Config

User Guide

Issue	01
Date	2023-12-30

HUAWEI TECHNOLOGIES CO., LTD.

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

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

Trademarks and Permissions

HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process*. For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

Copyright © Huawei Technologies Co., Ltd.

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 you cannot find resources on the **Resource List** page, check if the resource recorder is enabled or if the resource type is within the monitoring scope. 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**.

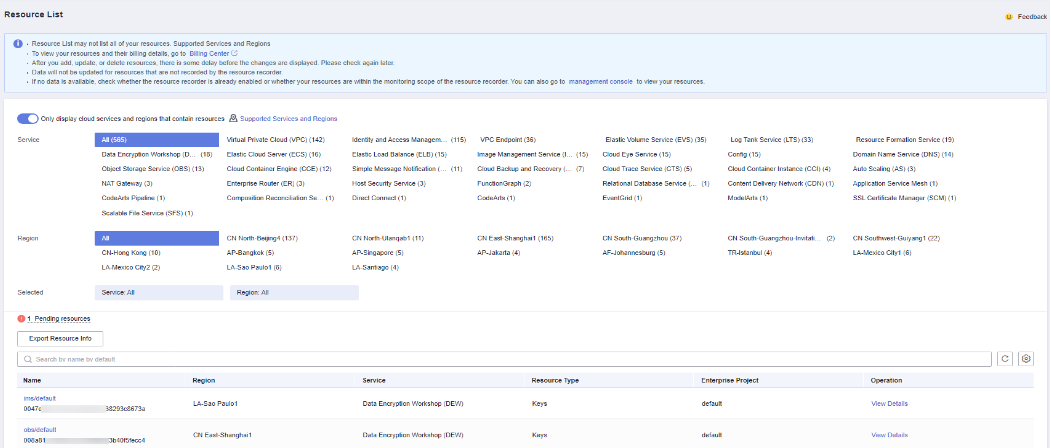
Procedure

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

Figure 1-1 Resource List



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

Selected: Service: All, Region: All

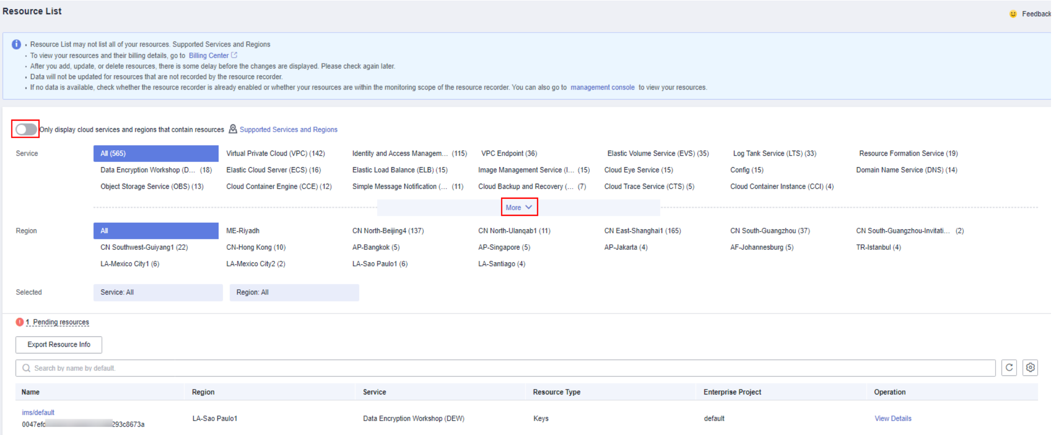
1 Pending resources

Name	Region	Service	Resource Type	Enterprise Project	Operation
ims/default 0047e[redacted]38293c8673a	LA-Sao Paulo1	Data Encryption Workshop (DEW)	Keys	default	View Details
obs/default 008a81[redacted]3b40f5fecc4	CN East-Shanghai1	Data Encryption Workshop (DEW)	Keys	default	View Details

Feedback
Supported Services and Regions
Service
All (565)
Virtual Private Cloud (VPC) (142)
Identity and Access Managem... (115)
VPC Endpoint (36)
Elastic Volume Service (EVS) (35)
Log Tank Service (LTS) (33)
Resource Formation Service (19)
Data Encryption Workshop (D... (18)
Elastic Cloud Server (ECS) (16)
Elastic Load Balance (ELB) (15)
Image Management Service (I... (15)
Cloud Eye Service (15)
Config (15)
Domain Name Service (DNS) (14)
Object Storage Service (OBS) (13)
Cloud Container Engine (CCE) (12)
Simple Message Notification (... (11)
Cloud Backup and Recovery (... (7)
Cloud Trace Service (CTS) (5)
Cloud Container Instance (CCI) (4)
Auto Scaling (AS) (3)
NAT Gateway (3)
Enterprise Router (ER) (3)
Host Security Service (3)
FunctionGraph (2)
Relational Database Service (... (1)
Content Delivery Network (CDN) (1)
Application Service Mesh (1)
CodeArts Pipeline (1)
Composition Reconciliation Se... (1)
Direct Connect (1)
CodeArts (1)
EventGrid (1)
ModelArts (1)
SSL Certificate Manager (SCM) (1)
Scalable File Service (SFS) (1)
Region
All
CN North-Beijing4 (137)
CN North-Ulanqab1 (11)
CN East-Shanghai1 (165)
CN South-Guangzhou (37)
CN South-Guangzhou-Invitati... (2)
CN Southwest-Guiyang1 (22)
CN-Hong Kong (10)
AP-Bangkok (5)
AP-Singapore (5)
AP-Jakarta (4)
AF-Johannesburg (5)
TR-Istanbul (4)
LA-Mexico City1 (6)
LA-Mexico City2 (2)
LA-Sao Paulo1 (6)
LA-Santiago (4)
Export Resource Info
Search by name by default.

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

Figure 1-2 Viewing all supported services



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

Selected: Service: All, Region: All

1 Pending resources

Name	Region	Service	Resource Type	Enterprise Project	Operation
ims/default 0047efc[redacted]293c8673a	LA-Sao Paulo1	Data Encryption Workshop (DEW)	Keys	default	View Details

Feedback
Supported Services and Regions
Service
All (565)
Virtual Private Cloud (VPC) (142)
Identity and Access Managem... (115)
VPC Endpoint (36)
Elastic Volume Service (EVS) (35)
Log Tank Service (LTS) (33)
Resource Formation Service (19)
Data Encryption Workshop (D... (18)
Elastic Cloud Server (ECS) (16)
Elastic Load Balance (ELB) (15)
Image Management Service (I... (15)
Cloud Eye Service (15)
Config (15)
Domain Name Service (DNS) (14)
Object Storage Service (OBS) (13)
Cloud Container Engine (CCE) (12)
Simple Message Notification (... (11)
Cloud Backup and Recovery (... (7)
Cloud Trace Service (CTS) (5)
Cloud Container Instance (CCI) (4)
More
Region
All
ME-Riyadh
CN North-Beijing4 (137)
CN North-Ulanqab1 (11)
CN East-Shanghai1 (165)
CN South-Guangzhou (37)
CN South-Guangzhou-Invitati... (2)
CN Southwest-Guiyang1 (22)
CN-Hong Kong (10)
AP-Bangkok (5)
AP-Singapore (5)
AP-Jakarta (4)
AF-Johannesburg (5)
TR-Istanbul (4)
LA-Mexico City1 (6)
LA-Mexico City2 (2)
LA-Sao Paulo1 (6)
LA-Santiago (4)
Export Resource Info
Search by name by default.

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

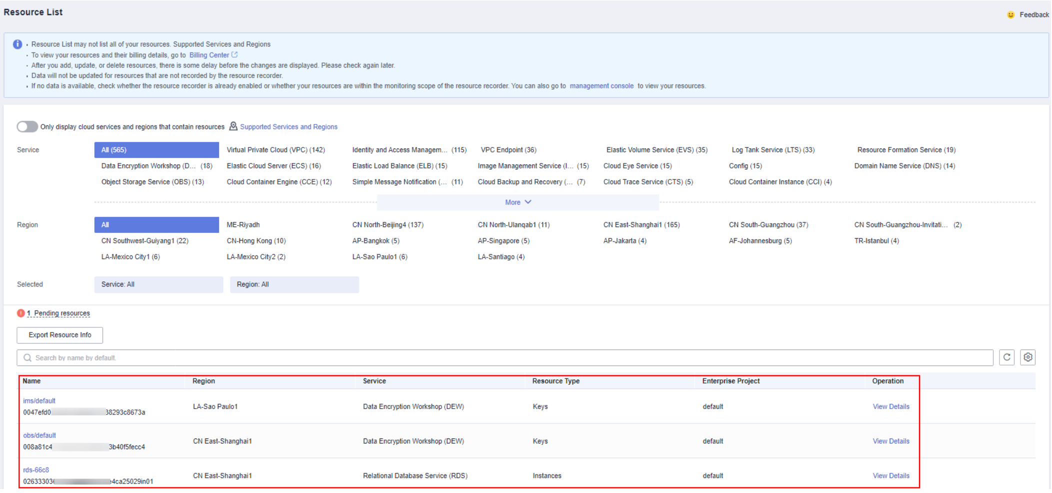
----End

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.

Figure 1-3 Resource List



Resource List

Feedback

- 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 (565)	Virtual Private Cloud (VPC) (142)	Identity and Access Managem... (115)	VPC Endpoint (36)	Elastic Volume Service (EVS) (35)	Log Tank Service (LTS) (33)	Resource Formation Service (19)
	Data Encryption Workshop (D... (18)	Elastic Cloud Server (ECS) (16)	Elastic Load Balance (ELB) (15)	Image Management Service (I... (15)	Cloud Eye Service (15)	Config (15)	Domain Name Service (DNS) (14)
	Object Storage Service (OBS) (13)	Cloud Container Engine (CCE) (12)	Simple Message Notification (... (11)	Cloud Backup and Recovery (... (7)	Cloud Trace Service (CTS) (5)	Cloud Container Instance (CCI) (4)	
			More				
Region	All	ME-Riyadh	CN North-Beijing4 (137)	CN North-Ulanqab1 (11)	CN East-Shanghai1 (165)	CN South-Guangzhou (37)	CN South-Guangzhou-Invitati... (2)
	CN Southwest-Guiyang1 (22)	CN-Hong Kong (10)	AP-Bangkok (5)	AP-Singapore (5)	AP-Jakarta (4)	AF-Johannesburg (5)	TR-Istanbul (4)
	LA-Mexico City1 (6)	LA-Mexico City2 (2)	LA-Sao Paulo1 (6)	LA-Santiago (4)			
Selected	Service: All	Region: All					

1 Pending resources

Export Resource Info

Search by name by default.

Name	Region	Service	Resource Type	Enterprise Project	Operation
ims/default 0047efd0[redacted]38293c8673a	LA-Sao Paulo1	Data Encryption Workshop (DEW)	Keys	default	View Details
obs/default 008a81c4[redacted]3b40f5fecc4	CN East-Shanghai1	Data Encryption Workshop (DEW)	Keys	default	View Details
rds-66c8 02633303[redacted]4ca25029in01	CN East-Shanghai1	Relational Database Service (RDS)	Instances	default	View Details

Procedure

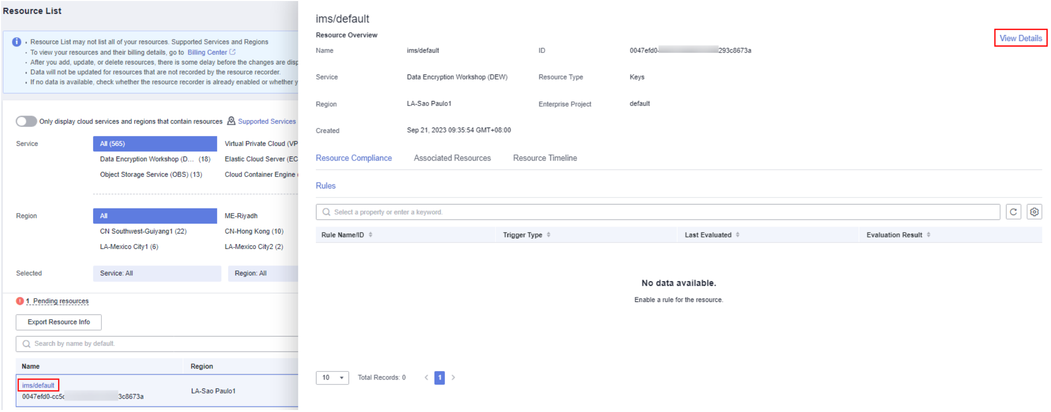
Step 1 Log in to the management console.

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 1-4 Resource overview



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 disp
- 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 y

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

Service	All (565)	Virtual Private Cloud (VP
	Data Encryption Workshop (D... (18)	Elastic Cloud Server (EC
	Object Storage Service (OBS) (13)	Cloud Container Engine
Region	All	ME-Riyadh
	CN Southwest-Guiyang1 (22)	CN-Hong Kong (10)
	LA-Mexico City1 (6)	LA-Mexico City2 (2)
Selected	Service: All	Region: All

1 Pending resources

Export Resource Info

Search by name by default.

Name	Region
ims/default 0047efd0-cc5c[redacted]3c8673a	LA-Sao Paulo1

ims/default

Resource Overview

View Details

Name	ims/default	ID	0047efd0-[redacted]293c8673a
Service	Data Encryption Workshop (DEW)	Resource Type	Keys
Region	LA-Sao Paulo1	Enterprise Project	default
Created	Sep 21, 2023 09:35:54 GMT+08:00		

Resource Compliance | Associated Resources | Resource Timeline

Rules

Select a property or enter a keyword.

Rule Name/ID	Trigger Type	Last Evaluated	Evaluation Result

No data available.

Enable a rule for the resource.

10 | Total Records: 0 | 1

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.
Tags	If you select **Tags** as a search criterion, **Tag key** and **Tag value** are displayed in sequence, and you need to select a tag key and value.
Enterprise Project	The enterprise project which resources belong to. If you select an enterprise project, resources in this enterprise project will be displayed.

NOTE

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

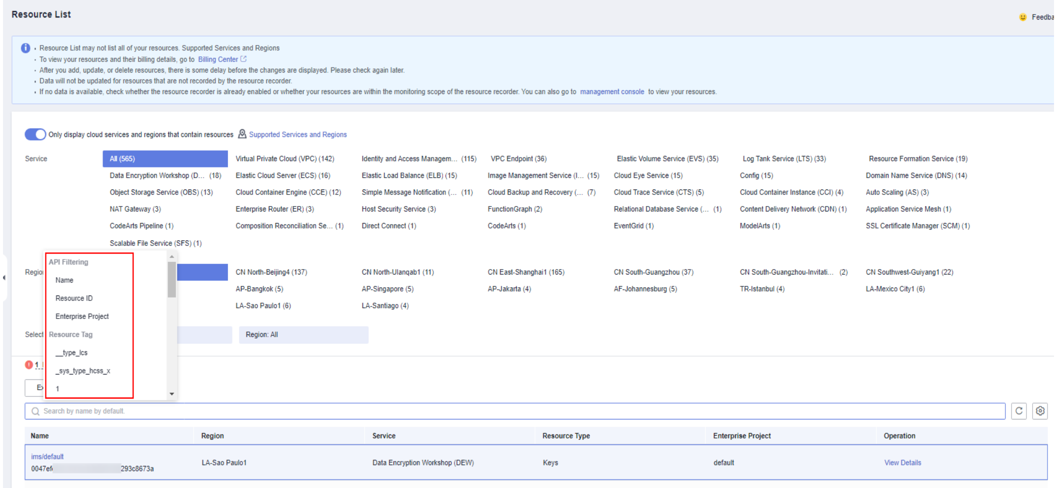
Procedure

Step 1 Log in to the management console.

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

Step 3 Specify one or more search options: the enterprise project, resource name, resource ID, and resource tag to filter resources.

