of a query statement exceeds 15 seconds, a timeout error will be returned.
- If the result set to be returned exceeds the size limit, an error will occur. Make sure that the data volume returned by each statement is within the size limit.

- Up to 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.

NOTICE

To get full functionality of advanced queries, you need to enable the resource recorder. The following describes how the resource recorder may affect your use of advanced queries.

- If you have never enabled the resource recorder, no resources can be queried with an advanced query.
- If you have enabled the resource recorder and a monitoring scope is specified, only resources within the monitoring scope can be queried with an advanced query.
- If you enable the resource recorder and disable it after a period of time, only resource data collected during the period when the resource recorder was enabled can be queried with an advanced query.

For details about how to enable and configure the resource recorder, see **Configuring the Resource Recorder**.

5.3 Creating a Custom 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.

This section includes the following content:

- **Creating a Custom Query**
- **Using a Predefined Query**
- **Configuration Examples of Advanced Queries**

Creating a Custom Query

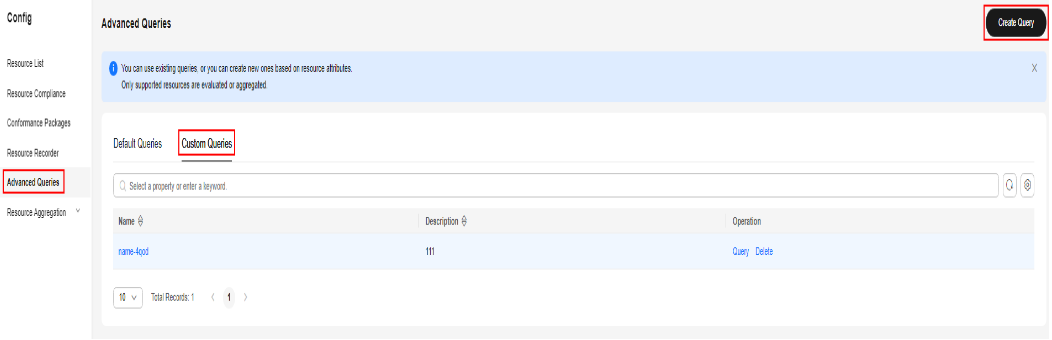
Step 1 Log in to the management console.

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

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

Step 4 Choose the **Custom Queries** tab and click **Create Query** in the upper right corner.

Figure 5-1 Creating a query



You can use existing queries, or you can create new ones based on resource attributes.
Only supported resources are evaluated or aggregated.

Name	Description	Operation
name-4qod	111	Query Delete

Step 5 In the **Query Editor**, enter the query statements.

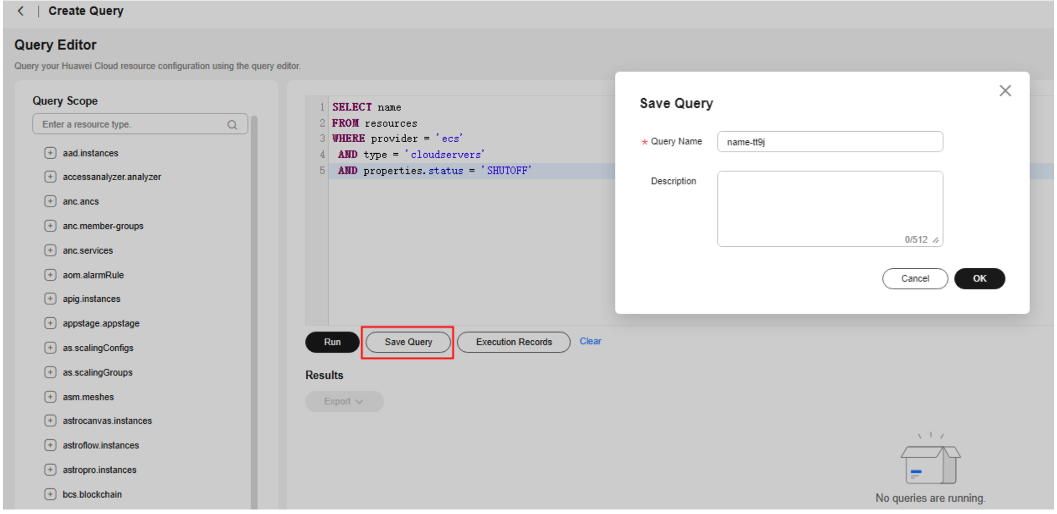
On the left of the page, the Schema information is displayed. Schema information shows detailed resource attributes that are specified by the **properties** parameter in the statement. For details about query statements, see **Configuration Examples of Advanced Queries**.

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

A query name can contain only digits, letters, underscores (_), and hyphens (-). It cannot exceed 64 characters.

Step 7 Click **OK**.

Figure 5-2 Save Query



Query your Huawei Cloud resource configuration using the query editor.

```
SELECT name
FROM resources
WHERE provider = 'ecs'
 AND type = 'cloudservers'
 AND properties.status = 'SHUTOFF'
```

* Query Name: name-tt9j
Description: 0/512

NOTE

There is a limit to how many custom queries you can create. If you exceed this limit, you will receive a notification: "The maximum number of custom queries has been reached." Although the query cannot be saved, you can still run the query and export the results.

Step 8 Click **Run** and then view the query results. Up to 4,000 query results can be displayed and exported.

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

Step 10 Click **Execution Records** to view details about when the query was executed and the query statements.

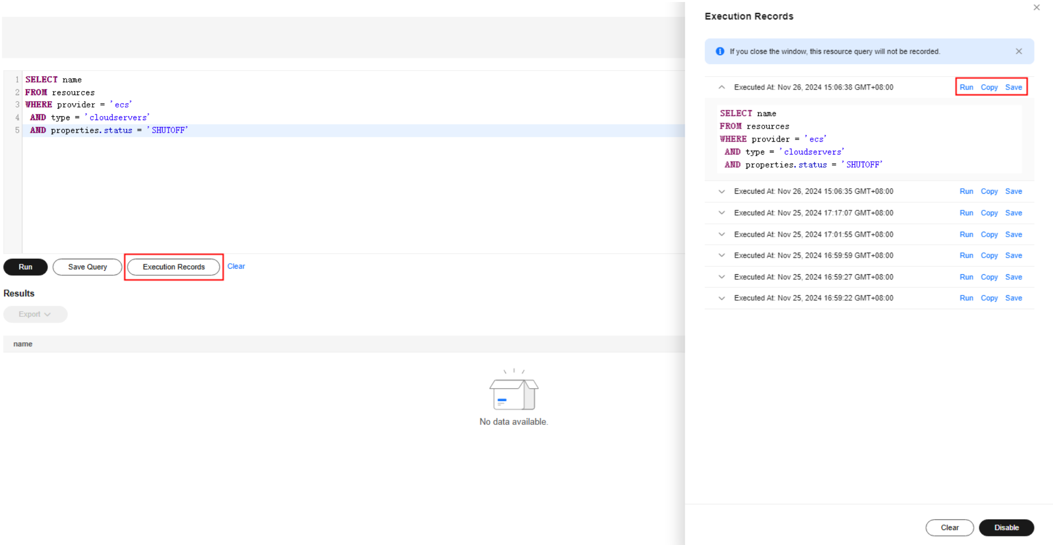
You can perform the following operations:

- **Run**: running the query
- **Copy**: copying the query statements
- **Save**: saving the query as a new query

NOTE

After you close the browser window or log out, the execution records of advanced queries will be cleared.

Figure 5-3 Execution records



```
SELECT name
FROM resources
WHERE provider = 'ecs'
 AND type = 'cloudservers'
 AND properties.status = 'SHUTOFF'
```

If you close the window, this resource query will not be recorded.

Executed At: Nov 26, 2024 15:06:38 GMT+08:00 Run Copy Save

```
SELECT name
FROM resources
WHERE provider = 'ecs'
 AND type = 'cloudservers'
 AND properties.status = 'SHUTOFF'
```

Executed At: Nov 26, 2024 15:06:35 GMT+08:00 Run Copy Save

Executed At: Nov 25, 2024 17:17:07 GMT+08:00 Run Copy Save

Executed At: Nov 25, 2024 17:01:55 GMT+08:00 Run Copy Save

Executed At: Nov 25, 2024 16:59:59 GMT+08:00 Run Copy Save

Executed At: Nov 25, 2024 16:59:27 GMT+08:00 Run Copy Save

Executed At: Nov 25, 2024 16:59:22 GMT+08:00 Run Copy Save

----End

Using a Predefined Query

You can modify the name, description, and statement of a default query or a custom query and save it as a new query. The following procedure uses a default query as an example.

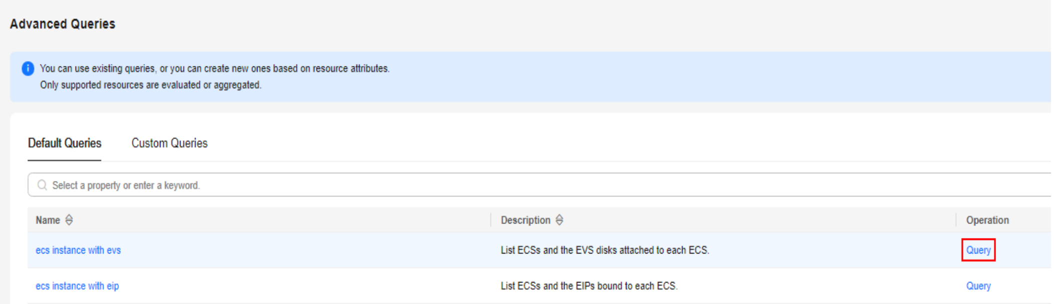
Step 1 Choose **Advanced Queries** > **Default Queries**.

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 5-4 Default queries



Advanced Queries

You can use existing queries, or you can create new ones based on resource attributes.
Only supported resources are evaluated or aggregated.

Name	Description	Operation
ecs instance with evs	List ECSs and the EVS disks attached to each ECS.	Query
ecs instance with eip	List ECSs and the EIPs bound to each ECS.	Query

Step 3 In the **Query Editor**, modify the query.