Figure 1-5 Filtering resources



Resource List

Feedba

- 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 (565) | Virtual Private Cloud (VPC) (142) | Identity and Access Managem... (115) | VPC Endpoint (36) | Elastic Volume Service (EVS) (35) | Log Tank Service (LTS) (33) | Resource Formation Service (19)
Data Encryption Workshop (D... (18) | Elastic Cloud Server (ECS) (16) | Elastic Load Balance (ELB) (15) | Image Management Service (I... (15) | Cloud Eye Service (15) | Config (15) | Domain Name Service (DNS) (14)
Object Storage Service (OBS) (13) | Cloud Container Engine (CCE) (12) | Simple Message Notification (... (11) | Cloud Backup and Recovery (... (7) | Cloud Trace Service (CTS) (5) | Cloud Container Instance (CCI) (4) | Auto Scaling (AS) (3)
NAT Gateway (3) | Enterprise Router (ER) (3) | Host Security Service (3) | FunctionGraph (2) | Relational Database Service (... (1) | Content Delivery Network (CDN) (1) | Application Service Mesh (1)
CodeArts Pipeline (1) | Composition Reconciliation Se... (1) | Direct Connect (1) | CodeArts (1) | EventGrid (1) | ModelArts (1) | SSL Certificate Manager (SCM) (1)
Scalable File Service (SFS) (1)

Regio | CN North-Beijing4 (137) | CN North-Ulanqab1 (11) | CN East-Shanghai1 (165) | CN South-Guangzhou (37) | CN South-Guangzhou-Invitati... (2) | CN Southwest-Guiyang1 (22)
AP-Bangkok (5) | AP-Singapore (5) | AP-Jakarta (4) | AF-Johannesburg (5) | TR-Istanbul (4) | LA-Mexico City1 (6)
LA-Sao Paulo1 (6) | LA-Santiago (4)

Select | Region: All

API Filtering
Name
Resource ID
Enterprise Project
Resource Tag
__type_lcs
_sys_type_hcss_x
1

Search by name by default.

Name	Region	Service	Resource Type	Enterprise Project	Operation
ims/default 0047ef[redacted]293c8673a	LA-Sao Paulo1	Data Encryption Workshop (DEW)	Keys	default	View Details

----End

1.1.4 Exporting the Resource List

Scenarios

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

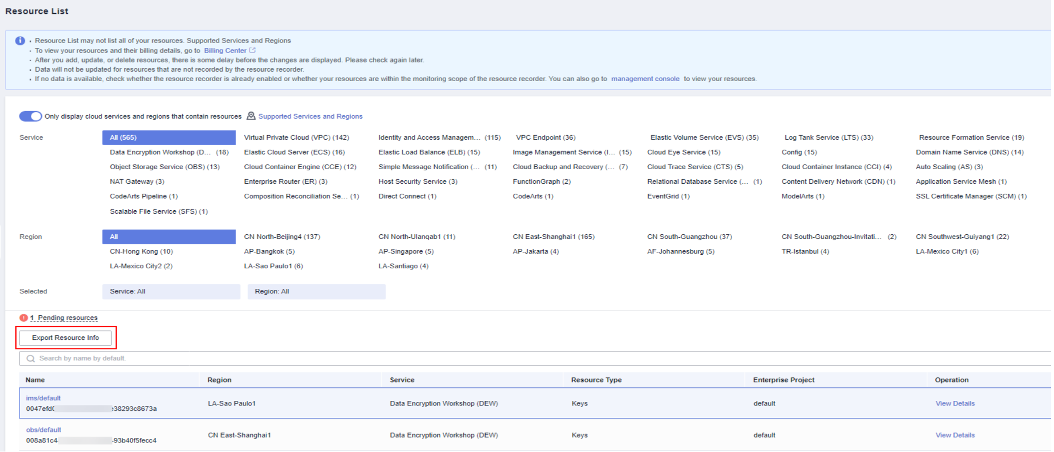
Procedure

Step 1 Log in to the management console.

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

Step 3 Click **Export Resource Info** above the list.

Figure 1-6 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 (565) | Virtual Private Cloud (VPC) (142) | Identity and Access Managem... (115) | VPC Endpoint (36) | Elastic Volume Service (EVS) (35) | Log Tank Service (LTS) (33) | Resource Formation Service (19)
Data Encryption Workshop (D... (18) | Elastic Cloud Server (ECS) (16) | Elastic Load Balance (ELB) (15) | Image Management Service (I... (15) | Cloud Eye Service (15) | Config (15) | Domain Name Service (DNS) (14)
Object Storage Service (OBS) (13) | Cloud Container Engine (CCE) (12) | Simple Message Notification (... (11) | Cloud Backup and Recovery (... (7) | Cloud Trace Service (CTS) (5) | Cloud Container Instance (CCI) (4) | Auto Scaling (AS) (3)
NAT Gateway (3) | Enterprise Router (ER) (3) | Host Security Service (3) | FunctionGraph (2) | Relational Database Service (... (1) | Content Delivery Network (CDN) (1) | Application Service Mesh (1)
CodeArts Pipeline (1) | Composition Reconciliation Se... (1) | Direct Connect (1) | CodeArts (1) | EventGrid (1) | ModelArts (1) | SSL Certificate Manager (SCM) (1)
Scalable File Service (SFS) (1)

Region: All | CN North-Beijing4 (137) | CN North-Ulanqab1 (11) | CN East-Shanghai1 (165) | CN South-Guangzhou (37) | CN South-Guangzhou-Invitati... (2) | CN Southwest-Guiyang1 (22)
CN-Hong Kong (10) | AP-Bangkok (5) | AP-Singapore (5) | AP-Jakarta (4) | AF-Johannesburg (5) | TR-Istanbul (4) | LA-Mexico City1 (6)
LA-Mexico City2 (2) | LA-Sao Paulo1 (6) | LA-Santiago (4)

Selected: Service: All | Region: All

1 Pending resources

Export Resource Info

Search by name by default.

Name	Region	Service	Resource Type	Enterprise Project	Operation
ims/default 0047efd([redacted]38293c8673a	LA-Sao Paulo1	Data Encryption Workshop (DEW)	Keys	default	View Details
obs/default 008a81c4[redacted]-93b40f5fecc4	CN East-Shanghai1	Data Encryption Workshop (DEW)	Keys	default	View Details

----End

NOTE

Information of all resources will be exported to an Excel file, containing all attributes of the resources.

1.2 Viewing Resource Compliance Data

Scenarios

Config provides you with rules to evaluate resources. You can view compliance data of the resources evaluated in the **Resource Overview** page.

Procedure

Step 1 Log in to the management console.

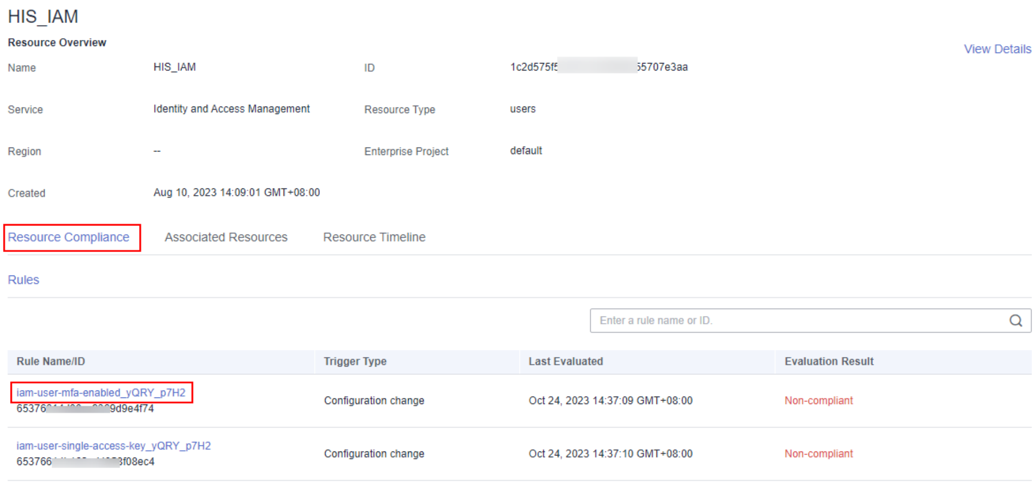
Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

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

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

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

Figure 1-7 Viewing resource compliance data



HIS_IAM

Resource Overview

Name	HIS_IAM	ID	1c2d575f[redacted]5707e3aa
Service	Identity and Access Management	Resource Type	users
Region	--	Enterprise Project	default
Created	Aug 10, 2023 14:09:01 GMT+08:00		

Rule Name/ID	Trigger Type	Last Evaluated	Evaluation Result
iam-user-mfa-enabled_yQRY_p7H2 65376[redacted]9d9e4f74	Configuration change	Oct 24, 2023 14:37:09 GMT+08:00	Non-compliant
iam-user-single-access-key_yQRY_p7H2 653766[redacted]3f08ec4	Configuration change	Oct 24, 2023 14:37:10 GMT+08:00	Non-compliant

----End

1.3 Viewing Resource Relationships

Scenarios

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

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

Procedure

Step 1 Log in to the management console.

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

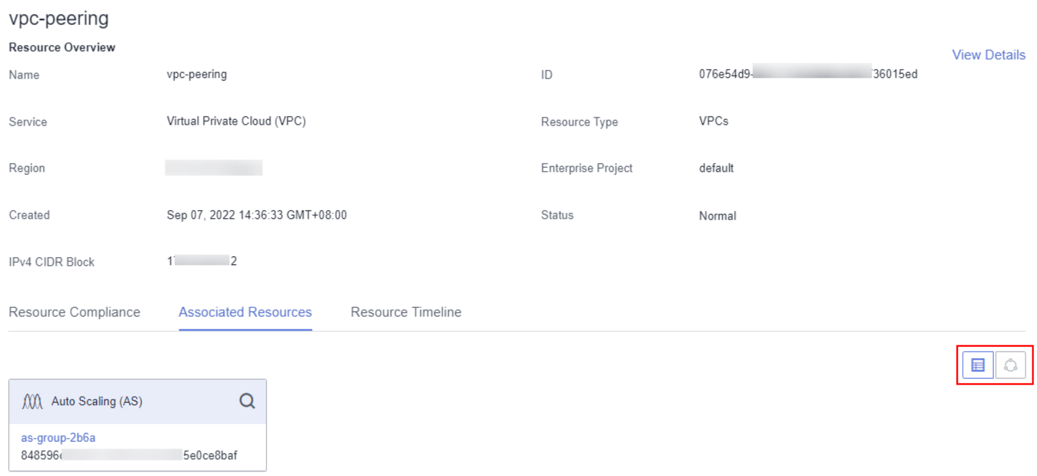
Step 3 On the **Resource List** page, click the name of a target resource.

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

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

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

Figure 1-8 Viewing associated resources



vpc-peering

Resource Overview

View Details

Name	vpc-peering	ID	076e54d9-[redacted]36015ed
Service	Virtual Private Cloud (VPC)	Resource Type	VPCs
Region	[redacted]	Enterprise Project	default
Created	Sep 07, 2022 14:36:33 GMT+08:00	Status	Normal
IPv4 CIDR Block	1[redacted]2		

as-group-2b6a
848596[redacted]5e0ce8baf

----End

NOTE

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

Scenarios

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

Procedure

Step 1 Log in to the management console.

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

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

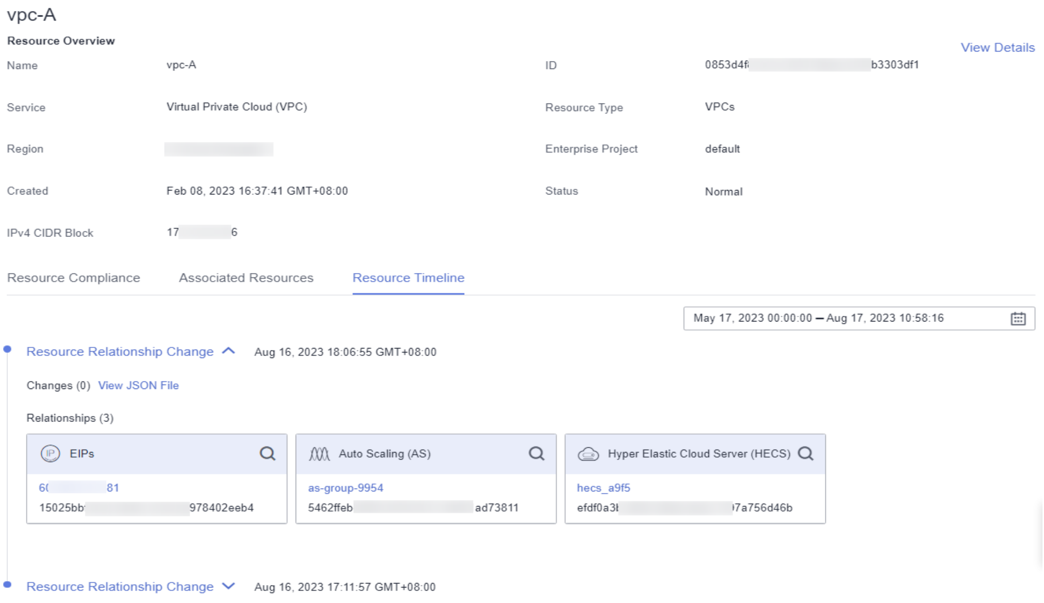
Step 4 Choose the **Resource Timeline** tab to view the resource changes.

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

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

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

Figure 1-9 Resource timeline



vpc-A

Resource Overview

View Details

Name	vpc-A	ID	0853d4f[redacted]b3303df1
Service	Virtual Private Cloud (VPC)	Resource Type	VPCs
Region	[redacted]	Enterprise Project	default
Created	Feb 08, 2023 16:37:41 GMT+08:00	Status	Normal
IPv4 CIDR Block	17[redacted]6		

Resource Compliance | Associated Resources | Resource Timeline

May 17, 2023 00:00:00 – Aug 17, 2023 10:58:16

Resource Relationship Change Aug 16, 2023 18:06:55 GMT+08:00

Changes (0) View JSON File

Relationships (3)

EIPs	Auto Scaling (AS)	Hyper Elastic Cloud Server (HECS)
6[redacted]81 15025bb[redacted]978402eeb4	as-group-9954 5462ffeb[redacted]ad73811	hecs_a9f5 efdf0a3[redacted]7a756d46b

Resource Relationship Change Aug 16, 2023 17:11:57 GMT+08:00

----End

2 Resource Recorder

2.1 Overview

Introduction

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

To be specific, the resource recorder

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

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

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

Notes and Constraints

- When enabling and configuring the resource recorder, you must configure **Topic** or **Resource Dump**.
- 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 confirmation for the topic.
- The resource recorder only updates data for the resources within the monitoring scope.
- By default, resource configuration information is stored for seven years (2,557 days).

NOTICE

To get full functionality of Config, you need to enable the resource recorder. If the resource recorder is disabled, Config may fail to update your resource data, aggregate resource data from source accounts, or accurately evaluate your resources.

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.

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

After the resource recorder is enabled, Config will notify you of any resource changes (creations, modifications, deletions, or relationship changes) and periodically store your notifications and resource snapshots.

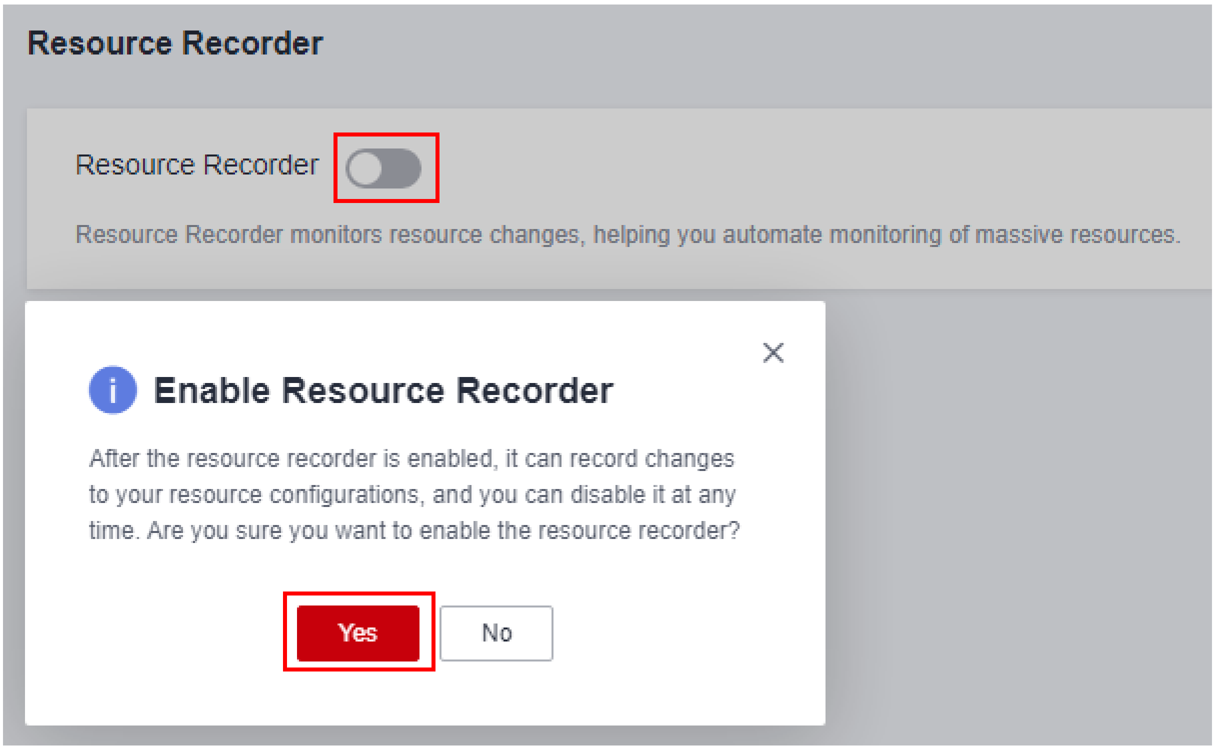
Step 1 Log in to the management console.