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

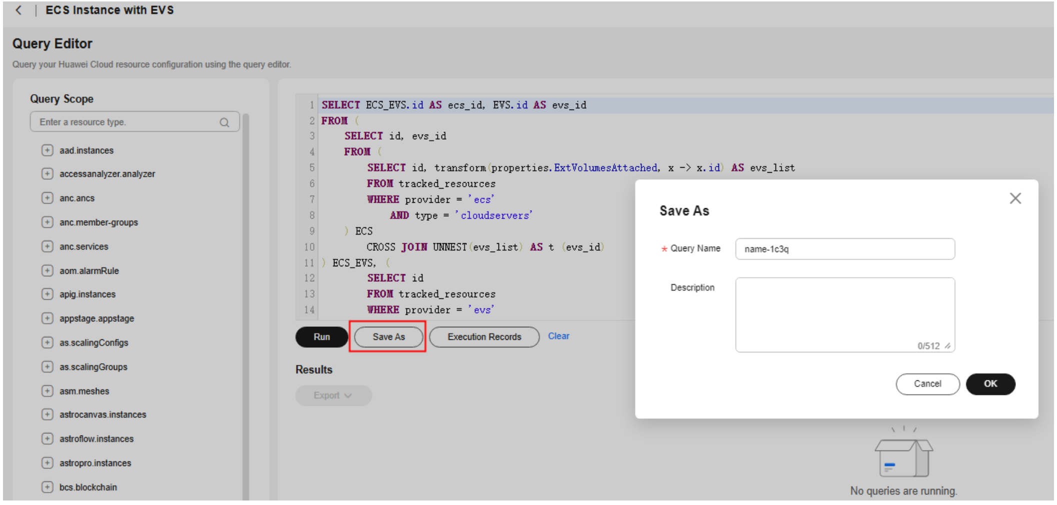
Step 4 Click **Save As** and enter the query name and description.

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

After a new query is created, the new query becomes a custom query and will be displayed in the custom query list.

On the **Execution Records** page, you can also save an existing query as a new query. For details, see **Step 10**.

Figure 5-5 Saving a default query as a new query



```
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 tracked_resources
        WHERE provider = 'ecs'
            AND type = 'cloudservers'
    ) ECS
        CROSS JOIN UNNEST(evs_list) AS t (evs_id)
) ECS_EVS, (
        SELECT id
        FROM tracked_resources
        WHERE provider = 'evs'
```

* Query Name: name-1c3q

Description: 0/512

----End

Configuration Examples of Advanced Queries

Advanced queries use 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.
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.

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 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 **Advanced Queries**.

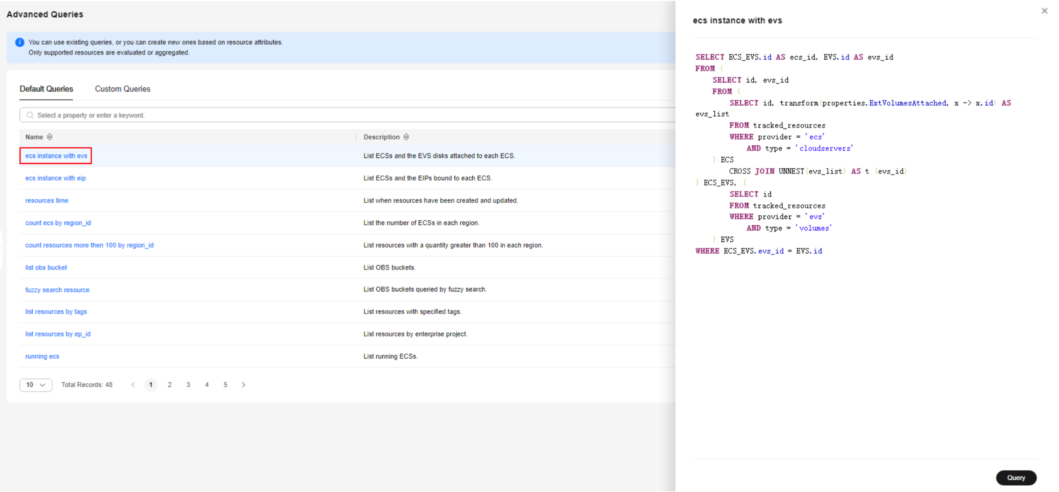
By default, the default query list is displayed. To view custom queries, click **Custom Queries**.

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 5-6 Viewing query details



Advanced Queries

You can use existing queries, or you can create new ones based on resource attributes.
Only supported resources are evaluated or aggregated.

Name	Description
ecs instance with evs	List ECSs and the EVS disks attached to each ECS.
ecs instance with eip	List ECSs and the EIPs bound to each ECS.
resources time	List when resources have been created and updated.
count ecs by region_id	List the number of ECSs in each region.
count resources more then 100 by region_id	List resources with a quantity greater than 100 in each region.
list obs bucket	List OBS buckets.
fuzzy search resource	List OBS buckets queried by fuzzy search.
list resources by tags	List resources with specified tags.
list resources by ep_id	List resources by enterprise project.
running ecs	List running ECSs.

ecs instance with evs

```
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 tracked_resources
        WHERE provider = 'ecs'
            AND type = 'cloudservers'
    ) ECS
        CROSS JOIN UNNEST(evs_list) AS t (evs_id)
) ECS_EVS, (
        SELECT id
        FROM tracked_resources
        WHERE provider = 'evs'
            AND type = 'volumes'
    ) EVS
WHERE ECS_EVS.evs_id = EVS.id
```

----End

5.5 Modifying a Custom Query

Scenarios

You can perform the following procedure to modify the statement, name, and description of a custom query.

NOTE

You can modify the statement, name, and description of a predefined query and save it as a new custom query. For details, see **Using a Predefined Query**.

Procedure

Step 1 Log in to the management console.

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

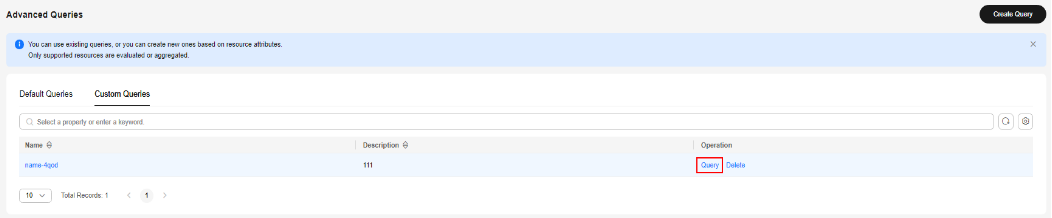
Step 3 In the navigation pane on the left, choose **Advanced Queries**.

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 Editor** page.

Figure 5-7 Modifying a custom query



You can use existing queries, or you can create new ones based on resource attributes.
Only supported resources are evaluated or aggregated.

Name	Description	Operation
name-4qod	111	Query Delete

Step 6 In the **Query Editor**, modify the query.

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

Step 7 Click **Save**.

Step 8 In the displayed dialog box, modify the query name and description and click **OK**.

A query name can contain only digits, letters, underscores (_), and hyphens (-). It cannot exceed 64 characters.

----End

5.6 Deleting a Query

Scenarios

You can delete a custom query if you no longer need it.

NOTE

Default queries cannot be deleted.

Procedure

Step 1 Log in to the management console.

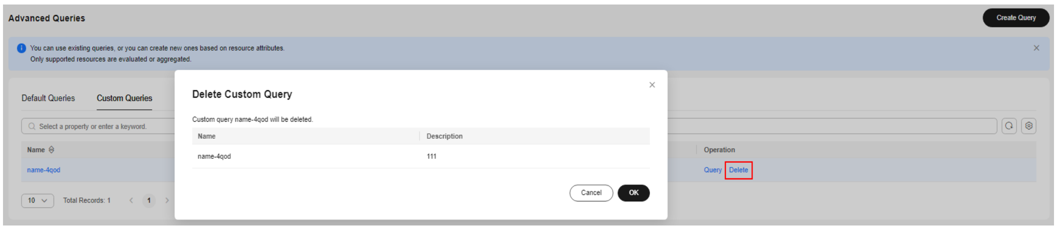
Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

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

Step 4 Click **Custom Queries**.

Step 5 Locate the custom query to be deleted and click **Delete** in the **Operation** column.

Figure 5-8 Deleting a custom query



You can use existing queries, or you can create new ones based on resource attributes.
Only supported resources are evaluated or aggregated.

Delete Custom Query

Custom query name-4qod will be deleted.

Name	Description
name-4qod	111

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 for centralized data query.

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 snapshots from a source account.

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.

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 aggregated. 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 an 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

An aggregator account must gain authorization from source accounts for data collection. An organization aggregator, however, does not need authorization to collect data from members.

6.2 Restrictions

The following lists aggregator constraints:

- 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 every 7 days.
- Up to 1 organization specific aggregator can be created in an account.
- You can only create one organization within 24 hours. If you create and then delete an organization aggregator, creating an organization aggregator will not be supported within 24 hours of the creation.
- To aggregate data from source accounts, the resource recorder in each source account must be enabled. The following lists more detailed information:
- Organization aggregator will only aggregate data from member accounts that are in the normal state.

NOTICE

The following provides more detailed information:

- If the resource recorder in a source account has not been enabled, neither resource nor compliance data can be aggregated.
- If a monitoring scope has been configured in a source account, only related data of the resources within the specified scope will be aggregated.
- If the resource recorder in a source account is enabled and then disabled, data aggregated from the source account will be deleted after the resource recorder is disabled.

For details about how to enable and configure the resource recorder, see **Configuring the Resource Recorder**.

6.3 Creating a Resource Aggregator

Scenarios

You can create an account specific or organization specific aggregator.

To aggregate data from a source account, an account aggregator must obtain related authorization. For details, see **Authorizing a Resource Aggregator Account**.

NOTE

To create an organization aggregator, you need the following permissions for Organizations:

- organizations:organizations:get
- organizations:accounts:list
- organizations:delegatedAdministrators:list
- organizations:trustedServices:enable
- organizations:trustedServices:list

Procedure

Step 1 Log in to the management console.