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

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

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

Figure 2-1 Enabling the resource recorder



Resource Recorder

Resource Recorder

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

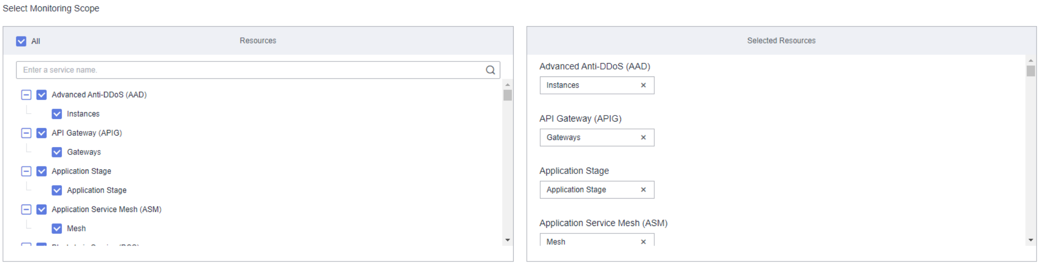
Enable Resource Recorder

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

Figure 2-2 Selecting the monitoring scope



Select Monitoring Scope

☑ Advanced Anti-DDoS (AAD)
☑ Instances
☑ API Gateway (APIG)
☑ Gateways
☑ Application Stage
☑ Application Stage
☑ Application Service Mesh (ASM)
☑ Mesh

Selected Resources

Advanced Anti-DDoS (AAD)
Instances ×

API Gateway (APIG)
Gateways ×

Application Stage
Application Stage ×

Application Service Mesh (ASM)
Mesh ×

Step 6 Specify an OBS bucket.

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

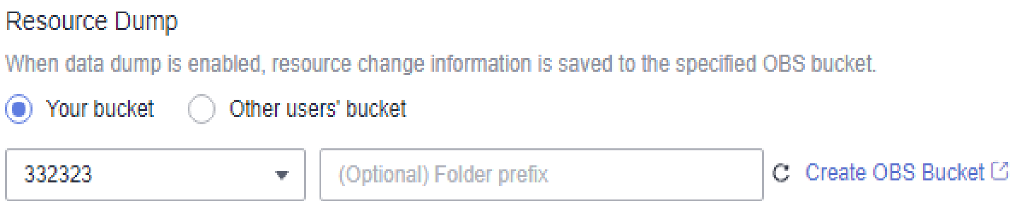
- **Select an OBS bucket from the current account**:
  Click **Your bucket**. If the OBS bucket name has a prefix, you need to enter the prefix. If no OBS buckets are available of the current account, create one. For details about how to create an OBS bucket, see ***Object Storage Service User Guide***.
- **Select an OBS bucket from another account**:
  Select **Other users' bucket**, then configure **Region ID** and **Bucket Name**. If the OBS bucket name has a prefix, you need to enter the prefix. If you select a

bucket from another account, you need required permissions granted by the account. For details, see **Cross-Account Authorization**.

NOTE

After you specify an OBS bucket, Config will write an empty file named **ConfigWritabilityCheckFile** to the OBS bucket to verify whether resources can be written to the OBS bucket.

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

332323

Step 7 Specify a data retention period.

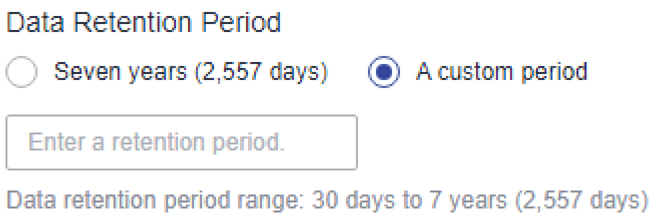
Select **Seven years (2557 days)** or select **A custom period** and enter a retention period from 30 days to 2557 days.

NOTE

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

Config will delete data that has been reserved for a longer time than the specified retention period.

Figure 2-4 Specifying a data retention period



Data Retention Period

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

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

Step 8 Select 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 no SMN topics are available, create one. For details about how to create an SMN topic, see ***Simple Message Notification User Guide***.

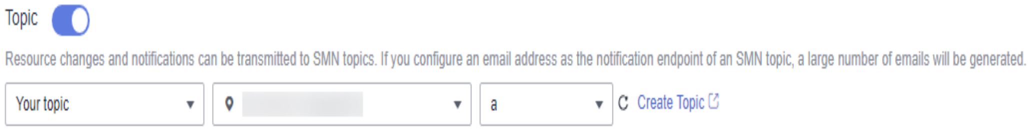
- **Select a topic from another account.**

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

NOTE

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

Figure 2-5 Selecting an SMN topic



Topic

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

Your topic ▾ | ▾ | a ▾ | Create Topic

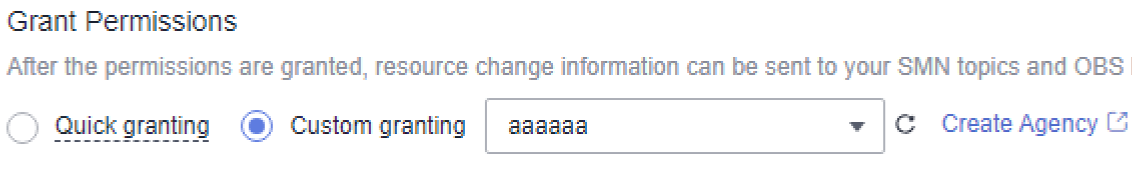
Step 9 Grant permissions.

- **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** doesn't contain KMS permissions, and 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 the **KMS Administrator** permission to the agency or use custom authorization. For details, see **Storing Resource Change Notifications and Resource Snapshots to an Encrypted OBS Bucket**.
- **Custom granting**: You can create an agency using IAM to customize authorization for RMS. The agency must include permissions for sending notifications using an SMN topic and for writing data into an OBS bucket. To store resource changes and snapshots to an OBS bucket that is encrypted using KMS, you need the **KMS Administrator** permission. For details, see **Storing Resource Change Notifications and Resource Snapshots to an Encrypted OBS Bucket**. For details about how to create an agency, see ***Identity and Access Management User Guide***.

  NOTE

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

Figure 2-6 Grant permissions



Grant Permissions

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

○ Quick granting ● Custom granting | aaaaaa ▾ | Create Agency

Step 10 Click **Save**.

Step 11 In the displayed dialog box, click **Yes**.

----End

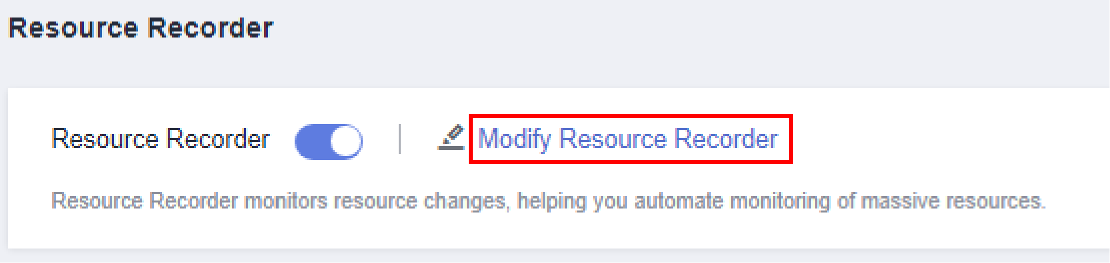
Modifying the Resource Recorder

You can modify the resource recorder at any time.

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

Step 2 Click **Modify Resource Recorder**.

Figure 2-7 Modifying the 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 **Yes**.

----End

Disabling the Resource Recorder

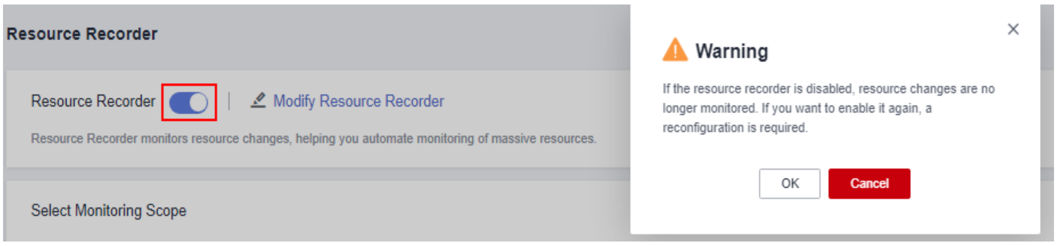
You can disable the resource recorder at any time.

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

Step 2 Toggle off the resource recorder.

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

Figure 2-8 Disabling the resource recorder



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

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. Sign 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**.

- **Granting OBS bucket permissions to another account**

  a. Sign in to the management console with the authorizing account and go to the OBS console.

  b. Attach related OBS permissions to target accounts based on **Creating a Custom Bucket Policy (JSON View)**.

     Add the following bucket policy:

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

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

Storing Resource Change 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 from another account, 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. Sign in to the Data Encryption Workshop (DEW) console and go to the **Key Management Service** page.

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

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

   - Select **Account** for **User or Account** and enter an account ID.
   - Select **Create Data Key** for **Granted Operations**.

2.3 Notifications

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

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

Config send notifications when:

- Resources are created, modified, or deleted.
- Resource relationships change.
- Notifications of resource changes are stored.
- Resource snapshots are stored.

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

2.4 Storing Resources

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

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

2.5 Storing Resource Change 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 confirmation for the topic.

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

3 Resource Compliance

3.1 Rules

3.1.1 Adding a Predefined Rule

Scenarios

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

This section describes how to add predefined rules.

Constraints and Limitations

Up to 500 rules can be added to an account.

NOTICE

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

- If you have never enabled the resource recorder, no resources will be available for evaluation.
- If you have enabled the resource recorder and a monitoring scope is configured, only resources within the monitoring scope can be evaluated.
- If you enable the resource recorder and then disable it after a period of time, only resource data collected during the period when the resource recorder is enabled can be evaluated.

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

Procedure

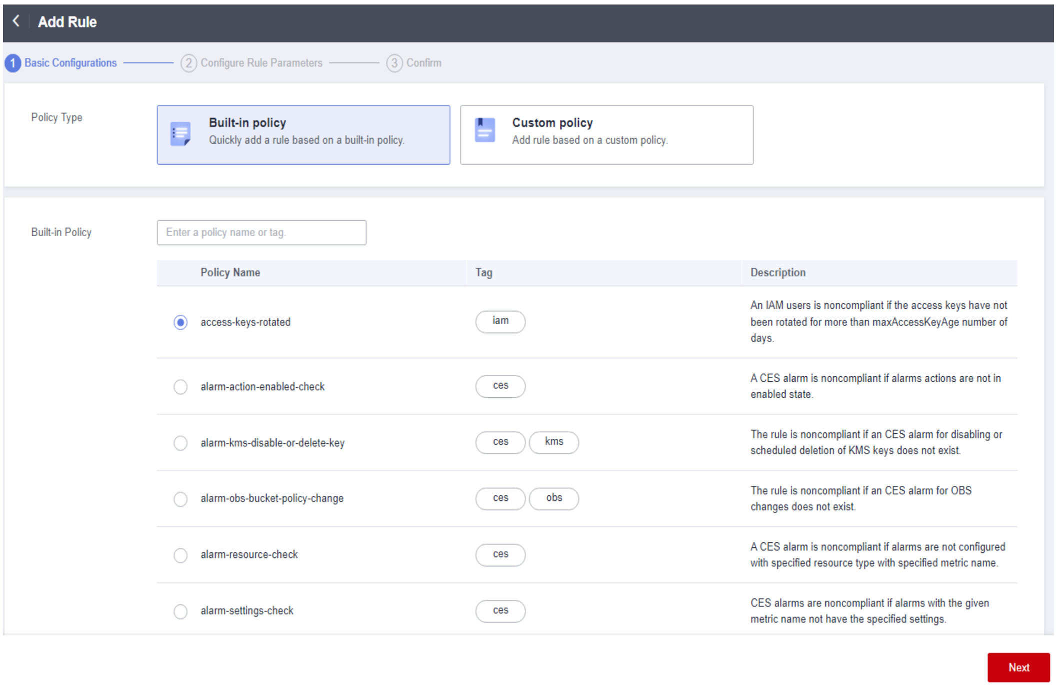
Step 1 Log in to the management console.

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

Figure 3-1 Configuring basic details



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 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.
○	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 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.

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

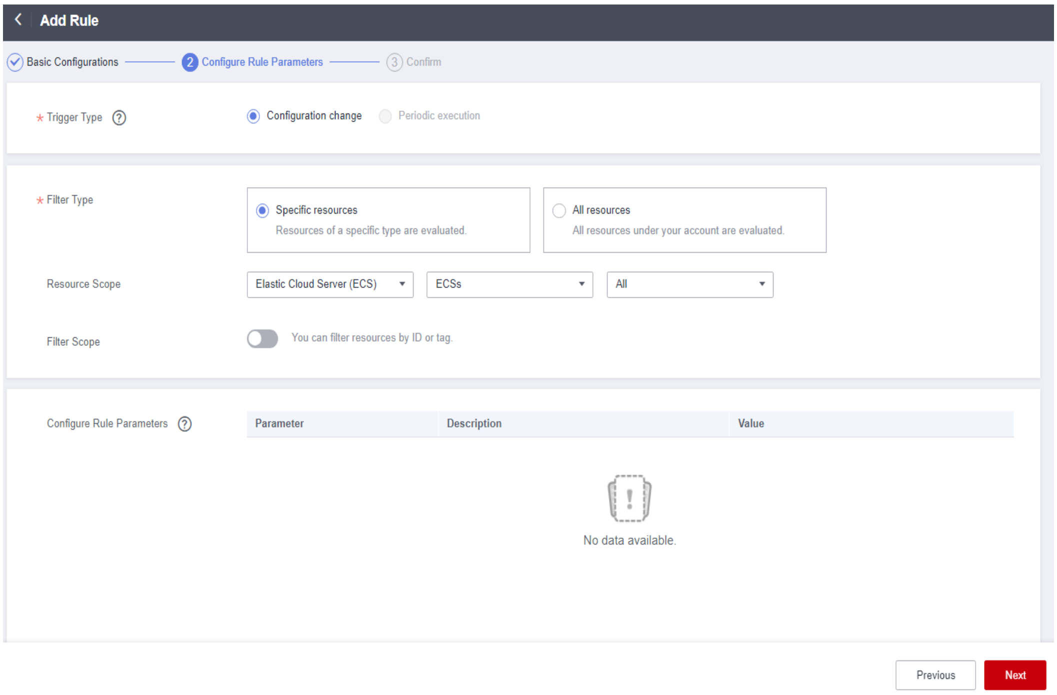
Table 3-1 Basic configuration parameters

Parameter	Description
Policy Type	Possible values are: - **Built-in policy** - **Custom policy**
Built-in Policy	Specifies the policy that has been developed for a service. You can use built-in policies to quickly add rules. For details, see **Predefined Policies**.
Custom Policy	Config allows you to create custom policies to add rules. For details, see **Example Custom Policies**.

Parameter	Description
Rule Name	By default, the predefined policy name is reused as the rule name. A rule name must be unique. The rule name can contain only digits, letters, underscores (_), and hyphens (-).
Description	By default, the rule description is the same as the selected predefined policy description. You can also customize the rule description. There are no restrictions on the rule description.
FunctionGraph Function	Specifies the URN of the FunctionGraph function in the custom policy. For details about how to create a FunctionGraph function, see **Creating a FunctionGraph Function for a Config Custom Policy**. This parameter is mandatory only when **Policy Type** is set to **Custom policy**.
Grant Permissions	This agency grants Config the read-only and call permissions of FunctionGraph. These permissions allow you to customize rules to query FunctionGraph or send events to FunctionGraph. This parameter is mandatory only when **Policy Type** is set to **Custom policy**. NOTE ● **Quick granting**: This option will automatically create an agency named **rms_custom_policy_agency** to grant the permissions required for the customized rule to work properly. The permissions include the read-only and call permissions for FunctionGraph. ● **Custom granting**: This option allows you to create an agency and assign permissions in IAM. The permissions assigned must include the read-only and call permissions of FunctionGraph. For details about how to create an agency, see ***Identity and Access Management User Guide***.

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

Figure 3-2 Configure Rule Parameters



* 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 | All

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

Configure Rule Parameters

Parameter	Description	Value

No data available.

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

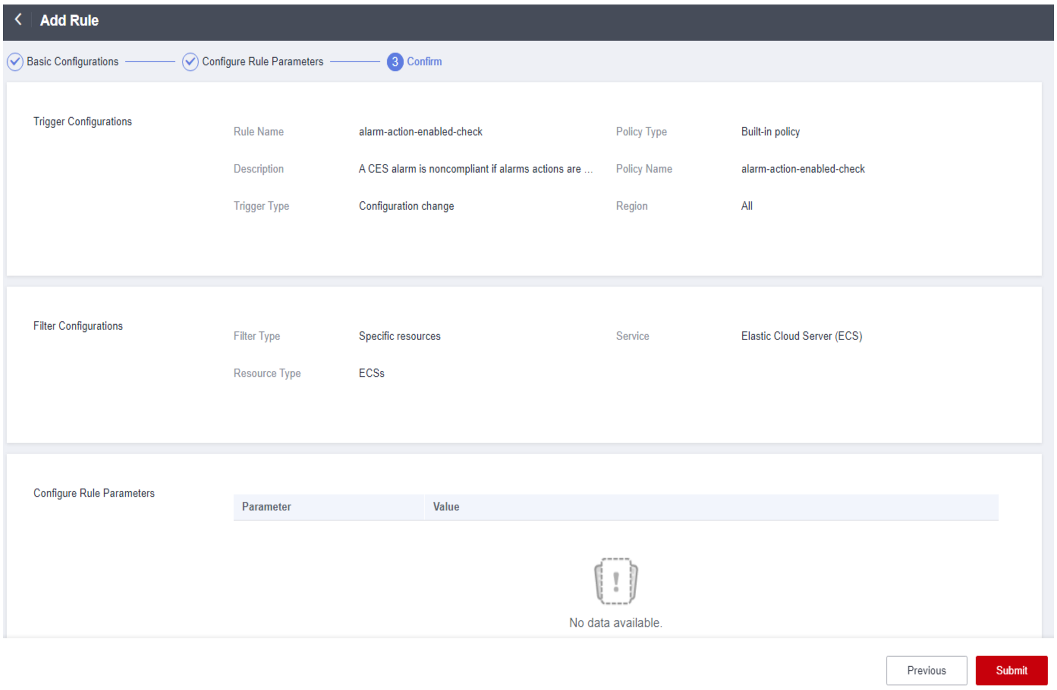
Table 3-2 Parameter descriptions

Parameter	Description
Trigger Type	Specifies the conditions under which rules are triggered. Possible values are: - **Configuration change**: The rule is triggered when a specific cloud resource is changed. - **Periodic execution**: The rule is triggered at a specific frequency.
Filter Type	Specifies the resources to be evaluated. Possible types are: - **Specific resources**: Resources of a specific type will be evaluated. - **All resources**: All resources from your account will be evaluated. This parameter is mandatory only when **Trigger Type** is set to **Configuration change**.

Parameter	Description
Resource Scope	If you set **Filter Type** to **Specific resources**, you need to specify a resource scope. ● Service: Select the service the resource belongs to. ● Resource type: Select the resource type of the corresponding service. ● Region: Select the region where the resource is located. This parameter is mandatory only when **Trigger Type** is set to **Configuration change**.
Filter Scope	After you enable **Filter Scope**, you can filter resources by resource ID or tag. You can specify a specific resource for compliance evaluation. This parameter is mandatory only when **Trigger Type** is set to **Configuration change**.
Execute Every	Indicates how often a rule is triggered. This parameter is mandatory only when **Trigger Type** is set to **Periodic execution**.
Configure Rule Parameters	Specifies the parameter configuration for the built-in policy or custom policy you selected in step **Configure Basic Details**. For example, if you select policy **required-tag-check** and **Keywords** is **tag**, you need to specify a tag key and a tag value here. Then, resources that do not have this tag are non-compliant. Not all built-in policies have parameters to be configured. For example, if you select policy **volumes-encrypted-check**, you do not need to configure any rule parameters. You can set up to 10 rule parameters for a custom policy.

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

Figure 3-3 Confirm



Trigger Configurations

Rule Name: alarm-action-enabled-check

Policy Type: Built-in policy

Description: A CES alarm is noncompliant if alarms actions are ...

Policy Name: alarm-action-enabled-check

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

NOTE

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

----End

3.1.2 Adding a Custom Rule

Scenario

You can create custom rules to supplement predefined rules.

To create a custom rule, you need to use FunctionGraph. Each custom rule is associated with a Function Graph function. The function collects rule parameters and resource attributes from the event sent by Config to evaluate your resources and returns evaluation results using the OpenAPI of Config. Config sends events based on the trigger type (configuration changes or periodic) of a rule. For details about how to use FunctionGraph, see **FunctionGraph User Guide**.

NOTICE

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

- If you have never enabled the resource recorder, no resources will be available for evaluation.
- If you have enabled the resource recorder and a monitoring scope is configured, only resources within the monitoring scope can be evaluated.
- If you enable the resource recorder and then disable it after a period of time, only resource data collected during the period when the resource recorder is enabled can be evaluated.

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

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**

Creating a Function with FunctionGraph

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

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

Step 3 Set **Function Type** to **Event Function** and configure the required IAM agency. The agency is used to grant the function required permissions. It must include the **rms:policyStates:update** permission.

Step 4 Click **Create Function**.

Step 5 In the code box, enter a function and click **Deploy**.

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

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

Step 7 Click **Save**.

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

----End

Adding a Custom Rule

Step 1 Log in to the management console.

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

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

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

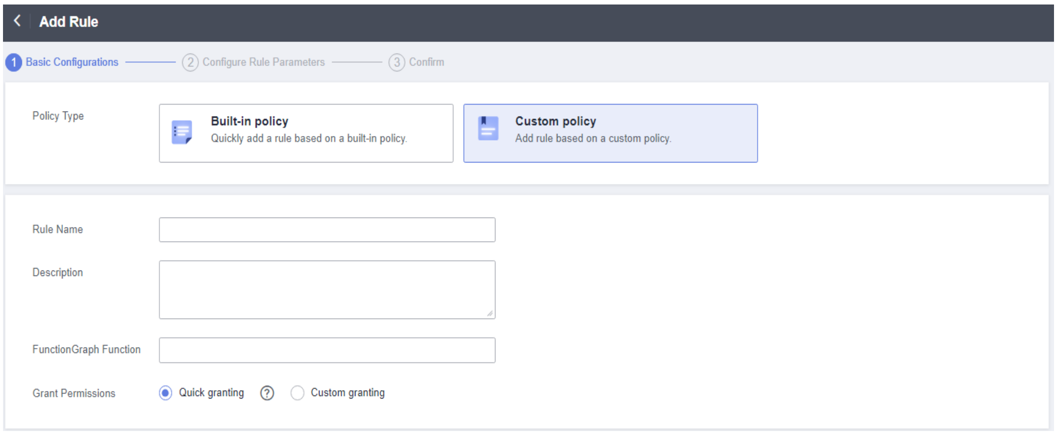
Step 5 Set **Policy Type** to **Custom Policy**. Set related parameters, select **Quick granting** or **Custom granting** to grant permissions, and click **Next**.

- **Quick granting**: Quick granting quickly grants you permissions of the rms_custom_policy_agency agency. The permissions ensure proper functioning of a custom policy, including the permissions for obtaining and asynchronously execute a function through FunctionGraph.
- **Custom granting**: You need to use IAM to create an agency and then :attach the agency to Config. You can set the authorization statement as follows.

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

For details about how to create an agency, see **Creating an Agency (by a Delegating Party)**.

Figure 3-4 Adding a rule using a custom policy



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

Description

FunctionGraph Function

Grant Permissions ● Quick granting ⓘ ○ Custom granting

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

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

----End

3.1.3 Viewing a Rule

Scenario

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

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

Procedure

Step 1 Log in to the management console.

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

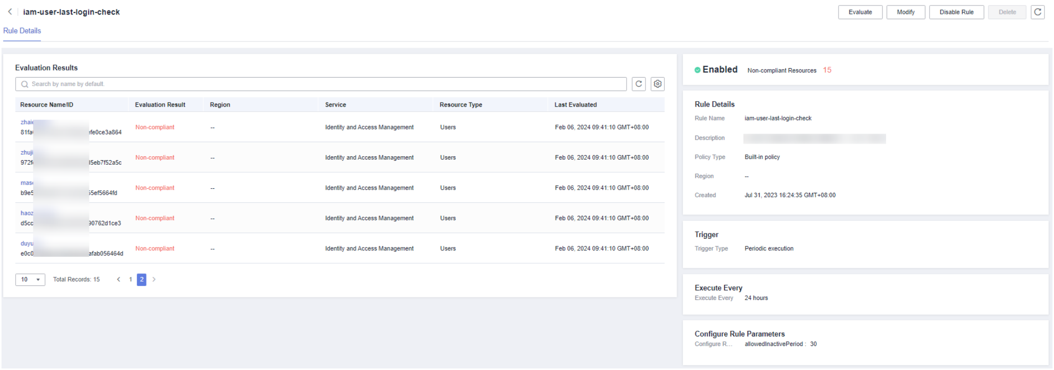
Step 3 In the navigation pane on the left, choose **Resource Compliance**.

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

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

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

Figure 3-5 Rule details



Evaluation Results

Search by name by default.

Resource Name/ID	Evaluation Result	Region	Service	Resource Type	Last Evaluated
zhai[redacted] 81fa[redacted]fe0ce3a864	Non-compliant	--	Identity and Access Management	Users	Feb 06, 2024 09:41:10 GMT+08:00
zhuji[redacted] 972f[redacted]i5eb7f52a5c	Non-compliant	--	Identity and Access Management	Users	Feb 06, 2024 09:41:10 GMT+08:00
mas[redacted] b9e5[redacted]5ef5664fd	Non-compliant	--	Identity and Access Management	Users	Feb 06, 2024 09:41:10 GMT+08:00
haoz[redacted] d5cc[redacted]90762d1ce3	Non-compliant	--	Identity and Access Management	Users	Feb 06, 2024 09:41:10 GMT+08:00
duyu[redacted] e0c0[redacted]afab056464d	Non-compliant	--	Identity and Access Management	Users	Feb 06, 2024 09:41:10 GMT+08:00

10 Total Records: 15 ‹ 1 2 ›

● Enabled Non-compliant Resources 15

Rule Details

Rule Name iam-user-last-login-check

Description [redacted]

Policy Type Built-in policy

Region --

Created Jul 31, 2023 16:24:35 GMT+08:00

Trigger

Trigger Type Periodic execution

Execute Every

Execute Every 24 hours

Configure Rule Parameters

Configure R... allowedInactivePeriod : 30

NOTE

A rule may be in one of the following statuses:

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

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

----End

3.1.4 Triggering a Rule

Scenarios

Rules can be triggered automatically or manually.

- **Automatic**

  A rule will be automatically triggered:

  – When you add a rule.

  – When you modify a rule

   - When you enable a rule
   - When there is a change to any of your monitored resources if you set **Trigger Type** to **Configuration change**.

  At a specific frequency if you set **Trigger Type** to **Periodic execution**.

- **Manual**

  You can manually initiate rule evaluation at any time through the console or the **run-evaluation** API.

Limitations and Constraints

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

- If you have never enabled the resource recorder, no resources will be available for evaluation.
- The resource recorder only collects data of specified resources within the monitoring scope that you have configured when you enable the resource recorder.
- If you enable the resource recorder and then disable it after a period of time, the recorder only collects and evaluates resource data during the period when it is enabled.

Procedure

Step 1 Log in to the management console.

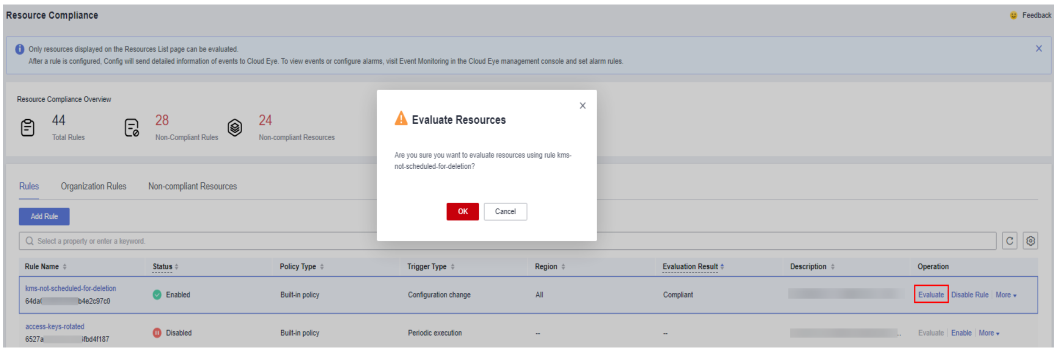
Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

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

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

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

Figure 3-6 Manually triggering 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 in the Cloud Eye management console and set alarm rules.

Resource Compliance Overview

44 Total Rules
28 Non-Compliant Rules
24 Non-compliant Resources

Evaluate Resources

Are you sure you want to evaluate resources using rule kms-not-scheduled-for-deletion?

Rule Name	Status	Policy Type	Trigger Type	Region	Evaluation Result	Description	Operation
kms-not-scheduled-for-deletion 64da[redacted]b4e2c97c0	Enabled	Built-in policy	Configuration change	All	Compliant	[redacted]	Evaluate Disable Rule More
access-keys-rotated 6527a[redacted]fbd4f187	Disabled	Built-in policy	Periodic execution	--	--	[redacted]..	Evaluate Enable More

----End

3.1.5 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

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.

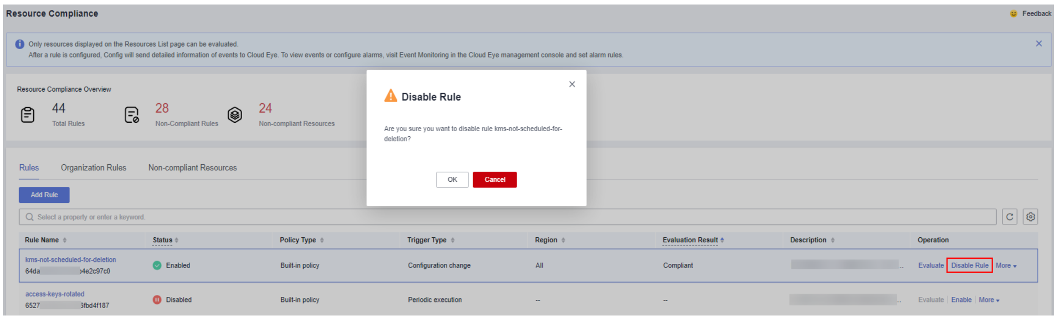
Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

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 3-7 Disabling 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 in the Cloud Eye management console and set alarm rules.

Resource Compliance Overview

44 Total Rules
28 Non-Compliant Rules
24 Non-compliant Resources

Disable Rule

Are you sure you want to disable rule kms-not-scheduled-for-deletion?

Rule Name	Status	Policy Type	Trigger Type	Region	Evaluation Result	Description	Operation
kms-not-scheduled-for-deletion 64da[redacted]4e2c97c0	Enabled	Built-in policy	Configuration change	All	Compliant	[redacted]	Evaluate Disable Rule More
access-keys-rotated 6527[redacted]5fbd4f187	Disabled	Built-in policy	Periodic execution	--	--	[redacted]	Evaluate Enable More

----End

Enabling a Rule

Step 1 Log in to the management console.

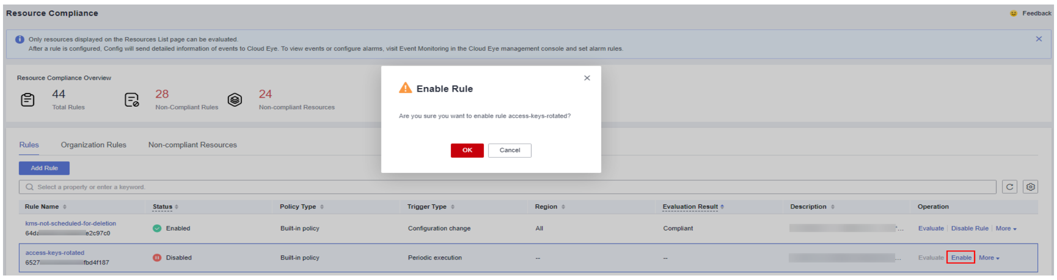
Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

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**.