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

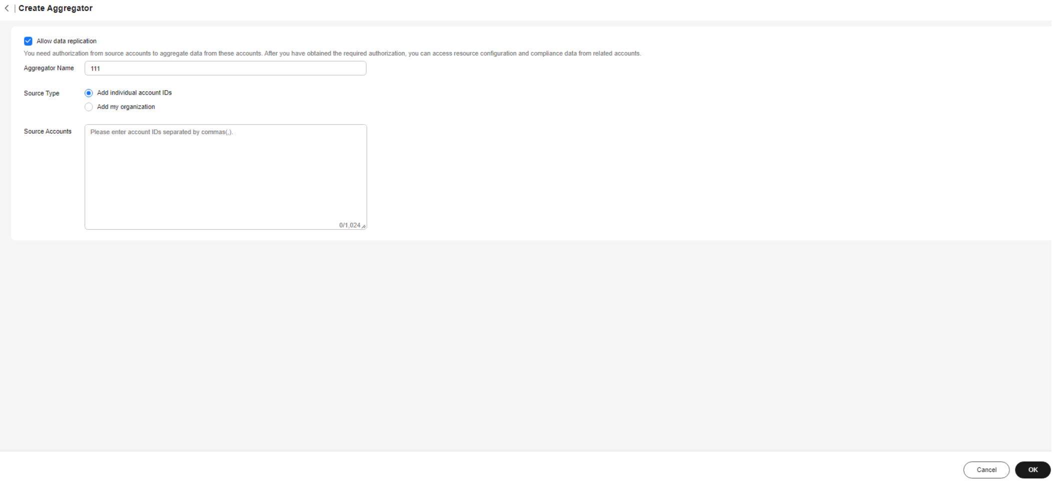
Step 3 In the navigation pane on the left, choose **Resource Aggregation** > **Aggregators**.

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 account IDs and separate them with commas (,). If you select **Add my organization**, the resource aggregator automatically aggregates data from all member accounts that are in the normal state in the organization.

Figure 6-1 Create Aggregator



Create Aggregator

☑ Allow data replication

You need authorization from source accounts to aggregate data from these accounts. After you have obtained the required authorization, you can access resource configuration and compliance data from related accounts.

Aggregator Name: 111

Source Type: ● Add individual account IDs ○ Add my organization

Source Accounts: Please enter account IDs separated by commas(,). 0/1,024

NOTE

- An account specific aggregator can only aggregate data from accounts, so source account IDs must be specified. For details about how to obtain an account ID, see **Obtaining Account, IAM User, Group, Project, Region, and Agency Information**.
- 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.

NOTE

To view resource and compliance data aggregated by an organization aggregator, you need the following permissions:

- organizations:organizations:get
- organizations:delegatedAdministrators:list
- organizations:trustedServices: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 In the navigation pane on the left, 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.

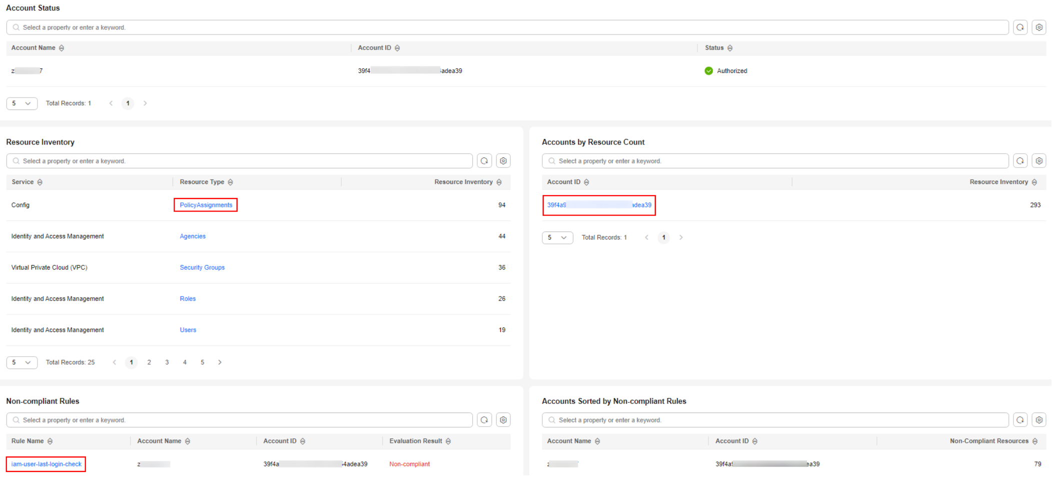
Step 5 Locate the aggregator you want to view and click its name.

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 **Non-compliant Rules** area to view details of this rule.

Figure 6-2 Resource aggregator details page



Account Status

Select a property or enter a keyword.

Account Name	Account ID	Status
z[redacted]7	39f4[redacted]adea39	✓ Authorized

5 Total Records: 1 < 1 >

Resource Inventory

Select a property or enter a keyword.

Service	Resource Type	Resource Inventory
Config	PolicyAssignments	94
Identity and Access Management	Agencies	44
Virtual Private Cloud (VPC)	Security Groups	36
Identity and Access Management	Roles	26
Identity and Access Management	Users	19

5 Total Records: 25 < 1 2 3 4 5 >

Accounts by Resource Count

Select a property or enter a keyword.

Account ID	Resource Inventory
39f4a9[redacted]adea39	293

5 Total Records: 1 < 1 >

Non-compliant Rules

Select a property or enter a keyword.

Rule Name	Account Name	Account ID	Evaluation Result
iam-user-last-login-check	z[redacted]	39f4a[redacted]4adea39	Non-compliant

Accounts Sorted by Non-compliant Rules

Select a property or enter a keyword.

Account Name	Account ID	Non-Compliant Resources
z[redacted]	39f4a[redacted]a39	79

----End

6.5 Modifying an Aggregator

Scenarios

You can modify the name and source accounts for an account aggregator at any time. However, you can only modify the name rather than source accounts for an organization aggregator.

The following procedure describes how to modify an account aggregator.

NOTE

To modify configurations of an organization aggregator, you need the following permissions:

- organizations:organizations:get
- organizations:accounts:list
- organizations:delegatedAdministrators:list
- organizations:trustedServices:enable
- organizations:trustedServices:list

Procedure

Step 1 Log in to the management console.

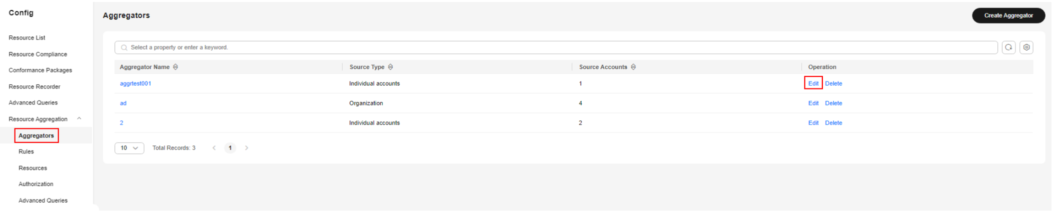
Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

Step 3 In the navigation pane on the left, 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 Modifying an aggregator



Aggregator Name	Source Type	Source Accounts	Operation
aggrtest001	Individual accounts	1	Edit Delete
ad	Organization	4	Edit Delete
2	Individual accounts	2	Edit Delete

Step 5 On the **Edit Aggregator** page, edit the name and 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 Log in to the management console.

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

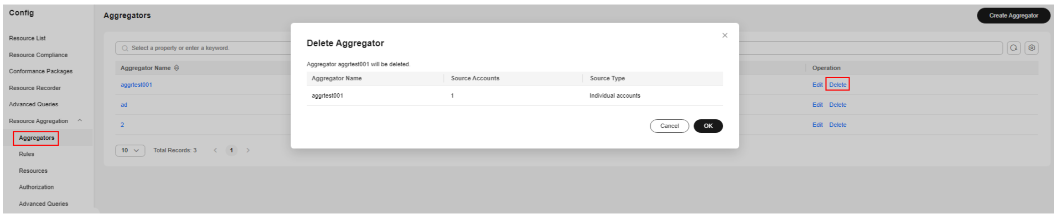
Step 3 In the navigation pane on the left, choose **Resource Aggregation** > **Aggregators**.

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 6-4 Delete Aggregator



Delete Aggregator

Aggregator aggrtest001 will be deleted.

Aggregator Name	Source Accounts	Source Type
aggrtest001	1	Individual accounts

----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.

NOTE

To view compliance data aggregated by an organization aggregator, you need the following permissions:

- organizations:organizations:get
- organizations:delegatedAdministrators:list
- organizations:trustedServices:list

Procedure

Step 1 Log in to the management console.

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

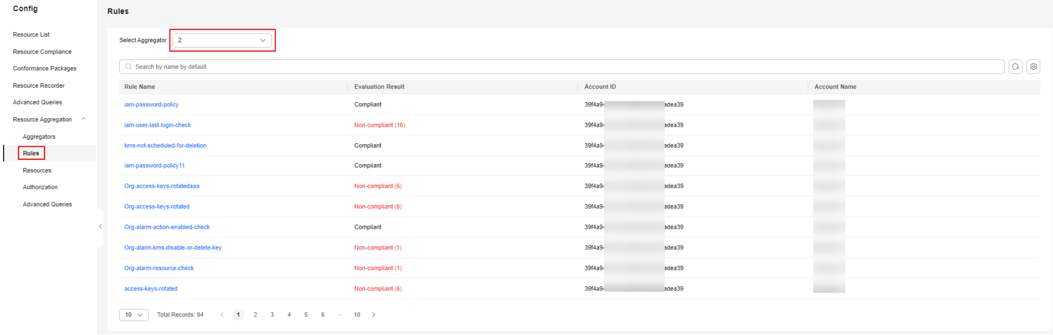
Step 3 On the left navigation, choose **Resource Aggregation** > **Rules**.

Step 4 In the upper right corner, select an aggregator from the drop-down list.

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 an account ID to filter compliance data.

Figure 6-5 Viewing aggregated rules



Select Aggregator 2

Search by name by default.

Rule Name	Evaluation Result	Account ID	Account Name
iam-password-policy	Compliant	39f4a9-[redacted]adea39	[redacted]
iam-user-last-login-check	Non-compliant (16)	39f4a9-[redacted]adea39	[redacted]
kms-not-scheduled-for-deletion	Compliant	39f4a9-[redacted]adea39	[redacted]
iam-password-policy11	Compliant	39f4a9-[redacted]adea39	[redacted]
Org-access-keys-rotatedaaa	Non-compliant (6)	39f4a9-[redacted]adea39	[redacted]
Org-access-keys-rotated	Non-compliant (6)	39f4a9-[redacted]adea39	[redacted]
Org-alarm-action-enabled-check	Compliant	39f4a9-[redacted]adea39	[redacted]
Org-alarm-kms-disable-or-delete-key	Non-compliant (1)	39f4a9-[redacted]adea39	[redacted]
Org-alarm-resource-check	Non-compliant (1)	39f4a9-[redacted]adea39	[redacted]
access-keys-rotated	Non-compliant (6)	39f4a9-[redacted]adea39	[redacted]

10 Total Records: 94 < 1 2 3 4 5 6 ··· 10 >

----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.