Figure 3-8 Enabling 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 in the Cloud Eye management console and set alarm rules.

Are you sure you want to enable rule access-keys-rotated?

Rule Name	Status	Policy Type	Trigger Type	Region	Evaluation Result	Description	Operation
kms-not-scheduled-for-deletion 64d[redacted]e2c97c0	Enabled	Built-in policy	Configuration change	All	Compliant	[redacted]	Evaluate | Disable Rule | More
access-keys-rotated 6527[redacted]fbd4f187	Disabled	Built-in policy	Periodic execution	--	--	[redacted]	Evaluate | Enable | More

----End

Modifying a Rule

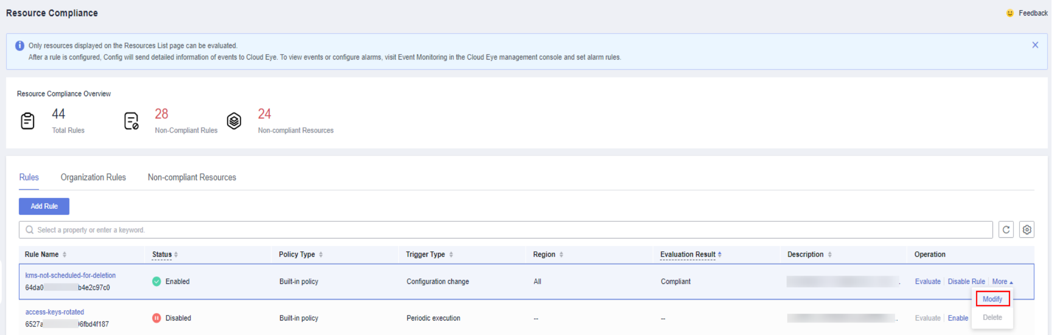
Step 1 Log in to the management console.

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 3-9 Modifying 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 in the Cloud Eye management console and set alarm rules.

Rule Name	Status	Policy Type	Trigger Type	Region	Evaluation Result	Description	Operation
kms-not-scheduled-for-deletion 64da0[redacted]b4e2c97c0	Enabled	Built-in policy	Configuration change	All	Compliant	[redacted]	Evaluate | Disable Rule | More
access-keys-rotated 6527a[redacted])6fbd4f187	Disabled	Built-in policy	Periodic execution	--	--	[redacted]	Evaluate | Enable

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

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

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

----End

Deleting a Rule

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

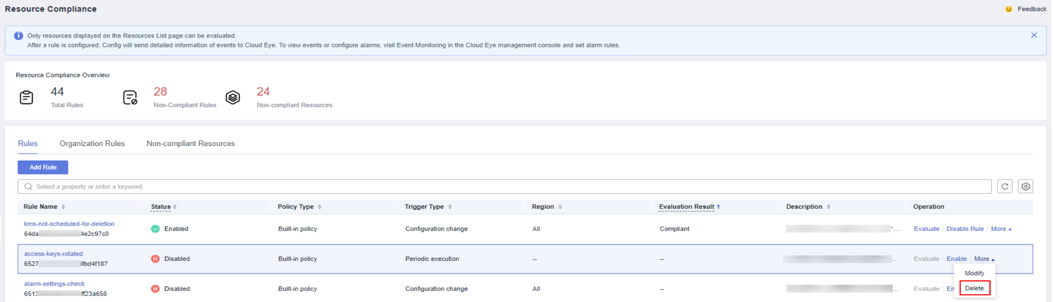
Step 1 Log in to the management console.

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

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

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

Figure 3-10 Deleting 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 in the Cloud Eye management console and set alarm rules.

Resource Compliance Overview

44 Total Rules
28 Non-Compliant Rules
24 Non-compliant Resources

Rule Name	Status	Policy Type	Trigger Type	Region	Evaluation Result	Description	Operation
kms-not-scheduled-for-deletion 64da[redacted]4e2c97c0	Enabled	Built-in policy	Configuration change	All	Compliant	[redacted]	Evaluate | Disable Rule | More
access-keys-rotated 6527[redacted]fbd4f187	Disabled	Built-in policy	Periodic execution	--	--	[redacted]	Evaluate | Enable | More
alarm-settings-check 6513[redacted]ff23a658	Disabled	Built-in policy	Configuration change	All	--	[redacted]	Evaluate | En

Step 5 Click **OK**.

----End

3.1.6 Example Custom Rules

3.1.6.1 Example Functions (Python)

Example Function for Evaluations Triggered by Configuration Changes

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

```
import 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.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", {})
    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 for 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.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 IAM API ShowDomainLoginPolicy is invoked.
In this case, you may need to set a timeout and memory limit for the function.
"""
def evaluate_compliance(context, domain_id):
    credentials = GlobalCredentials(context.getAccessKey(), context.getSecretKey())
    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**.

3.1.6.2 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
  }
}
```

3.2 Organization Rules

3.2.1 Adding a Predefined Organization Rule

Scenarios

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

A deployed organization rule will be displayed in the rule list of each 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

- Up to 500 rules can be added to an account.
- The **Organization Rules** tab is inaccessible for a non-organization member.

NOTICE

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

- If you have never enabled the resource recorder, no resources will be available for evaluation.
- If you have enabled the resource recorder and a monitoring scope is configured, only resources within the monitoring scope can be evaluated.
- If you enable the resource recorder and then disable it after a period of time, only resource data collected during the period when the resource recorder is enabled can be evaluated.

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

Procedure

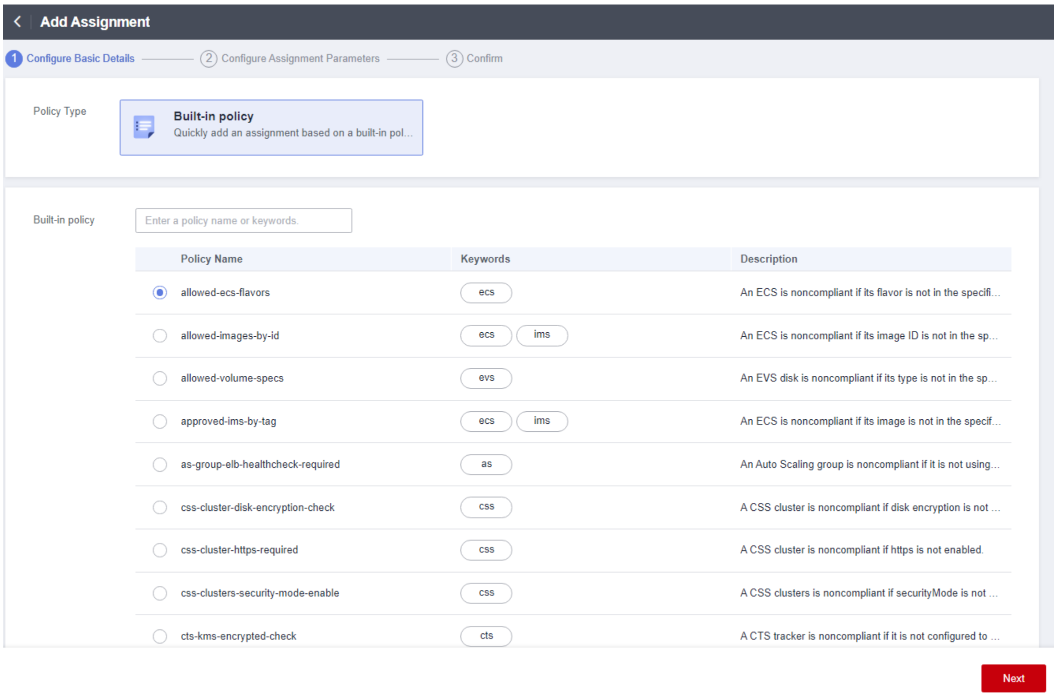
Step 1 Sign in to the Config console as an organization administrator or an agency administrator of Config.

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

Step 3 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 3-11 Basic configuration



Add Assignment

1 Configure Basic Details — 2 Configure Assignment Parameters — 3 Confirm

Policy Type: Built-in policy
Quickly add an assignment based on a built-in pol...

Built-in policy: Enter a policy name or keywords.

	Policy Name	Keywords	Description
●	allowed-ecs-flavors	ecs	An ECS is noncompliant if its flavor is not in the specifi...
○	allowed-images-by-id	ecs ims	An ECS is noncompliant if its image ID is not in the sp...
○	allowed-volume-specs	evs	An EVS disk is noncompliant if its type is not in the sp...
○	approved-ims-by-tag	ecs ims	An ECS is noncompliant if its image is not in the specif...
○	as-group-elb-healthcheck-required	as	An Auto Scaling group is noncompliant if it is not using...
○	css-cluster-disk-encryption-check	css	A CSS cluster is noncompliant if disk encryption is not ...
○	css-cluster-https-required	css	A CSS cluster is noncompliant if https is not enabled.
○	css-clusters-security-mode-enable	css	A CSS clusters is noncompliant if securityMode is not ...
○	cts-kms-encrypted-check	cts	A CTS tracker is noncompliant if it is not configured to ...

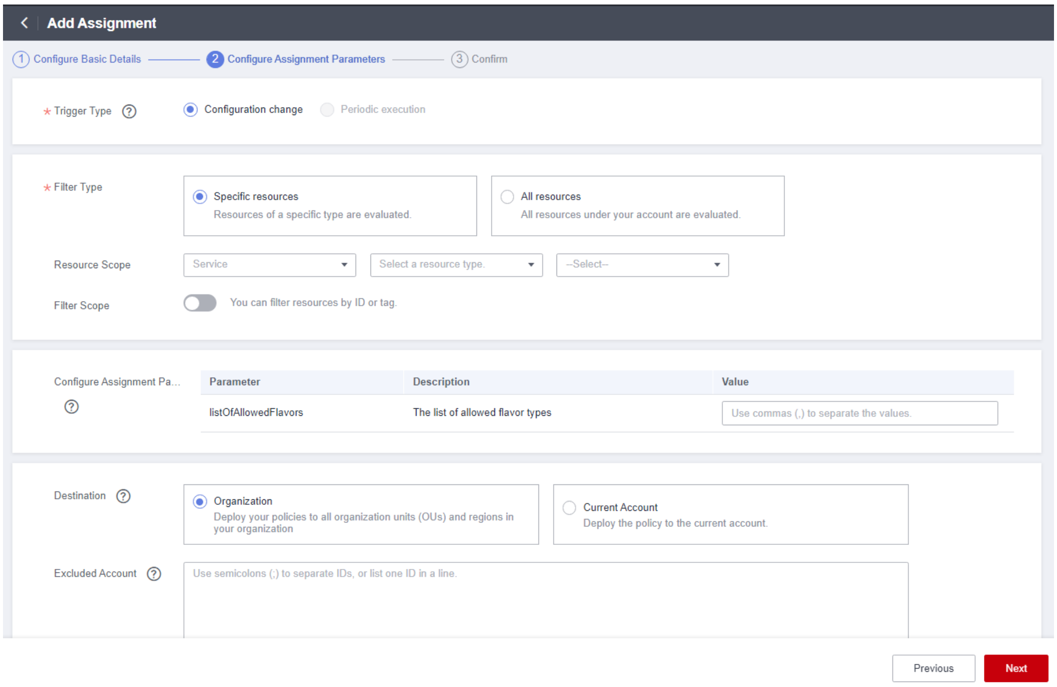
For details about parameter settings, see **Table 3-3**.

Table 3-3 Parameters of the basic configuration

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

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

Figure 3-12 Rule parameters



* 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 | Select a resource type. | --Select--

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

Configure Assignment Pa...

Parameter	Description	Value
listOfAllowedFlavors	The list of allowed flavor types	Use commas (,) to separate the values.

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.

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

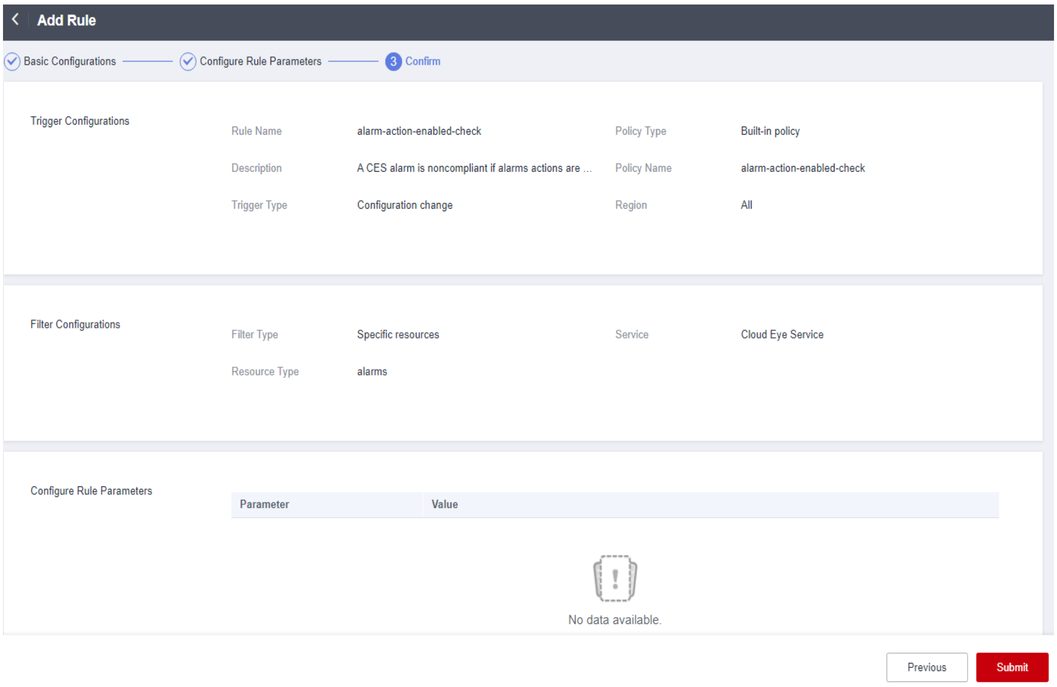
Table 3-4 Rule parameter description

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

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

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

Figure 3-13 Confirming a rule



Add Rule

Basic Configurations — Configure Rule Parameters — 3 Confirm

Trigger Configurations

Rule Name	alarm-action-enabled-check	Policy Type	Built-in policy
Description	A CES alarm is noncompliant if alarms actions are ...	Policy Name	alarm-action-enabled-check
Trigger Type	Configuration change	Region	All

Filter Configurations

Filter Type	Specific resources	Service	Cloud Eye Service
Resource Type	alarms		

Configure Rule Parameters

Parameter	Value

No data available.

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**.

3.2.2 Viewing an Organization Rule

Scenario

You can view organization rules and their details.

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

Viewing an Organization Rule

You can view details about a created organization rule.

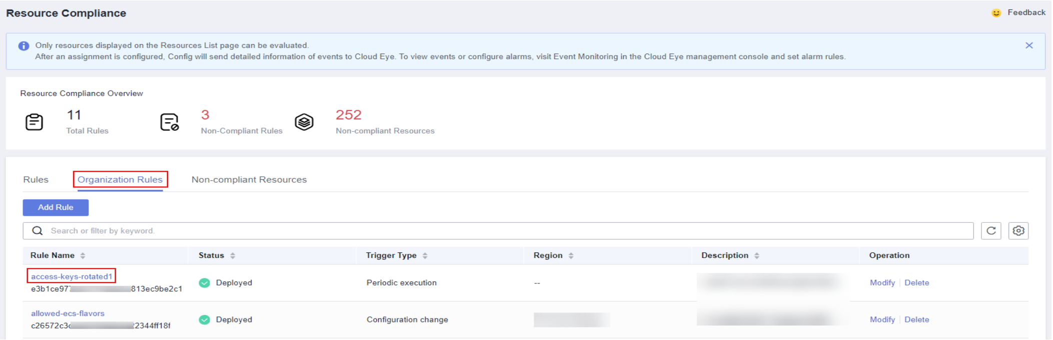
Step 1 Sign in to the Config console using the account with which the organization rules are created.

Step 2 Click ☰ in the upper left corner. 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 3-14 Viewing organization rules



Resource Compliance

Feedback

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.

Resource Compliance Overview

11 Total Rules

3 Non-Compliant Rules

252 Non-compliant Resources

Rules | Organization Rules | Non-compliant Resources

Add Rule

Search or filter by keyword.

Rule Name	Status	Trigger Type	Region	Description	Operation
access-keys-rotated1 e3b1ce97[redacted]813ec9be2c1	Deployed	Periodic execution	--	[redacted]	Modify | Delete
allowed-ecs-flavors c26572c3[redacted]2344ff18f	Deployed	Configuration change	[redacted]	[redacted]	Modify | Delete

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

NOTE

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

----End

Viewing Organization Rules Deployed to Member Accounts

A deployed organization rule will be displayed in the rule list of each member account in the organization. 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 Sign in to the management console as an organization member.

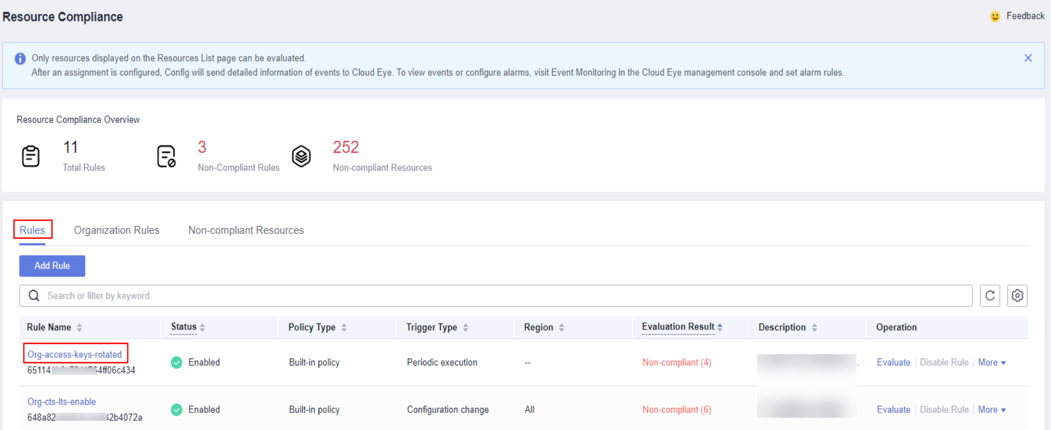
Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

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 3-15 Viewing organization rules deployed to member accounts



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.

Rule Name	Status	Policy Type	Trigger Type	Region	Evaluation Result	Description	Operation
Org-access-keys-rotated 65114[redacted]4ff06c434	Enabled	Built-in policy	Periodic execution	--	Non-compliant (4)	[redacted]	Evaluate | Disable Rule | More
Org-cts-lts-enable 648a82[redacted]2b4072a	Enabled	Built-in policy	Configuration change	All	Non-compliant (6)	[redacted]	Evaluate | Disable Rule | More

NOTE

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

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

----End

3.2.3 Modifying an Organization Rule

Scenarios

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

Procedure

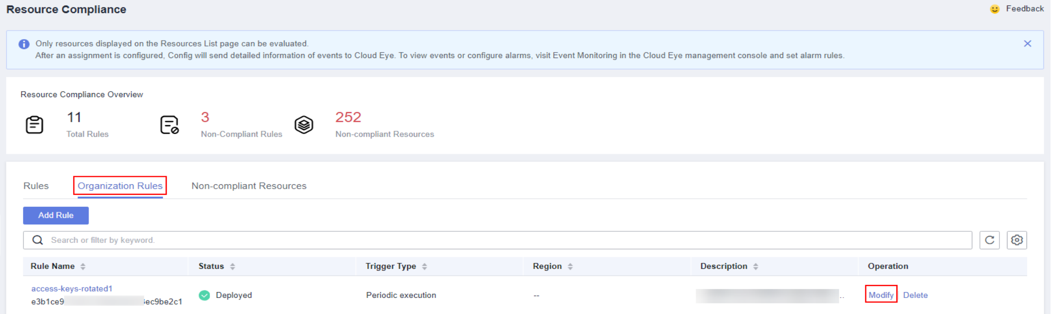
Step 1 Sign in to the Config console using the account with which the organization rules are created.

Step 2 Click ☰ in the upper left corner. 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 3-16 Editing an organization rule



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.

Rule Name	Status	Trigger Type	Region	Description	Operation
access-keys-rotated1 e3b1ce9[redacted]ec9be2c1	Deployed	Periodic execution	--	[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

3.2.4 Deleting an Organization Rule

Scenarios

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

Procedure

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

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

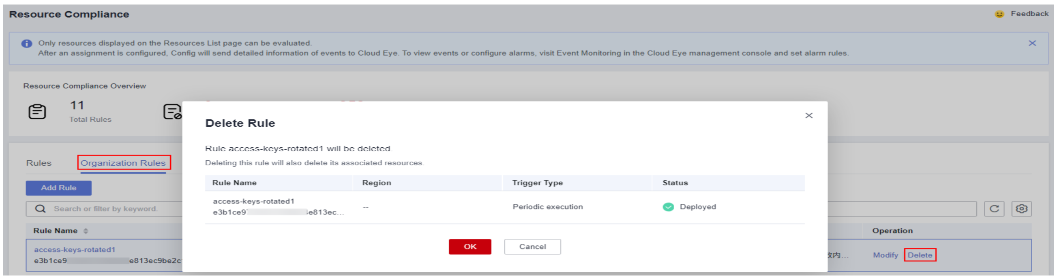
Step 3 In the navigation pane on the left, choose **Resource Compliance**.

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 **Delete Rule** dialog box, confirm the information and click **OK**.

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

Figure 3-17 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.

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

OK Cancel

----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 Viewing Noncompliant Resources

Scenarios

You can view all noncompliant resources detected by your rules.

Procedure

Step 1 Log in to the management console.

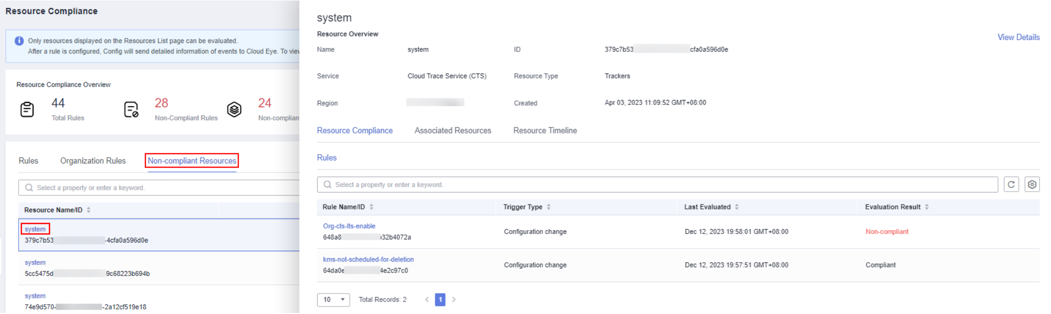
Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

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

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

Step 5 Click a resource name to view resource overview.

Figure 3-18 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

Resource Compliance Overview

44 Total Rules
28 Non-Compliant Rules
24 Non-complian

Rules | Organization Rules | Non-compliant Resources

Select a property or enter a keyword.

Resource Name/ID
system 379c7b53[redacted]-4cfa0a596d0e
system 5cc5475d[redacted]9c68223b694b
system 74e9d570-[redacted]-2a12cf519e18

system

Resource Overview

View Details

Name	system	ID	379c7b53[redacted]cfa0a596d0e
Service	Cloud Trace Service (CTS)	Resource Type	Trackers
Region	[redacted]	Created	Apr 03, 2023 11:09:52 GMT+08:00

Resource Compliance | Associated Resources | Resource Timeline

Rules

Select a property or enter a keyword.

Rule Name/ID	Trigger Type	Last Evaluated	Evaluation Result
Org-cts-lts-enable 648a8[redacted]32b4072a	Configuration change	Dec 12, 2023 19:58:01 GMT+08:00	Non-compliant
kms-not-scheduled-for-deletion 64da0e[redacted]4e2c97c0	Configuration change	Dec 12, 2023 19:57:51 GMT+08:00	Compliant

10 Total Records: 2 < 1 >

----End

3.4 Compliance Rule Concepts

3.4.1 Policies

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

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

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

Table 3-5 Policy parameters

Parameter	Description	Remarks
id	Policy ID	N/A
name	Policy name	A policy name can contain up to 64 characters.
display_name	Display name of a policy	A policy display name can contain up to 64 characters.

Parameter	Description	Remarks
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.
policy_type	Policy type The options are as follows: ● **builtin** ● **custom**	● **builtin**: specifies the type of policies that are provided and maintained by Config. For details, see **Predefined Policies**. ● **custom**: specifies the type of policies that are customized by users.

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

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

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

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

3.4.2 Rule

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

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

Table 3-6 Rule in JSON

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

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

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

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

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

NOTE

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

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

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

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

```
{
  "id": "719d8696dfb78231e6f2f719",
  "name": "test_consume_policy",
"description": "A resource is non-compliant if it does not contain the specific tag.",
  "policy_filter": {
      "region_id": "regionid_1",
      "resource_provider": "ecs",
      "resource_type": "cloudservers",
      "tag_key": null,
      "tag_value": null
  },
  "period": null,
  "state": "Enabled",
  "created": "2022-07-19T01:34:14.266Z",
  "updated": "2022-07-19T01:34:14.266Z",
  "policy_definition_id": null,
  "custom_policy": {
    "function_urn": "urn:fss:regionid_1:projectidforpolicy:function:default:test_consume_policy:latest",
    "auth_type": "agency",
    "auth_value": {"agency_name": "rms_fg_agency"}
  },
  "parameters": {
      "vpcId": {"value": "allowed-vpc-id"}
    }
  }
}
```

3.4.3 Evaluation Results

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

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

Table 3-7 Evaluation result in JSON

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

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

The following JSON indicates a non-compliant evaluation result:

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

3.5 Predefined Policies

3.5.1 Predefined Policy List

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

The following table lists predefined policies provided by Config.

Table 3-8 Predefined policies

Service	Policy	Triggered By	Object
General policies	**Resource Names Meet Regular Expression Requirements**	Configuration change	All resources

Service	Policy	Triggered By	Object
	Resources Are Attached with All the Specified Tags	Configuration change	Supported Services and Resources
	Resources Are Attached with One of the Specified Tags	Configuration change	Supported Services and Resources
	Tag Prefixes and Suffixes Check	Configuration change	Supported Services and Resources
	A Resource Is Attached with at Least One Tag	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
	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

Service	Policy	Triggered By	Object
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	**CodeArts Clusters Are Available**	Configuration change	codeartsdeploy.host-cluster
MapReduce Service (MRS)	**MRS Clusters Are Attached with Specified Security Groups**	Configuration change	mrs.mrs
	MRS Clusters Are in Specified VPSs	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 Have No Public IPs Attached	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	vpcep.endpoints
Web Application Firewall (WAF)	**WAF Instances Are Attached with Protection Policies**	Configuration change	waf.instance
	WAF Protection Policies Are Not Empty	Configuration change	waf.policy

Service	Policy	Triggered By	Object
ELB	**Elastic load balancers do not have public IP addresses 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
Elastic IP (EIP)	**Bandwidth Check**	Configuration change	vpc.publicips
	Idle Elastic IP Check	Configuration change	vpc.publicips
	Elastic IPs Attached Within a Given 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
Scalable File Service (SFS)	**Encryption Check**	Configuration change	sfsturbo.shares
Elastic Cloud Server (ECS)	**Flavor Check**	Configuration change	ecs.cloudservers
	Image Check by ID	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
	Login Mode Check	Configuration change	ecs.cloudservers
	ECSs Cannot Be Accessed Through Public Networks	Configuration change	ecs.cloudservers
	An ECS Does Not Have Multiple IPs Attached	Configuration change	ecs.cloudservers
	Idle ECS Check	Periodic	ecs.cloudservers
	All ECSs Are Attached with at Leat One IAM Agency	Configuration change	ecs.cloudservers
	Image Check	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
	DCS Memcached Instances Do Not Have Public IPs Attached	Configuration change	dcs.memcached
	Access Mode Check	Configuration change	dcs.memcached

Service	Policy	Triggered By	Object
	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 Public IPs 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
Content Delivery Network (CDN)	**CDN Uses HTTPS Certificates**	Configuration change	cdn.domains
	Origin Protocol Policy Check	Configuration change	cdn.domains
	TLS Version Check	Configuration change	cdn.domains
	Certificate Source Check	Configuration change	cdn.domains

Service	Policy	Triggered By	Object
Config	**The Resource Recorder Has Been Enabled**	Periodic	config.trackers
Data Warehouse Service (DWS)	**KMS Encryption Check**	Configuration change	dws.clusters
	DWS Clusters Have Enabled Audit Log Dumps	Configuration change	dws.clusters
	DWS Clusters Have Enabled Automated Snapshots	Configuration change	dws.clusters
	DWS Clusters Use SSL	Configuration change	dws.clusters
	DWS Clusters Are Not Attached with Any Public IPs	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
Data Encryption Workshop (DEW)	**Key Status Check**	Configuration change	kms.keys
	Key Rotation Has Been Enabled	Configuration change	kms.keys
	CSMS Secretes Are Rotated	Configuration change	csms.secrets
Identity and Access Management (IAM)	**Key Rotation Check**	Periodic	iam.users
	No Blocked Actions on KMS Keys	Configuration changes	iam.roles &iam.policies

Service	Policy	Triggered By	Object
	Each User Group Has at Least One User	Configuration change	iam.groups
	Password Policy 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 Access Key Is Unavailable	Periodic	iam.users
	Access Mode Check	Configuration change	iam.users
	Access Key Creation Check	Configuration change	iam.users
	IAM Users Are in at Least One User Group	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
	MFA Has Been Enabled for the Root Account	Periodic	iam.users

Service	Policy	Triggered By	Object
	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
Document Database Service (DDS)	**SSL Has Been Enabled**	Configuration change	dds.instances
	Instance Type Check	Configuration change	dds.instances
	DDS Instances Do Not Have Public IPs	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)	**Unused ACL Check**	Configuration change	vpc.firewallGroups
	Default Security Group Check	Configuration change	vpc.securityGroups
	VPCs Have Enabled Flow Logs	Configuration change	vpc.vpcs
	Security Groups Only Allow Traffic Over Some Ports	Configuration change	vpc.securityGroups
	Ports Have Addresses Restricted	Configuration change	vpc.securityGroups

Service	Policy	Triggered By	Object
	SSH Check	Configuration change	vpc.securityGroups
	All Accessible Ports Are Whitelisted	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 Created For KMS Events	Periodic	ces.alarms
	Alarm Rules Have Been Created for OBS Bucket Policy Changes	Periodic	ces.alarms
	An Alarm Rule Has Been Created for the Specified Metric	Periodic	ces.alarms
	Alarm Rule Configurations Check	Configuration change	ces.alarms
	Alarm Rules Have Been Created for VPC Changes	Periodic	ces.alarms
Cloud Container Engine (CCE)	**End of Maintenance Check**	Configuration change	cce.clusters
	Oldest Supported Version Check	Configuration change	cce.clusters
	CCE Clusters Are Not Publicly Accessible	Configuration change	cce.clusters
	Flavor Check	Configuration change	cce.clusters

Service	Policy	Triggered By	Object
Cloud Trace Service (CTS)	**CTS Trackers Are Encrypted**	Configuration change	cts.trackers
	Log Transfer to LTS Is Enabled	Configuration change	cts.trackers
	Trackers Have Been Created for the Specified OBS Bucket	Periodic	cts.trackers
	Trace File Verification Is Enabled	Configuration change	cts.trackers
	At Least One Tracker Has Been Created	Periodic	cts.trackers
	There Are Trackers In the Specified Regions	Periodic	cts.trackers
Relational Database Service (RDS)	**GaussDB Instances Are in the Specified VPC**	Configuration change	gaussdb.instance
	Single-AZ Cluster Check	Configuration change	nosql.instances
	GaussDB NoSQL Backup Check	Configuration change	nosql.instances
	GaussDB NoSQL Instances Use Disk Encryption	Configuration change	nosql.instances
	Error Log Collection Is Enabled for GaussDB NoSQL Instances	Configuration change	nosql.instances
	GaussDB NoSQL Instances Support Slow Query Log Collection	Configuration change	nosql.instances
	Audit Logs Are Collected for GaussDB Instances	Configuration change	gaussdb.instance
	Automated Backup Is Enabled	Configuration change	gaussdb.instance

Service	Policy	Triggered By	Object
	Error Log Collection Is Enabled for GaussDB Instances	Configuration change	gaussdb.instance
	GaussDB Instances Support Slow Query Log Collection	Configuration change	gaussdb.instance
	Audit Logs Are Collected for GaussDB for MySQL Instances	Configuration change	gaussdb.instance
	Backup Is Enabled for GaussDB for MySQL Instances	Configuration change	gaussdb.instance
	Error Log Collection Is Enabled for GaussDB for MySQL Instances	Configuration change	gaussdb.instance
	GaussDB for MySQL Support Slow Query Log Collection	Configuration change	gaussdb.instance
	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 Public IPs	Configuration change	rds.instances
	RDS Instances Use KMS Encryption	Configuration change	rds.instances
	RDS Instances Are in the Specified VPC	Configuration change	rds.instances

Service	Policy	Triggered By	Object
	Both Error Logs and Slow Query Logs Are Collected for RDS Instances	Configuration change	rds.instances
	Flavor Check	Configuration change	rds.instances
Cloud Search Service (CSS)	**CSS Clusters Use Authority Verification**	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
	Security Mode Is Enabled for CSS Clusters	Configuration change	css.clusters
	CSS Clusters Cannot Be Accessed by All Public IPs	Configuration change	css.clusters
	Kibana Cannot Be Accessed by All Public IPs	Configuration change	css.clusters

Service	Policy	Triggered By	Object
Elastic Volume Service (EVS)	**EVS Disk Type Check**	Configuration changes	evs.volumes
	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
Cloud Certificate Manager (CCM)	**Expiration Check for Private CAs**	Periodic	pca.ca
	Expiration Check for Private Certificates	Periodic	pca.cert
Distributed Message Service (for Kafka)	**SSL Is Required for DMS Kafka Access over Private Networks**	Configuration change	dms.kafkas
	SSL Is Required for DMS Kafka over Public Networks	Configuration change	dms.kafkas
	DMS Kafka Instances Are Not Publicly Accessible	Configuration change	dms.kafkas
Distributed Message Service for RabbitMQ (for RabbitMQ)	**SSL Is Enabled for DMS RabbitMq Instances**	Configuration change	dms.rabbitmqs
Distributed Message Service for RocketMQ (for RocketMQ)	**SSL Is Enabled for DMS Reliability Instances**	Configuration change	dms.reliabilitys
Organizations	**The Current Account Has Been Added to an Organization**	Periodic	organizations.account

Service	Policy	Triggered By	Object
Cloud Firewall (CFW)	**CFW Instances Are Attached with Protection Policies**	Configuration change	cfw.cfw_instance

3.5.2 General Service Policies

3.5.2.1 Resource Names Meet Regular Expression Requirements

Rule Details

Table 3-9 Rule details

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

3.5.2.2 Resources Are Attached with All the Specified Tags

Rule Details

Table 3-10 Rule details

Parameter	Description
Rule Name	required-all-tags
Identifier	required-all-tags

Parameter	Description
Description	If a resource is not attached with all the specified tag key, 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.