NOTE

To view resource data aggregated by an organization aggregator, you need the following permissions:

- organizations:organizations:get
- organizations:delegatedAdministrators:list
- organizations:trustedServices:list

Procedure

Step 1 Log in to the management console.

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

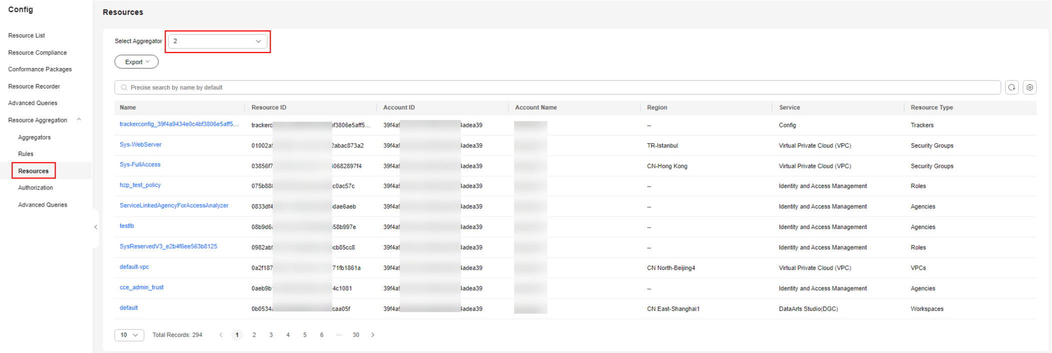
Step 3 In the navigation pane, choose **Resource Aggregation** > **Resources**.

Step 4 In the upper left corner of the page, select a resource aggregator to be viewed. All resources aggregated by this aggregator will be displayed in a list. You can export all resource data.

In the search box above the list, enter the name, ID, or type of a resource to filter resource data.

In the resource list, click a target resource name to view resource details.

Figure 6-6 Viewing aggregated resources



Resources

Select Aggregator 2

Name	Resource ID	Account ID	Account Name	Region	Service	Resource Type
trackerconfig_39f4a9434e0c4bf3806e5aff5...	trackerc[redacted]f3806e5aff5...	39f4a[redacted]adea39	[redacted]	--	Config	Trackers
Sys-WebServer	01002a[redacted]2abac873a2	39f4a[redacted]adea39	[redacted]	TR-Istanbul	Virtual Private Cloud (VPC)	Security Groups
Sys-FullAccess	03856f7[redacted]0682897f4	39f4a[redacted]adea39	[redacted]	CN-Hong Kong	Virtual Private Cloud (VPC)	Security Groups
hzp_test_policy	075b88[redacted]c0ac57c	39f4a[redacted]adea39	[redacted]	--	Identity and Access Management	Roles
ServiceLinkedAgencyForAccessAnalyzer	0833df4[redacted]dae6aeb	39f4a[redacted]adea39	[redacted]	--	Identity and Access Management	Agencies
testlb	08b9d6[redacted]58b997e	39f4a[redacted]adea39	[redacted]	--	Identity and Access Management	Agencies
SysReservedV3_e2b4f6ee563b8125	0982ab[redacted]cb85cc8	39f4a[redacted]adea39	[redacted]	--	Identity and Access Management	Roles
default-vpc	0a2f187[redacted]71fb1861a	39f4a[redacted]adea39	[redacted]	CN North-Beijing4	Virtual Private Cloud (VPC)	VPCs
cce_admin_trust	0aeb9b[redacted]4c1081	39f4a[redacted]adea39	[redacted]	--	Identity and Access Management	Agencies
default	0b0534[redacted]caa05f	39f4a[redacted]adea39	[redacted]	CN East-Shanghai1	DataArts Studio(DGC)	Workspaces

10 Total Records: 294 < 1 2 3 4 5 6 ··· 30 >

----End

6.9 Authorizing an Aggregator Account

Scenarios

To aggregate data from a source account, an aggregator account must obtain authorization from this source account. After the authorization, all aggregators created before or after the authorization with this aggregator account can aggregate data from this source account.

An organization specific aggregator can collect resource data of all member accounts in an organization without source account authorization.

This section describes the following topics:

- Adding Authorization
- Accepting Authorization
- Deleting an Authorization

Adding Authorization

You can use the **Add Authorization** function to authorize an aggregator account.

Step 1 Log in to the management console.

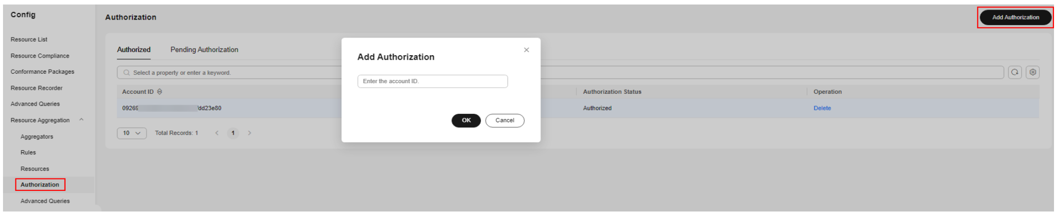
Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

Step 3 In the navigation pane on the left, choose **Resource 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 6-7 Adding authorization



Add Authorization

Enter the account ID.

Account ID	Authorization Status	Operation
09269[redacted]dd23e80	Authorized	Delete

Step 6 Click **OK**.

After the authorization is complete, an authorization record will be displayed in the **Authorized** list.

----End

Accepting Authorization

You can approve a pending authorization request to authorize an aggregator account.

Step 1 Log in to the management console.

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

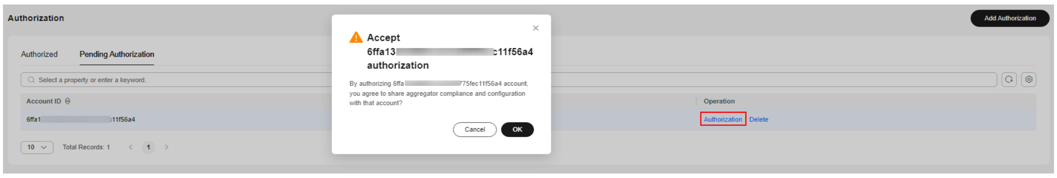
Step 3 In the navigation pane on the left, choose **Resource Aggregation** > **Authorizations**.

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 6-8 Accepting authorization



Accept 6ffa13[redacted]c11f56a4 authorization

By authorizing 6ffa[redacted]75fec11f56a4 account, you agree to share aggregator compliance and configuration with that account?

Account ID	Operation
6ffa1[redacted]11f56a4	Authorization Delete

----End

Deleting an Authorization

You can revoke authorization from an aggregator account.

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 Aggregation** > **Authorizations**.

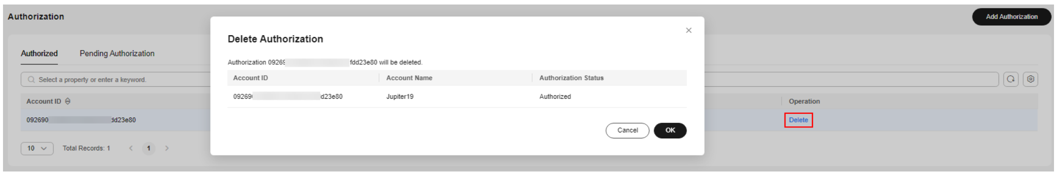
Step 4 Locate the authorization to be deleted in the list, and click **Delete** in the **Operation** column.

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

The authorization record will be moved to the **Pending Authorization** tab, and the authorization status will change to **Pending authorization**.

To authorize the aggregator account again, you can click **Authorize** in the **Operation** column in the **Pending Authorization** list.

Figure 6-9 Delete Authorization



Delete Authorization

Authorization 0926[redacted]fdd23e80 will be deleted.

Account ID	Account Name	Authorization Status
09269[redacted]d23e80	Jupiter19	Authorized

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 resources from one or more source accounts.

You can use ResourceQL and the query editor to customize queries for viewing and search for resources.

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.

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.

Limitations

To prevent a single user from occupying resources for queries for too long, the following constraints are set on advanced queries:

- If the execution duration of a query statement exceeds 15 seconds, a timeout error will be returned.
- If the result set to be returned exceeds the size limit, an error will occur. Make sure that the data volume returned by each statement is within the size limit.
- Up to 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.
- Advanced queries of resource aggregators do not support checksum and provisioning_state.

NOTICE

To get full functionality of advanced queries, you need to enable the resource recorder. The following describes how the resource recorder may affect your use of advanced queries.

- If you have never enabled the resource recorder, no resources can be queried with an advanced query.
- If you have enabled the resource recorder and a monitoring scope is specified, only resources within the monitoring scope can be queried with an advanced query.
- If you enable the resource recorder and disable it after a period of time, only resource data collected during the period when the resource recorder was enabled can be queried with an advanced query.

For details about how to enable and configure the resource recorder, see **Configuring the Resource Recorder**.

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 navigation pane on the left, choose **Resource Aggregation** > **Advanced Queries**.

Step 4 Choose the **Custom Queries** tab and click **Create Query** in the upper right corner.

Step 5 In the **Query Range** area on the right, select a target aggregator. In the text box below, enter the statement.