3.5.2.3 Resources Are Attached with One of the Specified Tags

Rule Details

Table 3-11 Rule details

Parameter	Description
Rule Name	required-tag-exist
Identifier	required-tag-exist
Description	If a resource is not attached with 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 tags. - TagValues: Indicates the specified tag values.

3.5.2.4 Tag Prefixes and Suffixes Check

Rule Details

Table 3-12 Rule details

Parameter	Description
Rule Name	resource-tag-key-prefix-suffix
Identifier	resource-tag-key-prefix-suffix

Parameter	Description
Description	If a resource is not attached with any tags that are defined by tag keys with specific 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.

3.5.2.5 A Resource Is Attached with at Least One Tag

Rule Details

Table 3-13 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

3.5.2.6 Resource Tag Check

Rule Details

Table 3-14 Rule details

Parameter	Description
Rule Name	required-tag-check

Parameter	Description
Identifier	required-tag-check
Description	If a resource is not attached with the specified tag, this resource is considered noncompliant.
Tag	tag
Trigger Type	Configuration change
Filter Type	**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.

3.5.2.7 Resources Are in Specified Enterprise Projects

Rule Details

Table 3-15 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.

3.5.2.8 Resources Are in Specified Regions

Rule Details

Table 3-16 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, the value of this parameter is **global**.

3.5.2.9 Resource Type Check by Specifying Allowed Resource Types

Rule Details

Table 3-17 Rule Details

Parameter	Description
Rule Name	resources-in-allowed-types
Identifier	resources-in-allowed-types
Description	If there are resources that are not within the specified resource types, the result is noncompliant.
Tag	type
Trigger Type	Configuration change
Filter Type	All resources
Rule Parameter	providerAndTypes: Resource types. The value format is ['provider.type'].

3.5.2.10 Resource Type Check by Specifying Unallowed Resource Types

Rule Details

Table 3-18 Rule details

Parameter	Description
Rule Name	resources-in-not-allowed-types
Identifier	resources-in-not-allowed-types
Description	If there are resources that are within the specified resource types, the result is noncompliant.
Tag	type
Trigger Type	Configuration change
Filter Type	All resources
Rule Parameter	providerAndTypes: Resource types. The value format is ['provider.type'].

3.5.3 API Gateway (APIG)

3.5.3.1 Dedicated API Gateways Have an Authorization Type Set

Rule Details

Table 3-19 Rule details

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

3.5.3.2 Dedicated API Gateways Have Logging Enabled

Rule Details

Table 3-20 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 API gateway, this gateway is considered non-compliant.
Tag	apig
Trigger Type	Configuration change
Filter Type	apig.instances
Configure Rule Parameters	None

3.5.3.3 Dedicated API Gateways Use SSL certificates

Rule Details

Table 3-21 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 API gateway, this gateway is considered noncompliant.
Tag	apig
Trigger Type	Configuration changes
Filter Type	apig.instances
Configure rule parameters	None

3.5.4 CodeArts Deploy

3.5.4.1 CodeArts Clusters Are Available

Rule Details

Table 3-22 Rule details

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

3.5.5 MapReduce Service (MRS)

3.5.5.1 MRS Clusters Are Attached with Specified Security Groups

Rule Details

Table 3-23 Rule details

Parameter	Description
Rule Name	mrs-cluster-in-allowed-security-groups
Identifier	mrs-cluster-in-allowed-security-groups
Description	If there is an MRS cluster that is not attached with the specified security group, the result 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.

3.5.5.2 MRS Clusters Are in Specified VPSs

Rule Details

Table 3-24 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**: indicatew the VPC ID. This is a string type parameter.

3.5.5.3 MRS Clusters Have Kerberos Enabled

Rule Details

Table 3-25 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

3.5.5.4 MRS Clusters Support Multi-AZ Deployment

Rule Details

Table 3-26 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
Filter Type	mrs.mrs
Configure Rule Parameters	None

3.5.5.5 MRS Clusters Have No Public IPs Attached

Rule Details

Table 3-27 Rule details

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

3.5.6 NAT Gateway

3.5.6.1 Private NAT Private Gateways Are in Specified VPCs

Rule Details

Table 3-28 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**: indicates the IDs of the specified VPCs. If there are no VPCs specified, all values are allowed. This is an array type parameter. You can include up to 10 VPCs.

3.5.7 VPC Endpoint (VPCEP)

3.5.7.1 VPC Endpoint Check for Specified Services

Rule Details

Table 3-29 Rule details

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

3.5.8 Web Application Firewall (WAF)

3.5.8.1 WAF Instances Are Attached with Protection Policies

Rule Details

Table 3-30 Rule details

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

3.5.8.2 WAF Protection Policies Are Not Empty

Rule Details

Table 3-31 Rule details

Parameter	Description
Rule Name	waf-policy-not-empty
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

3.5.9 Elastic Load Balance (ELB)

3.5.9.1 Elastic load balancers do not have public IP addresses attached.

Rule Details

Table 3-32 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

3.5.9.2 ELB Listeners Have Specified Security Policies Added

Rule Details

Table 3-33 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 the specified security policy. The default value is **tls-1-0**. Example values: tls-1-0, tls-1-1, tls-1-2, tls-1-0-inherit, tls-1-2-strict, tls-1-0-with-1-3, tls-1-2-fs-with-1-3, tls-1-2-fs, and hybrid-policy-1-0. For more information, see **TLS Security Policy**.

3.5.9.3 ELB Listeners Are Configured with HTTPS

Rule Details

Table 3-34 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 is not configured with HTTPS, this load balancer is noncompliant.
Tag	elb
Trigger Type	Configuration change
Filter Type	elb.loadbalancers
Configure Rule Parameters	None

3.5.9.4 Weight Check for Backend Servers

Rule Details

Table 3-35 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, the result is noncompliant.
Tag	elb
Trigger Type	Configuration change
Filter Type	elb.members
Configure Rule Parameters	**weight**: the weight of the backend server. Requests are routed to backend servers in the same backend server group based on their weights. The larger the weight is, the more requests the backend server receives. Value range: 0–100

3.5.10 Elastic IP (EIP)

3.5.10.1 Bandwidth Check

Rule Details

Table 3-36 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, the result is noncompliant.
Tag	eip
Trigger Type	Configuration change
Filter Type	vpc.publicips
Configure Rule Parameters	**bandwidthSize**: indicates the bandwidth size of an EIP. The unit is Mbit/s. This is a string type parameter.

3.5.10.2 Idle Elastic IP Check

Rule Details

Table 3-37 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

3.5.10.3 Elastic IPs Attached Within a Given Time

Rule Details

Table 3-38 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.

3.5.11 Auto Scaling (AS)

3.5.11.1 Priority Policy Check

Rule Details

Table 3-39 Rule details

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

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

Rule Details

Table 3-40 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, the result is noncompliant.
Tag	as
Trigger Type	Configuration change
Filter Type	as.scalingGroups
Configure Rule Parameters	None

3.5.11.3 Multi-AZ Deployment Has Been Configured

Rule Details

Table 3-41 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

3.5.12 Scalable File Service (SFS)

3.5.12.1 Encryption Check

Rule Details

Table 3-42 Rule details

Parameter	Description
Rule Name	sfsturbo-encrypted-check
Identifier	as-multiple-az
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

3.5.13 Elastic Cloud Server (ECS)

3.5.13.1 Flavor Check

Rule Details

Table 3-43 Rule details

Parameter	Description
Rule Name	allowed-ecs-flavors
Identifier	SFS Turbo
Description	If there are any unallowed ECS flavors, the result is noncompliant.
Tag	ecs
Trigger Type	Configuration change
Filter Type	ecs.cloudservers
Configure Rule Parameters	**listOfAllowedFlavors**: indicates the list of allowed ECS flavors. The value must be an array with up to 10 elements. Example ECS flavors are as follows: s6.small.1, s6.xlarge.2, m7.large.8, and t6.small.1. To get more details, see ECS documentation.

3.5.13.2 Image Check by ID

Rule Details

Table 3-44 Rule details

Parameter	Description
Rule Name	allowed-images-by-id
Identifier	allowed-images-by-id
Description	If there is an ECS configured with an unallowed image, the result is noncompliant.
Tag	ecs, ims
Trigger Type	Configuration change
Filter Type	ecs.cloudservers
Configure Rule Parameters	**listOfAllowedImages**: indicates the list of allowed image IDs. The value must be an array with up to 10 elements.

3.5.13.3 Image Check by Tag

Rule Details

Table 3-45 Rule details

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

3.5.13.4 Security Group Check by ID

Rule Details

Table 3-46 Rule details

Parameter	Description
Rule Name	ecs-in-allowed-security-groups
Identifier	ecs-in-allowed-security-groups
Description	If there are any ECSs configured with security groups that are within the specified scope, the result is noncompliant.
Tag	ecs
Trigger Type	Configuration change
Filter Type	ecs.cloudservers
Configure Rule Parameters	● **specifiedECSTagKey**: indicates the tag key of an ECS. The value must be a string. ● **specifiedECSTagValue**: indicates the 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**: indicates IDs of security groups. The value must be an array with up to 10 IDs.

3.5.13.5 VPC Check by ID

Rule Details

Table 3-47 Rule details

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

3.5.13.6 Login Mode Check

Rule Details

Table 3-48 Rule details

Parameter	Description
Rule Name	ecs-instance-key-pair-login
Identifier	ecs-instance-key-pair-login
Description	If there is an ECS whose login mode is not set as the key pair, the result is noncompliant.
Tag	ecs
Trigger Type	Configuration change
Filter Type	ecs.cloudservers
Configure Rule Parameters	None

3.5.13.7 ECSs Cannot Be Accessed Through Public Networks

Rule Details

Table 3-49 Rule details

Parameter	Description
Rule Name	ecs-instance-no-public-ip
Identifier	ecs-instance-no-public-ip
Description	If there is an ECS that is configured with a public IP, the result is noncompliant.
Tag	ecs
Trigger Type	Configuration change
Filter Type	ecs.cloudservers
Configure Rule Parameters	None

3.5.13.8 An ECS Does Not Have Multiple IPs Attached

Rule Details

Table 3-50 Rule details

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

3.5.13.9 Idle ECS Check

Rule Details

Table 3-51 Rule details

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

3.5.13.10 All ECSs Are Attached with at Leat One IAM Agency

Rule Details

Table 3-52 Rule details

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

3.5.13.11 Image Check

Rule Details

Table 3-53 Rule details

Parameter	Description
Rule Name	allowed-images-by-name
Identifier	allowed-images-by-name
Description	If the image of an ECS is not within the specified image scope, this ECS is noncompliant.
Tag	ecs
Trigger Type	Configuration change
Filter Type	ecs.cloudservers
Rule Parameter	imageNames: Names of images.

3.5.14 Distributed Cache Service (DCS)

3.5.14.1 DCS Memcached Instances Support SSL

Rule Details

Table 3-54 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

3.5.14.2 DCS Memcached Instances Are in a Specified VPC

Rule Details

Table 3-55 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**: indicates the VPC ID. The value must be a string.

3.5.14.3 DCS Memcached Instances Do Not Have Public IPs Attached

Rule Details

Table 3-56 Rule details

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

3.5.14.4 Access Mode Check

Rule Details

Table 3-57 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

3.5.14.5 DCS Redis Instances Support SSL

Rule Details

Table 3-58 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

3.5.14.6 Cross-AZ Deployment Check

Rule Details

Table 3-59 Rule details

Parameter	Description
Rule Name	dcs-redis-high-tolerance
Identifier	cs-redis-high-tolerance
Description	If cross-AZ deployment is not configured for DCS Redis instances, the result is noncompliant.
Tag	dcs
Trigger Type	Configuration change
Filter Type	dcs.redis
Configure Rule Parameters	None

3.5.14.7 DCS Redis Instances Are in the Specified VPC

Rule Details

Table 3-60 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**: indicates the VPC ID. The value must be a string.

3.5.14.8 DCS Redis Instances Do Not Have Public IPs Attached

Rule Details

Table 3-61 Rule details

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

3.5.14.9 Access Mode Check

Rule Details

Table 3-62 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

3.5.15 FunctionGraph

3.5.15.1 Concurrency Check

Rule Details

Table 3-63 Rule details

Parameter	Description
Rule Name	function-graph-concurrency-check
Identifier	If the concurrent request amount allowed by a function is not within the specified range, the result is noncompliant.
Description	If the number of concurrent requests of a function is not within the specified range, this function is noncompliant.
Tag	fgs
Trigger Type	Configuration change
Filter Type	fgs.functions

Parameter	Description
Configure Rule Parameters	- **concurrencyLimitLow**: indicates the minimum number of concurrent requests. The value must be an integer. - **concurrencyLimitHigh**: indicates the maximum number of concurrent requests. The value must be an integer.

3.5.15.2 Functions Are in the Specified VPC

Rule Details

Table 3-64 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**: indicates the VPC ID. The value must be a string.

3.5.15.3 Public Access Check

Rule Details

Table 3-65 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

Parameter	Description
Trigger Type	Configuration change
Filter Type	fgs.functions
Configure Rule Parameters	None

3.5.15.4 Basic Configuration Check

Rule Details

Table 3-66 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**: indicates the runtime list. The value must be an array. ● **timeout**: indicates the maximum amount of time that a client waits for a request to complete (in seconds). The value must be an integer. ● **memorySize**: indicates maximum memory size (MB). The value must be an integer.