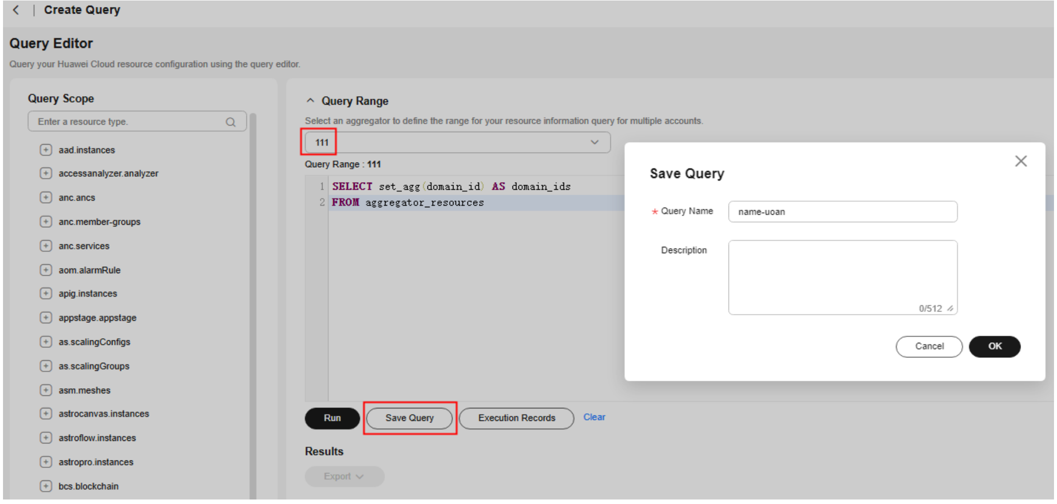
The Schema information used for advanced query is displayed on the left of the page. The properties parameter included in a request should be set to the Schema information which shows the detailed attributes of a cloud service resource. For details about the configuration example of the query statement,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

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

A query name can contain only digits, letters, underscores (_), and hyphens (-). It cannot exceed 64 characters.

Step 7 Click **OK**.

Figure 6-10 Save Query



Query Editor

Query your Huawei Cloud resource configuration using the query editor.

Select an aggregator to define the range for your resource information query for multiple accounts.

111

Query Range : 111

```
SELECT set_agg(domain_id) AS domain_ids
FROM aggregator_resources
```

* Query Name: name-uoan

Description: 0/512

NOTE

There is a limit to how many custom queries you can create. If you exceed this limit, you will receive a notification: "The maximum number of custom queries has been reached." Although the query cannot be saved, you can still run the query and export the results.

Step 8 Click **Run** and then view the query results. Up to 4,000 query results can be displayed and exported.

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

Step 10 Click **Execution Records** to view details about when the query was executed and the query statements.

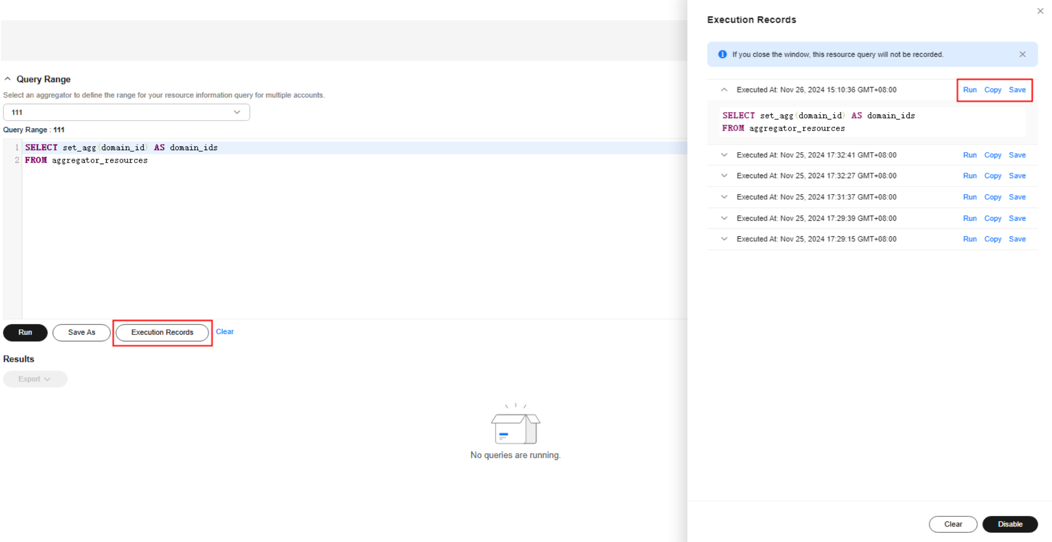
You can perform the following operations:

- **Run**: running the query
- **Copy**: copying the query statements
- **Save**: saving the query as a new query

NOTE

After you close the browser window or log out, the execution records of advanced queries will be cleared.

Figure 6-11 Execution records



Query Range

Select an aggregator to define the range for your resource information query for multiple accounts.

111

Query Range : 111

```
SELECT set_agg(domain_id) AS domain_ids
FROM aggregator_resources
```

Results

No queries are running.

Execution Records

If you close the window, this resource query will not be recorded.

Executed At: Nov 26, 2024 15:10:36 GMT+08:00

```
SELECT set_agg(domain_id) AS domain_ids
FROM aggregator_resources
```

Executed At: Nov 25, 2024 17:32:41 GMT+08:00

Executed At: Nov 25, 2024 17:32:27 GMT+08:00

Executed At: Nov 25, 2024 17:31:37 GMT+08:00

Executed At: Nov 25, 2024 17:29:39 GMT+08:00

Executed At: Nov 25, 2024 17:29:15 GMT+08:00

----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 **Using a Predefined Query**.
- 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 Custom 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

Advanced queries use 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 **aggregator_resources** table.

Table 6-1 aggregator_resources

Parameter	Type	Description
domain_id	String	Account ID
id	String	Resource ID
name	String	Resource name.

Parameter	Type	Description
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 Config 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 supported by CTS

Operation	Resource Type	Event Name
Creating rules	policy	createPolicyAssignments
Deleting rules	policy	deletePolicyAssignment
Updating rules	policy	updatePolicyAssignment
Triggering rules	policy	runEvaluation
Disabling rules	policy	disablePolicyAssignment
Enabling rules	policy	enablePolicyAssignment
Creating or updating rule remediation configurations	policy	createOrUpdateRemediationConfiguration
Deleting rule remediation configurations	policy	deleteRemediationConfiguration

Operation	Resource Type	Event Name
Running remediation actions (manual)	policy	runRemediationExecution
Batch creating remediation exceptions	policy	batchCreateRemediationExceptions
Batch deleting remediation exceptions	policy	batchDeleteRemediationExceptions
Updating evaluation results	policyState	updatePolicyState
Configuring or modifying the resource recorder	trackerConfig	createOrUpdateTrackerConfig
Disabling the resource recorder	trackerConfig	deleteTrackerConfig
Creating advanced queries	storedQuery	createStoredQuery
Updating advanced queries	storedQuery	updateStoredQuery
Deleting advanced queries	storedQuery	deleteStoredQuery
Creating organization rules	organizationPolicyAssignments	createOrganizationPolicyAssignment
Updating organization rules	organizationPolicyAssignments	updateOrganizationPolicyAssignment
Deleting an organization rule	organizationPolicyAssignments	deleteOrganizationPolicyAssignment
Authorizing aggregator accounts	authorization	createAggregationAuthorization
Canceling aggregator account authorization	authorization	deleteAggregationAuthorization
Creating an aggregator	aggregator	createConfigurationAggregator
Deleting an aggregator	aggregator	deleteConfigurationAggregator
Updating an aggregator	aggregator	updateConfigurationAggregator
Deleting pending aggregation requests	aggregationRequests	deletePendingAggregationRequest
Creating a conformance package	conformancePacks	createConformancePack

Operation	Resource Type	Event Name
Deleting a conformance package	conformancePacks	deleteConformancePack
Updating conformance packages	conformancePacks	updateConformancePack
Creating organization conformance packages	organizationConformancePacks	createOrganizationConformancePack
Deleting organization conformance packages	organizationConformancePacks	deleteOrganizationConformancePack
Updating organization conformance packages	organizationConformancePacks	updateOrganizationConformancePack
Batch adding resource tags	policy	tagResource
Batch deleting resource tags	policy	unTagResource

7.2 Viewing CTS Traces in the Trace List

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 Object Storage Service (OBS) buckets. Cloud Trace Service (CTS) stores operation records (traces) generated in the last seven days.

This section describes how to query or 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

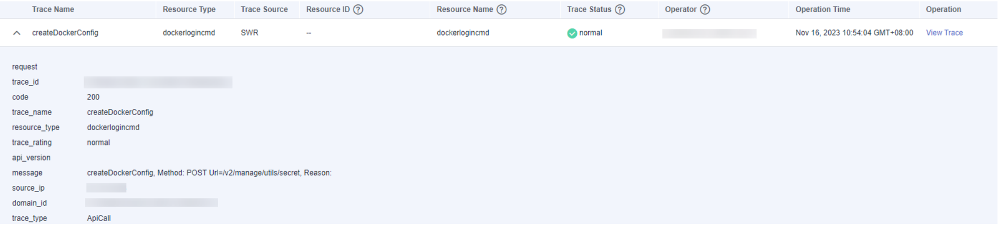
- Traces of a single account can be viewed on the CTS console. Multi-account traces can be viewed only on the **Trace List** page of each account, or in the OBS bucket or the **CTS/system** log stream configured for the management tracker with the organization function enabled.
- You can only query operation records of the last seven days on the CTS console. To store operation records for longer than seven days, you must configure transfer to OBS or Log Tank Service (LTS) so that you can view them in OBS buckets or LTS log groups.
- After performing operations on the cloud, you can query management traces on the CTS console one minute later and query data traces five minutes later.
- These operation records are retained for seven days on the CTS console and are automatically deleted upon expiration. Manual deletion is not supported.

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.
   - **Enterprise Project ID**: Enter an enterprise project ID.
   - **Access Key**: Enter a temporary or permanent access key ID.
   - Time range: Select **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range within the last seven days.
5. On the **Trace List** page, you can also export and refresh the trace list, and customize columns to display.
   - Enter any keyword in the search box and press **Enter** to filter desired traces.
   - Click **Export** to export all traces in the query result as an .xlsx file. The file can contain up to 5,000 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

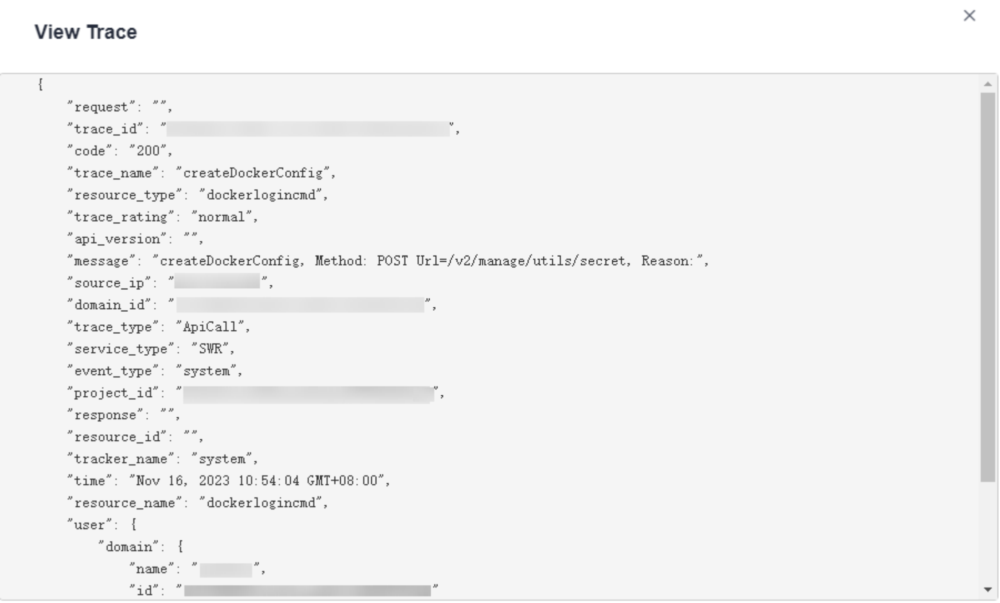
1. Log in to the management console.
2. Click ☰ in the upper left corner and choose **Management & Governance** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. Each time you log in to the CTS console, the new edition is displayed 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. The following filters are available.
   - **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: Select **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range within the last seven days.
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 5,000 records.
   - Click ↻ to view the latest information about traces.
8. Click ⌄ on the left of a trace to expand its details.



Trace Name	Resource Type	Trace Source	Resource ID ⓘ	Resource Name ⓘ	Trace Status ⓘ	Operator ⓘ	Operation Time	Operation
createDockerConfig	dockerlogincmd	SWR	--	dockerlogincmd	✓ normal	[redacted]	Nov 16, 2023 10:54:04 GMT+08:00	View Trace

request	
trace_id	[redacted]
code	200
trace_name	createDockerConfig
resource_type	dockerlogincmd
trace_rating	normal
api_version	
message	createDockerConfig, Method: POST Url=/v2/manage/utils/secret, Reason:
source_ip	[redacted]
domain_id	[redacted]
trace_type	ApiCall

9. Click **View Trace** in the **Operation** column. The trace details are displayed.



View Trace

```
{
    "request": "",
    "trace_id": "[redacted]",
    "code": "200",
    "trace_name": "createDockerConfig",
    "resource_type": "dockerlogincmd",
    "trace_rating": "normal",
    "api_version": "",
    "message": "createDockerConfig, Method: POST Url=/v2/manage/utils/secret, Reason:",
    "source_ip": "[redacted]",
    "domain_id": "[redacted]",
    "trace_type": "ApiCall",
    "service_type": "SWR",
    "event_type": "system",
    "project_id": "[redacted]",
    "response": "",
    "resource_id": "",
    "tracker_name": "system",
    "time": "Nov 16, 2023 10:54:04 GMT+08:00",
    "resource_name": "dockerlogincmd",
    "user": {
        "domain": {
            "name": "[redacted]",
            "id": "[redacted]"
```

10. For details about key fields in the trace structure, see **Trace Structure** and **Example Traces** in the *CTS User Guide*.

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

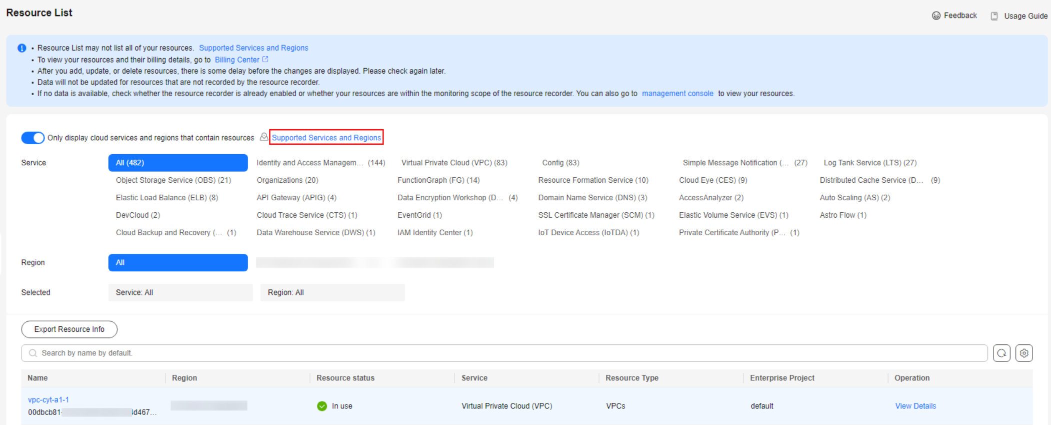
8.1 Supported Services and Regions

For details about the services and regions supported by Config, see the Config console.

Step 1 Log in to the management console and choose **Config** from the service list.

Step 2 On the Resource List page, click **Supported Services and Regions**.

Figure 8-1 Viewing supported services and regions



Resource List

- Resource List may not list all of your resources. Supported Services and Regions
- To view your resources and their billing details, go to Billing Center
- After you add, update, or delete resources, there is some delay before the changes are displayed. Please check again later.
- Data will not be updated for resources that are not recorded by the resource recorder.
- If no data is available, check whether the resource recorder is already enabled or whether your resources are within the monitoring scope of the resource recorder. You can also go to management console to view your resources.

Only display cloud services and regions that contain resources Supported Services and Regions

Service						
	All (482)	Identity and Access Managem... (144)	Virtual Private Cloud (VPC) (83)	Config (83)	Simple Message Notification (... (27)	Log Tank Service (LTS) (27)
	Object Storage Service (OBS) (21)	Organizations (20)	FunctionGraph (FG) (14)	Resource Formation Service (10)	Cloud Eye (CES) (9)	Distributed Cache Service (D... (9)
	Elastic Load Balance (ELB) (8)	API Gateway (APIG) (4)	Data Encryption Workshop (D... (4)	Domain Name Service (DNS) (3)	AccessAnalyzer (2)	Auto Scaling (AS) (2)
	DevCloud (2)	Cloud Trace Service (CTS) (1)	EventGrid (1)	SSL Certificate Manager (SCM) (1)	Elastic Volume Service (EVS) (1)	Astro Flow (1)
	Cloud Backup and Recovery (... (1)	Data Warehouse Service (DWS) (1)	IAM Identity Center (1)	IoT Device Access (IoTDA) (1)	Private Certificate Authority (P... (1)	

Region: All [redacted]

Selected: Service: All Region: All

Name	Region	Resource status	Service	Resource Type	Enterprise Project	Operation
vpc-cyt-a1-1 00dbcb81-[redacted]d467...	[redacted]	In use	Virtual Private Cloud (VPC)	VPCs	default	View Details

Step 3 Obtain details about the services and resources from the list displayed.

Step 4 In the search box above the list, specify a service or resource type to quickly find resources. You can also filter resources by region.

----End

8.2 Relationships with Supported Resources

Table 8-1 Relationships with supported resources

Service	Resource	Relationship	Related Service	Related Resource
Elastic Cloud Server	Cloud servers	isContainedIn	Virtual Private Cloud	VPCs
			Host Security Service	Host agents
			MapReduce Service	Clusters
		Contains	Cloud Backup and Recovery	Vaults
		isAttachedTo	Virtual Private Cloud	EIPs
			Cloud Backup and Recovery	Vaults
			Elastic Volume Service	Disks
		isAssociatedWith	Virtual Private Cloud	Security groups
			Image Management Service	Images
Bare Metal Server	Cloud servers	isContainedIn	Virtual Private Cloud	VPCs
		isAttachedTo	Elastic Volume Service	Disks
		isAssociatedWith	Virtual Private Cloud	Security groups
			Image Management Service	Images
Hyper Elastic Cloud Server	HECSs	isContainedIn	Virtual Private Cloud	VPCs
		Contains	Virtual Private Cloud	EIPs

Service	Resource	Relationship	Related Service	Related Resource
		isAttachedTo	Elastic Volume Service	Disks
		isAssociatedWith	Virtual Private Cloud	Security groups
			Image Management Service	Images
Auto Scaling	AS groups	isContainedIn	Virtual Private Cloud	VPCs
		isAssociatedWith	Virtual Private Cloud	Security groups
Distributed Cache Service	Memcached instances	isContainedIn	Virtual Private Cloud	VPCs
		isAssociatedWith	Virtual Private Cloud	Security groups
	Nodes	isContainedIn	Distributed Cache Service	Redis instances
	Redis instances	isContainedIn	Virtual Private Cloud	VPCs
		Contains	Distributed Cache Service	Nodes
		isAssociatedWith	Virtual Private Cloud	Security groups
Elastic Load Balance	Load balancers	Contains	Elastic Load Balance	Listeners
		isAttachedTo	Virtual Private Cloud	EIPs
			Elastic Load Balance	Backend server groups
			Elastic Load Balance	Active/ standby backend server groups
	Listeners	Is contained in	Elastic Load Balance	Load balancers

Service	Resource	Relationship	Related Service	Related Resource
		contains	Elastic Load Balance	Forwarding policies
		isAttachedTo	Elastic Load Balance	Backend server groups
			Elastic Load Balance	Active/ standby backend server groups
	Backend server groups	Contains	Elastic Load Balance	Backend servers
		Is attached to	Elastic Load Balance	Load balancers
			Elastic Load Balance	Listeners
	Active/ standby backend server groups	Contains	Elastic Load Balance	Backend servers
		isAttachedTo	Elastic Load Balance	Load balancers
			Elastic Load Balance	Listeners
	Forwarding policies	isContainedIn	Elastic Load Balance	Listeners
	Backend servers	isContainedIn	Elastic Load Balance	Backend server groups
			Elastic Load Balance	Active/ standby backend server groups
Virtual Private Cloud	VPCs	Contains	Elastic Cloud Server	Cloud servers
			Bare Metal Server	Cloud servers
			Hyper Elastic Cloud Server	HECSs
			AS	AS group

Service	Resource	Relationship	Related Service	Related Resource
			DCS	Memcached instance
			DCS	Redis instance
			MRS	Cluster
			VPC	Flow logs
			Virtual Private Cloud	EIPs
	Security groups	isAssociatedWith	Elastic Cloud Server	Cloud servers
			Bare Metal Server	Cloud servers
			HECS	HECS
			AS	AS group
			DCS	Memcached instance
			MRS	mrs
			DCS	Redis instance
		isContainedIn	Virtual Private Cloud	Ports
	Flow logs	isContainedIn	Virtual Private Cloud	Subnets
			Virtual Private Cloud	Ports
			Virtual Private Cloud	VPCs
	Ports	Contains	Virtual Private Cloud	Flow logs
			Virtual Private Cloud	Security groups
	Subnets	Contains	Virtual Private Cloud	Flow logs
	Bandwidth	contains	VPC	publicips
	Elastic IP	isContainedIn	VPC	Bandwidth

Service	Resource	Relationship	Related Service	Related Resource
			Virtual Private Cloud	VPC
		isAttachedTo	ECS	Cloud server
			ELB	Load balancer
			MRS	MRS
			NAT Gateway	Public NAT gateway
EVS	Volume	Contains	Cloud Backup and Recovery	Vaults
		isAttachedTo	ECS	Cloud server
			BMS	Cloud server
			Cloud Backup and Recovery	Vaults
			HECS	HECS
IMS	Image	isAssociatedWith	ECS	Cloud server
			BMS	Cloud server
			HECS	HECS
NAT Gateway	Public NAT gateway	isAttachedTo	VPC	Elastic IP
GeminiDB	Instances	Contains	GeminiDB	Nodes
	Node	isContainedIn	GeminiDB	Instances
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

Service	Resource	Relationship	Related Service	Related Resource
CCE	Cluster	contains	CCE	Node
	Node	isContainedIn	CCE	Cluster
Enterprise Router	Connection	isContainedIn	Enterprise Router	Instance
	Instance	contains	Enterprise Router	Connection
Identity and Access Management	Agencies	isAssociatedWith	Identity and Access Management	Policies
			Identity and Access Management	Roles
	User groups	Contains	Identity and Access Management	Users
		isAssociatedWith	Identity and Access Management	Policies
			Identity and Access Management	Roles
	Policies	isAssociatedWith	Identity and Access Management	Agencies
			Identity and Access Management	User groups
			Identity and Access Management	Users
	Roles	isAssociatedWith	Identity and Access Management	Agencies
			Identity and Access Management	User groups
			Identity and Access Management	Users

Service	Resource	Relationship	Related Service	Related Resource
	Users	isAssociatedWith	Identity and Access Management	Policies
			Identity and Access Management	Roles
		isContainedIn	Identity and Access Management	User groups
RDS	Instance	contains	RDS	Node
	Node	isContainedIn	RDS	Instance
Config	Conformance package	Contains	Config	Rule
	Rule	Is contained in	Config	Conformance package
Cloud Backup and Recovery	Vaults	isAttachedTo	ECS	Cloud servers
			Elastic Volume Service	Disks
			Scalable File Service Turbo (SFS Turbo)	SFS Turbo
	Policies	isAttachedTo	Cloud Backup and Recovery	Vaults
	Vaults	isAttachedTo	Cloud Backup and Recovery	Policies
		isContainedIn	Elastic Cloud Server	Cloud servers
			Elastic Volume Service	Disks
			Scalable File Service Turbo (SFS Turbo)	SFS Turbo
Document Database Service	Instances	Contains	Document Database Service	Nodes

Service	Resource	Relationship	Related Service	Related Resource
	Node	isContainedIn	Document Database Service	Instances
Host Security Service	Host agent	Contains	ECS	Cloud servers
Web Application Firewall	Instances	isContainedIn	Web Application Firewall	Policies
	Policies	Contains	Web Application Firewall	Instances
Scalable File Service Turbo (SFS Turbo)	SFS Turbo	Contains	Cloud Backup and Recovery	Vaults
	SFS Turbo	isAttachedTo	Cloud Backup and Recovery	Vaults

8.3 Supported Services and Resources

Currently, although most Huawei Cloud services and resources support tagging, tag information of some resources, such as OBS buckets, cannot be synchronized to Config. In this case, Config may fail to provide tag-related functions for these resources. For example, you cannot search for resources by tag or use tag-related Config rules.

The following table lists supported services and resource types.

Table 8-2 Services and resource types that support tagging

Service	Resource type
VPC Endpoint	● VPC Endpoints (vpcep.endpoints) ● VPC Endpoint Services (vpcep.endpointServices)
Data Replication Service (DRS)	● Data Synchronization Tasks (drs.synchronizationJob) ● Online Migration Tasks (drs.migrationJob) ● Disaster Recovery Tasks (drs.dataGuardJob) ● Data Subscription Tasks (drs.subscriptionJob) ● Backup Migration Tasks (drs.backupMigrationJob)

Service	Resource type
Bare Metal Server (BMS)	BMSs (bms.servers)
Elastic Cloud Server (ECS)	ECSs (ecs.cloudservers)
Hyper Elastic Cloud Server (HECS)	HECSs (hecs.hcloudservers)
Virtual Private Cloud (VPC)	● VPCs (vpc.vpcs) ● EIPs (vpc.publicips)
Elastic Volume Service (EVS)	Disks (evs.volumes)
Auto Scaling (AS)	AS Groups
Image Management Service (IMS)	Images (ims.images)
Distributed Cache Service (DCS)	● Redis Instance (dcs.redis) ● Instance Nodes (dcs.node)
Domain Name Service (DNS)	● Public Zones (dns.publiczones) ● Private Zones (dns.privatezones)
Virtual Private Network (VPN)	● Shared VPN Connections (vpnaas.vpnConnections) ● Shared VPN Gateways (vpnaas.vpnGateways)
Scalable File Service Turbo (SFS Turbo)	File Systems (sfsturbo.shares)
Elastic Load Balance (ELB)	● Load Balancers (elb.loadbalancers) ● Listeners (elb.listeners)
Simple Message Notification (SMN)	Topics (smn.topic)
Distributed Message Service	● Kafka Instances (dms.kafkas) ● Kafka Brokers (dms.kafka_nodes) ● RabbitMQ Instances (dms.rabbitmqs) ● RabbitMQ Brokers (dms.rabbitmq_nodes) ● RocketMQ Instances (dms.reliabilitys)
Relational Database Service (RDS)	● Instances (rds.instances) ● Nodes (dcs.node)
MapReduce Service (MRS)	Clusters (mrs.mrs)
Data Warehouse Service (DWS)	Clusters (dws.clusters)

Service	Resource type
Document Database Service (DDS)	- Instances (dds.instances) - Nodes (dds.nodes)
Cloud Search Service (CSS)	Clusters (css.clusters)
NAT Gateway	- Public NAT Gateways (nat.natGateways) - Private NAT Gateways (nat.privateNatGateways)
Cloud Backup and Recovery (CBR)	Vaults (cbr.vault)
Data Encryption Workshop (DEW)	keys (kms.keys)
Cloud Container Engine (CCE)	Clusters (cce.clusters)
GaussDB	- Instances (gaussdb.instances) - Nodes (gaussdb.nodes)
Database Security Service	Instances (dbss.cloudservers)
Content Delivery Network (CDN)	Domain Names (cdn.domains)
Direct Connect	- Virtual Gateways (dcaas.vgw) - LAGs (dcaas.lag) - Virtual Interfaces (dcaas.vif) - Network Topology (dcaas.directConnect)
Database and Application Migration UGO (UGO)	- Object Evaluation Projects (ugo.evaluationJob) - Object Migration Projects (ugo.migrationJob)
Advanced Anti-DDoS (AAD)	Instances (aad.instances)
Cloud Connect	- Cloud Connections (ccaas.cloud-connections) - Bandwidth Packages (ccaas.bandwidth-packages)
Cloud Native Anti-DDoS (CNAD)	Instances (cnad.instances)
Enterprise Router (ER)	- Enterprise Routers (er.instances) - Attachments (er.attachments)
Log Tank Service (LTS)	Log Streams (lts.topics)

Service	Resource type
IoT Device Access (IoTDA)	● Basic Instances (iotda.iotda) ● Enterprise Instances (iotda.iotda_instance) ● Standard Instances (iotda.iotda_standardinstance)
Global Accelerator (GA)	Accelerators (ga.accelerators)
MacroVerse SmartStage for Integrators	Flows (mssi.flow)
Cloud Bastion Host	CBH Instances (cbh.instance)
Cloud Firewall	Cloud Firewall Instances (cfw.cfw_instance)
Cloud Eye Service	Alarm Rules (ces.alarms)
API Gateway	Gateways (apig.instances)
FunctionGraph	Functions (fgs.functions)
Distributed Database Middleware (DDM)	● Instances (ddm.instances) ● Nodes (ddm.nodes)
LakeFormation	Instances (lakeformation.instance)
Blockchain Service	HBS Instances (bcs.huaweicloudchain)
CraftArtsIPDCenter	CraftArtsIPDCenter (ipdcenter.envs)
Industrial Digital Model Engine (iDME)	● MBM Foundation Service (idme.mbm) ● Runtime (idme.runtime)
Cloud Secret Management Service (CSMS)	Secrets (csms secrets)
Industrial Simulation Cloud Service	● SimSpace (craftartssim.simSpace) ● CPU Computing (craftartssim.cpuUnit) ● GUI Computing (craftartssim.guiUnit)
Private Certificate Authority	● Certificate Authority (pca.ca) ● Certificates (pca.cert)
Dedicated Distributed Storage Service (DSS)	Storage Pools (dss.dsspools)
Dedicated Host	DeHs (deh.dedicatedhosts)
AccessAnalyzer	AccessAnalyzer (accessanalyzer.analyzer)

8.4 Notification Models

8.4.1 Resource Change Notification Model

Resource Change Notification Model

Table 8-3 Parameters of the resource change notification model

Parameter	Type	Description
notification_type	String	The type of the notification. For a resource change notification, the notification type is **ResourceChanged**.
notification_creation_time	String	The time when the message was sent. The notification creation time is a UTC time (such as 2018-11-14T08:59:14Z) that complies with ISO8601.
domain_id	String	Account ID.
detail	Object	Notification details.

Table 8-4 detail parameters

Parameter	Type	Description
resource_id	String	Resource ID.
resource_type	String	Resource type.
event_type	Enum	Event type (**CREATE**, **UPDATE**, **DELETE**)
capture_time	String	The event capture time. The event capture time is a UTC time (such as 2018-11-14T08:59:14Z) that complies with ISO8601.
resource	Object	Resource details.

Table 8-5 resource

Parameter	Type	Description
id	String	Resource ID.
name	String	Resource name.

Parameter	Type	Description
provider	String	Cloud service name.
type	String	Resource type.
region_id	String	The ID of the region where the resource resides.
project_id	String	IAM project ID.
project_name	String	IAM project name.
ep_id	String	Enterprise project ID.
ep_name	String	Enterprise project name.
checksum	String	The checksum.
created	String	Resource creation time. The resource creation time is a UTC time (such as 2018-11-14T08:59:14Z) that complies with ISO8601.
updated	String	The time when the resource was last updated. The latest update time is a UTC time (such as 2018-11-14T08:59:14Z) that complies with ISO8601.
provisioning_state	String	Resource provisioning state.
tags	Map	Resource tags.
properties	Map	Resource attributes.

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.regionid1a.xxxxxx.com/v2/059b5e0a2500d5552fa1c00adada8c06/os-vendor-
volumes/3e62c0e6-e779-469e-b0f2-35743f6229d1"
          },
          {
            "rel": "bookmark",
            "href": "https://evs.regionid1a.xxxxxx.com/059b5e0a2500d5552fa1c00adada8c06/os-vendor-
volumes/3e62c0e6-e779-469e-b0f2-35743f6229d1"
          }
        ],
        "volHostAttrHost": "regionid1a-pod01.regionid1a#0",
        "multiattach": false,
        "status": "available"
      },
      "region_id": "regionid1a",
      "project_id": "059b5e0a2500d5552fa1c00adada8c06",
      "project_name": "regionid1a",
      "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"
}
```

8.4.2 Resource Relationship Change Notification Model

Resource Relationship Change Notification Model

Table 8-6 Parameters of the resource relationship change notification model

Parameters	Type	Description
notification_type	String	The type of a notification. For a resource relationship change notification, the notification type is **ResourceRelationChanged**.
notification_creation_time	String	The time when the message was sent. The notification creation time is a UTC time (such as 2018-11-14T08:59:14Z) that complies with ISO8601.
domain_id	String	Account ID.
detail	Object	Notification details.

Table 8-7 detail

Parameter	Type	Description
resource_id	String	Resource ID.
resource_type	String	Resource type.
event_type	Enum	Event type (**CHANGE**).
capture_time	String	The event capture time. The event capture time is a UTC time (such as 2018-11-14T08:59:14Z) that complies with ISO8601.
from_resource_id	String	Original resource ID (displayed only when there was an original resource)
from_resource_type	String	Original resource type (displayed only when there was an original resource)
relation_type	String	Resource relationship (displayed only when there was an original resource)

Notification Example of Resource Relationship Changes

```
{
  "detail" : {
    "resource_id" : "675d78fd****377b067be0531",
    "resource_type" : "config.policyAssignments",
    "event_type" : "CHANGE",
    "capture_time" : "2024-12-14T12:31:59.201Z",
    "from_resource_id" : "e336ffcfc2ab****4bf892423739c7125",
    "from_resource_type" : "config.conformancePacks",
    "relation_type" : "isContainedIn"
  },
  "notification_type" : "ResourceRelationChanged",
  "notification_creation_time" : "2024-12-14T12:31:59.404Z",
  "domain_id" : "017f09bdc0194******80082147f41a8"
}
```

8.4.3 Resource Snapshot Storage Notification Model

Resource Snapshot Storage Notification Model

Table 8-8 Parameters of the resource snapshot storage notification model

Parameter	Type	Description
notification_type	String	The type of a notification. For a resource snapshot storage notification, the notification type is **SnapshotArchiveCompleted**.
notification_creation_time	String	The time when the message was sent. The notification creation time is a UTC time (such as 2018-11-14T08:59:14Z) that complies with ISO8601.
domain_id	String	Account ID.
detail	Object	Notification details.

Table 8-9 detail

Parameter	Type	Description
snapshot_id	String	Resource snapshot ID.
region_id	String	The ID of the region where resource snapshots reside.
bucket_name	String	The name of the OBS bucket where resource snapshots are stored.
object_keys	Array of String	Path of the OBS object where resource snapshots are stored.

Notification Example of Resource Snapshot Storage

```
{
  "detail": {
    "snapshot_id": "474f85e6-72cd-442b-af4e-517120a5c669",
    "region_id": "regionid1a",
    "bucket_name": "test",
    "object_keys": [
      "RMSLogs/059b5c937100d3e40ff0c00a7675a0a0/Snapshot/
2020/8/11/059b5c937100d3e40ff0c00a7675a0a0_Snapshot_regionid1a_ResourceSnapshot_2020-08-10T1709
01_474f85e6-72cd-442b-af4e-517120a5c669_part-1.json.gz"
    ]
  },
  "notification_type": "SnapshotArchiveCompleted",
  "notification_creation_time": "2020-08-10T17:09:27.314Z",
  "domain_id": "059b5c937100d3e40ff0c00a7675a0a0"
}
```

8.4.4 Notification Model of Resource Change Notification Storage

Notification Model of Resource Change Notification Storage

Table 8-10 Parameters of the notification model of resource change notification storage

Parameter	Type	Description
notification_type	String	The type of a notification. For resource change notification storage, the notification type is **NotificationArchiveCompleted**.
notification_creation_time	String	The time when the message was sent. The notification creation time is a UTC time (such as 2018-11-14T08:59:14Z) that complies with ISO8601.
domain_id	String	Account ID.
detail	Object	Notification details.

Table 8-11 detail parameters

Parameter	Type	Description
region_id	String	The ID of the region where resource change notifications are stored.

Parameter	Type	Description
bucket_name	String	The name of the OBS bucket where resource change notifications are stored.
object_key	String	The path of an object in an OBS bucket for storing resource change notifications.

Notification Example of Resource Change Notification Storage

```
{
    "detail": {
        "region_id": "regionid1a",
        "bucket_name": "test",
        "object_key": "RMSLogs/059b5c937100d3e40ff0c00a7675a0a0/Notification/2020/12/10/
NotificationChunk/
059b5c937100d3e40ff0c00a7675a0a0_Notification_regionid1a_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"
}
```

8.5 Storage Models

8.5.1 Resource Snapshot Storage Model

Resource Snapshot Storage Model

Table 8-12 Resource snapshot storage model

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 8-13 Items parameters

Parameter	Type	Description
resource	Object	Specifies the resource.
relations	Array of Object	Specifies the item list of the resource relationship.

Table 8-14 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	The time when the resource was last 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 tags.
properties	Map	Specifies the cloud resource attributes.

Table 8-15 Relations parameters

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 Snapshot Storage Example

```
{
  "items": [
    {
      "resource": {
        "id": "c25ee8b3-c907-4cd4-9869-6c4b07c61a0b",
        "name": "rse-cdk-07-cdk-3sbz",
        "provider": "vpc",
        "type": "securityGroups",
        "region_id": "regionid1a",
        "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"
}
```

8.5.2 Storage Model of Resource Change Notifications

Storage Model of Resource Change Notifications

Table 8-16 Storage model of resource change notifications

Parameter	Type	Description
notification_items	Array of Object	Resource change notifications.

Table 8-17 notification_items parameters

Parameter	Parameter Type	Description
notification_type	String	Notification type. For a resource change notification, the notification type is **ResourceChanged**.
notification_creation_time	String	Notification sending time The notification sending time is a UTC time (such as 2018-11-14T08:59:14Z) that complies with ISO8601.
domain_id	String	Account ID.
detail	Object	Notification details.

Table 8-18 detail parameters

Parameter	Parameter Type	Description
resource_id	String	Resource ID.
resource_type	String	Resource type.
event_type	Enum	Event type (**CREATE**, **UPDATE**, **DELETE**)
capture_time	String	Event capture time. The event capture time is a UTC time (such as 2018-11-14T08:59:14Z) that complies with ISO8601.
resource	Object	Resource details.

Table 8-19 resource

Parameter	Type	Description
id	String	Resource ID.
name	String	Resource name.
provider	String	Service name.
type	String	Resource type.
region_id	String	The ID of the region where the resource resides.
project_id	String	IAM project ID.
project_name	String	IAM project name.
ep_id	String	Enterprise project ID.
ep_name	String	Enterprise project name.
checksum	String	The checksum.
created	String	Resource creation time. The resource creation time is a UTC time (such as 2018-11-14T08:59:14Z) that complies with ISO8601.

Parameter	Type	Description
updated	String	The time when the resource was last updated. The resource update time is a UTC time (such as 2018-11-14T08:59:14Z) that complies with ISO8601.
provisioning_state	String	Resource state.
tags	Map	Resource tags.
properties	Map	Resource attributes.

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": "regionid1a",
                    "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 ResourceQL Syntax

8.6.1 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 table lists seven data types supported by ResourceQL. For the array type, [] is used to index a position, and the number starts from 1.

Table 8-20 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 8-21 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.
ep_id	String	Specifies the enterprise project ID.
checksum	String	Specifies the resource checksum.
created	Date	Specifies the time when the resource was created.

Parameter	Type	Description
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.

provider and **type** represent a unique resource. For different resources, **properties** varies. For example, for an ECS, the **provider** and **type** are **ecs** and **cloudservers**, and the **properties** contains **flavor**. For a VPC, the **provider** and **type** are **vpc** and **publicips**, and the **properties** contains **bandwidth**.

You can obtain resource attributes that can be included in the **properties** element for each resource on Config console or by calling the related API. For more details, see **How Can I Obtain Resource Attributes Reported to Config?**

properties supports nested queries. The following shows an example of how to query the **addresses** parameter under **properties** for the running ECS.

```
SELECT name, created, updated, properties.addresses FROM resources
   WHERE provider = 'ecs' AND type = 'cloudservers' AND properties.status = 'ACTIVE'
```

8.6.2 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
```

8.6.3 Functions

ResourceQL supports the following functions.

Table 8-22 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*.

Function	Description
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 8-23 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.
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.

Function	Description
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 8-24 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 value of array *a*.
array_distinct(a) → array	Removes duplicate values from array *a*.
array_frequency(a) → map	Returns a map: keys are the unique elements in *array*, values are how many times the key appears.
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).

Function	Description
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_union(a, b) → array	Returns an array of the elements in the union of *a* and *b*, without duplicates.
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.

Function	Description
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 8-25 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.

Function	Description
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.
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 8-26 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**.