3.5.16 Content Delivery Network (CDN)

3.5.16.1 CDN Uses HTTPS Certificates

Rule Details

Table 3-67 Rule details

Parameter	Description
Rule Name	cdn-enable-https-certificate
Identifier	cdn-enable-https-certificate
Description	If there is a domain that does not have an HTTPS certificate configured, the result is noncompliant.
Tag	cdn
Trigger Type	Configuration change
Filter Type	cdn.domains
Configure Rule Parameters	None

3.5.16.2 Origin Protocol Policy Check

Rule Details

Table 3-68 Rule details

Parameter	Description
Rule Name	cdn-origin-protocol-no-http
Identifier	cdn-origin-protocol-no-http
Description	If HTTPS is not required for communication between CDN and origins, the result is noncompliant.
Tag	cdn
Trigger Type	Configuration change
Filter Type	cdn.domains
Configure Rule Parameters	None

3.5.16.3 TLS Version Check

Rule Details

Table 3-69 Rule details

Parameter	Description
Rule Name	cdn-security-policy-check
Identifier	cdn-security-policy-check
Description	If there is a domain that uses a TLS version earlier than v1.2, the result is noncompliant.
Tag	cdn
Trigger Type	Configuration change
Filter Type	cdn.domains
Configure Rule Parameters	None

3.5.16.4 Certificate Source Check

Rule Details

Table 3-70 Rule details

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

3.5.17 Config

3.5.17.1 The Resource Recorder Has Been Enabled

Rule Details

Table 3-71 Rule details

Parameter	Description
Rule Name	tracker-config-enabled-check
Identifier	tracker-config-enabled-check
Description	If the resource recorder has not been enabled, the result is noncompliant.
Tag	config
Trigger Type	Periodic
Filter Type	config.trackers
Configure Rule Parameters	None

3.5.18 Data Warehouse Service (DWS)

3.5.18.1 KMS Encryption Check

Rule Details

Table 3-72 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

3.5.18.2 DWS Clusters Have Enabled Audit Log Dumps

Rule Details

Table 3-73 Rule details

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

3.5.18.3 DWS Clusters Have Enabled Automated Snapshots

Rule Details

Table 3-74 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

3.5.18.4 DWS Clusters Use SSL

Rule Details

Table 3-75 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

3.5.18.5 DWS Clusters Are Not Attached with Any Public IPs

Rule Details

Table 3-76 Rule details

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

3.5.19 Data Replication Service (DRS)

3.5.19.1 Network Type Check for DR Tasks

Rule Details

Table 3-77 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

3.5.19.2 Network Type Check for Migration Tasks

Rule Details

Table 3-78 Rule details

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

3.5.19.3 Network Type Check for Synchronization Tasks

Rule Details

Table 3-79 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

3.5.20 Data Encryption Workshop (DEW)

3.5.20.1 Key Status Check

Rule Details

Table 3-80 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

3.5.20.2 Key Rotation Has Been Enabled

Rule Details

Table 3-81 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

3.5.20.3 CSMS Secretes Are Rotated

Rule Details

Table 3-82 Rule details

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

3.5.21 Identity and Access Management (IAM)

3.5.21.1 Key Rotation Check

Rule Details

Table 3-83 Rule details

Parameter	Description
Rule Name	access-keys-rotated
Identifier	access-keys-rotated
Description	If there is an access key that has not been rotated for longer than the specified time, the result is noncompliant.
Tag	iam
Trigger Type	Periodic
Filter Type	iam.users
Configure Rule Parameters	**maxAccessKeyAge**: indicates the maximum number of days that the AK/SK is allowed to remain unchanged. The default value is 90 days.

3.5.21.2 No Blocked Actions on KMS Keys

Rule Details

Table 3-84 Rule details

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

3.5.21.3 Each User Group Has at Least One User

Rule Details

Table 3-85 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 user, this user group is noncompliant.
Tag	iam
Trigger Type	Configuration change
Filter Type	iam.groups
Configure Rule Parameters	None

3.5.21.4 Password Policy Check

Rule Details

Table 3-86 Rule details

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

3.5.21.5 Unintended Policy Check

Rule Details

Table 3-87 Rule details

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

3.5.21.6 Admin Permissions Check

Rule Details

Table 3-88 Rule details

Parameter	Description
Rule Name	iam-policy-no-statements-with-admin-access
Identifier	iam-policy-no-statements-with-admin-access
Description	If there is an IAM policy or role that grants administrator permissions (the **Action** element is ***:*:***, ***:***, or *****), the result is noncompliant.
Tag	iam
Trigger Type	Configuration change
Filter Type	iam.roles, iam.policies
Configure Rule Parameters	None

3.5.21.7 Custom Policies Do Not Allow All Actions for a Service

Rule Details

Table 3-89 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, the result is noncompliant
Tag	iam
Trigger Type	Configuration change
Filter Type	iam.roles, iam.policies
Configure Rule Parameters	None

3.5.21.8 The Root Access Key Is Unavailable

Rule Details

Table 3-90 Rule details

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

3.5.21.9 Access Mode Check

Rule Details

Table 3-91 Rule details

Parameter	Description
Rule Name	iam-user-access-mode
Identifier	iam-user-access-mode
Description	If there is an IAM user that can accesses IAM through both the console and an API, the result is noncompliant.
Tag	iam
Trigger Type	Configuration change
Filter Type	iam.users
Configure Rule Parameters	None

3.5.21.10 Access Key Creation Check

Rule Details

Table 3-92 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 there is a user who has a console password and whose AK/SK pair is created when this user is created, the result is noncompliant.
Tag	iam
Trigger Type	Configuration change
Filter Type	iam.users
Configure Rule Parameters	None

3.5.21.11 IAM Users Are in at Least One User Group

Rule Details

Table 3-93 Rule details

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

3.5.21.12 Last Login Check

Rule Details

Table 3-94 Rule details

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

3.5.21.13 Multi-Factor Authentication Check

Rule Details

Table 3-95 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

3.5.21.14 A User Does Not have Multiple Active Access Keys

Rule Details

Table 3-96 Rule details

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

3.5.21.15 MFA Has Been Enabled for Console Login

Rule Details

Table 3-97 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

3.5.21.16 MFA Has Been Enabled for the Root Account

Rule Details

Table 3-98 Rule details

Parameter	Description
Rule Name	root-account-mfa-enabled
Identifier	root-account-mfa-enabled
Description	If multi-factor authentication is not enabled for the root user, the root user is noncompliant.
Tag	iam
Trigger Type	Periodic
Filter Type	iam.users
Configure Rule Parameters	None

3.5.21.17 All IAM Policies Are in Use

Rule Details

Table 3-99 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

3.5.21.18 All IAM Roles Are in Use

Rule Details

Table 3-100 Rule details

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

3.5.21.19 Login Protection Check

Rule Details

Table 3-101 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

3.5.22 Document Database Service (DDS)

3.5.22.1 SSL Has Been Enabled

Rule Details

Table 3-102 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

3.5.22.2 Instance Type Check

Rule Details

Table 3-103 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.

3.5.22.3 DDS Instances Do Not Have Public IPs

Rule Details

Table 3-104 Rule details

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

3.5.22.4 DDS Instances Are in the Specified VPC

Rule Details

Table 3-105 Rule details

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

3.5.23 Simple Message Notification (SMN)

3.5.23.1 Log Reporting to LTS Has Been Enabled

Rule Details

Table 3-106 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

3.5.24 Virtual Private Cloud (VPC)

3.5.24.1 Unused ACL Check

Rule Details

Table 3-107 Rule details

Parameter	Description
Rule Name	vpc-acl-unused-check
Identifier	vpc-acl-unused-check
Description	If there is a network ACL that has not been associated with any subnets, the result is noncompliant.
Tag	vpc
Trigger Type	Configuration change
Filter Type	vpc.firewallGroups
Configure Rule Parameters	None

3.5.24.2 Default Security Group Check

Rule Details

Table 3-108 Rule details

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

3.5.24.3 VPCs Have Enabled Flow Logs

Rule Details

Table 3-109 Rule details

Parameter	Description
Rule Name	vpc-flow-logs-enabled
Identifier	vpc-flow-logs-enabled
Description	If there is a flow log that has not been enabled for a VPC, the result is noncompliant.
Tag	vpc
Trigger Type	Configuration change
Filter Type	vpc.vpcs
Configure Rule Parameters	None

3.5.24.4 Security Groups Only Allow Traffic Over Some Ports

Rule Details

Table 3-110 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 has no port specified, this security group is noncompliant.
Tag	vpc
Trigger Type	Configuration change
Filter Type	vpc.securityGroups
Configure Rule Parameters	None

3.5.24.5 Ports Have Addresses Restricted

Rule Details

Table 3-111 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 addresses (0.0.0.0/0) to access a specified port, this security group is noncompliant.
Tag	vpc
Trigger Type	Configuration change
Filter Type	vpc.securityGroups
Configure Rule Parameters	**blockedPorts**: indicates the list of ports to be restricted. This is an array type parameter. The default value is **20, 21, 3306, and 3389**. ● **20**: File Transfer Protocol-data port ● **21**: File Transfer Protocol-control port ● **3306**: mysql port ● **3389**: Remote Desktop Protocol port

3.5.24.6 SSH Check

Rule Details

Table 3-112 Rule details

Parameter	Description
Rule Name	vpc-sg-restricted-ssh
Identifier	vpc-sg-restricted-ssh
Description	If the source address is set to **0.0.0.0/0** for the TCP 22 port, this security group is non-compliant.
Tag	vpc
Trigger Type	Configuration change
Filter Type	vpc.securityGroups

Parameter	Description
Configure Rule Parameters	None

3.5.24.7 All Accessible Ports Are Whitelisted

Rule Details

Table 3-113 Rule details

Parameter	Description
Rule Name	vpc-sg-by-white-list-ports-check
Identifier	vpc-sg-by-white-list-ports-check
Description	If a security group is set to allow traffic over a port that is not whitelisted, this security group is noncompliant.
Tag	vpc
Trigger Type	Configuration change
Filter Type	vpc.securityGroups
Rule Parameter	**white_list**: Whitelisted ports.

3.5.25 Virtual Private Network (VPN)

3.5.25.1 Connection State Check

Rule Details

Table 3-114 Rule details

Parameter	Description
Rule Name	vpn-connections-active
Identifier	vpn-connections-active
Description	If the state of a VPN connection is not connected, the result is noncompliant.
Tag	vpnaas
Trigger Type	Configuration change

Parameter	Description
Filter Type	vpnaas.vpnConnections, vpnaas.ipsec-site-connections
Configure Rule Parameters	None

3.5.26 Cloud Eye

3.5.26.1 Alarm Rules Are Enabled

Rule Details

Table 3-115 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

3.5.26.2 Alarm Rules Have Been Created For KMS Events

Rule Details

Table 3-116 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 KMS or deleting keys, the result is noncompliant.
Tag	ces, kms

Parameter	Description
Trigger Type	Periodic
Filter Type	ces.alarms
Configure Rule Parameters	None

3.5.26.3 Alarm Rules Have Been Created for OBS Bucket Policy Changes

Rule Details

Table 3-117 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, the result is noncompliant.
Tag	ces, obs
Trigger Type	Periodic
Filter Type	ces.alarms
Configure Rule Parameters	None

3.5.26.4 An Alarm Rule Has Been Created for the Specified Metric

Rule Details

Table 3-118 Rule details

Parameter	Description
Rule Name	alarm-resource-check
Identifier	alarm-resource-check
Description	If the specified metric is not configured with an alarm rule, the result is noncompliant.
Tag	ces
Trigger Type	Periodic

Parameter	Description
Filter Type	ces.alarms
Configure Rule Parameters	● **provider**: indicates a cloud service name. The value must be a string. ● **resourceType**: indicates a resource type. The value must be a string. ● **metricName**: indicates a metric name. The value must be a string.

3.5.26.5 Alarm Rule Configurations Check

Rule Details

Table 3-119 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 configuration standards, the result 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.

3.5.26.6 Alarm Rules Have Been Created for VPC Changes

Rule Details

Table 3-120 Rule details

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

3.5.27 Cloud Container Engine (CCE)

3.5.27.1 End of Maintenance Check

Rule Details

Table 3-121 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

3.5.27.2 Oldest Supported Version Check

Rule Details

Table 3-122 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

3.5.27.3 CCE Clusters Are Not Publicly Accessible

Rule Details

Table 3-123 Rule details

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

3.5.27.4 Flavor Check

Rule Details

Table 3-124 Rule details

Parameter	Description
Rule Name	allowed-cce-flavors
Identifier	allowed-cce-flavors
Description	If the flavor of a CCE cluster is not within the specified scope, this cluster is noncompliant.
Tag	cce
Trigger Type	Configuration change
Filter Type	cce.clusters
Rule Parameter	listOfAllowedFlavors: Cluster flavors

3.5.28 Cloud Trace Service (CTS)

3.5.28.1 CTS Trackers Are Encrypted

Rule Details

Table 3-125 Rule details

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

3.5.28.2 Log Transfer to LTS Is Enabled

Rule Details

Table 3-126 Rule details

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

3.5.28.3 Trackers Have Been Created for the Specified OBS Bucket

Rule Details

Table 3-127 Rule details

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

3.5.28.4 Trace File Verification Is Enabled

Rule Details

Table 3-128 Rule details

Parameter	Description
Rule Name	cts-support-validate-check
Identifier	cts-support-validate-check
Description	If **Verify Trace File** is not enabled for a CTS tracker, this tacker is noncompliant.
Tag	cts
Trigger Type	Configuration change
Filter Type	cts.trackers
Configure Rule Parameters	None

3.5.28.5 At Least One Tracker Has Been Created

Rule Details

Table 3-129 Rule details

Parameter	Description
Rule Name	cts-tracker-exists
Identifier	cts-tracker-exists
Description	If there are no trackers in the current account, the result is noncompliant.
Tag	cts
Trigger Type	Periodic
Filter Type	cts.trackers
Configure Rule Parameters	None

3.5.28.6 There Are Trackers In the Specified Regions

Rule Details

Table 3-130 Rule details

Parameter	Description
Rule Name	multi-region-cts-tracker-exists
Identifier	multi-region-cts-tracker-exists
Description	If there are no trackers in any of the specified regions, the result is noncompliant.
Tag	cts
Trigger Type	Periodic
Filter Type	cts.trackers
Configure Rule Parameters	**regionList**: indicates the specified regions. The value must be an array.

3.5.29 Relational Database Service (RDS)

3.5.29.1 GaussDB Instances Are in the Specified VPC

Rule Details

Table 3-131 Rule details

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

3.5.29.2 Single-AZ Cluster Check

Rule Details

Table 3-132 Rule details

Parameter	Description
Rule Name	gaussdb-nosql-deploy-in-single-az
Identifier	gaussdb-nosql-deploy-in-single-az
Description	If a GaussDB NoSQL cluster is deployed in a single availability zone, this cluster is noncompliant.
Tag	gaussdb nosql
Trigger Type	Configuration change
Filter Type	nosql.instances
Configure Rule Parameters	None

3.5.29.3 GaussDB NoSQL Backup Check

Rule Details

Table 3-133 Rule details

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

3.5.29.4 GaussDB NoSQL Instances Use Disk Encryption

Rule Details

Table 3-134 Rule details

Parameter	Description
Name	gaussdb-nosql-enable-disk-encryption
Identifier	gaussdb-nosql-enable-disk-encryption
Description	If **Disk Encryption** is disabled for a GaussDB NoSQL instance, this instance is noncompliant.
Tag	gaussdb nosql
Trigger Type	Configuration change
Filter Type	nosql.instances
Configure Rule Parameters	None

3.5.29.5 Error Log Collection Is Enabled for GaussDB NoSQL Instances

Rule Details

Table 3-135 Rule details

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

3.5.29.6 GaussDB NoSQL Instances Support Slow Query Log Collection

Rule Details

Table 3-136 Rule details

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

3.5.29.7 Audit Logs Are Collected for GaussDB Instances

Rule Details

Table 3-137 Rule details

Parameter	Description
Rule Name	gaussdb-instance-enable-auditLog
Identifier	gaussdb-instance-enable-auditLog
Description	If audit logs are not collected for a GaussDB instance, this instance is noncompliant.
Tag	gaussdb
Trigger Type	Configuration change
Filter Type	gaussdb.instance
Configure Rule Parameters	None

3.5.29.8 Automated Backup Is Enabled

Rule Details

Table 3-138 Rule details

Parameter	Description
Rule Name	gaussdb-instance-enable-backup
Identifier	gaussdb-instance-enable-backup
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

3.5.29.9 Error Log Collection Is Enabled for GaussDB Instances

Rule Details

Table 3-139 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

3.5.29.10 GaussDB Instances Support Slow Query Log Collection

Rule Details

Table 3-140 Rule details

Parameter	Description
Rule Name	gaussdb-instance-enable-slowLog
Identifier	gaussdb-instance-enable-slowLog
Description	If a GaussDB instance does not support slow query logs, this instance is noncompiant.
Tag	gaussdb
Trigger Type	Configuration change
Filter Type	gaussdb.instance
Configure Rule Parameters	None

3.5.29.11 Audit Logs Are Collected for GaussDB for MySQL Instances

Rule Details

Table 3-141 Rule details

Parameter	Description
Rule Name	gaussdb-mysql-instance-enable-auditlog
Identifier	gaussdb-mysql-instance-enable-auditlog
Description	If audit logs are not collected for a GaussDB for MySQL instance, this instance is noncompliant.
Tag	gaussdb
Trigger Type	Configuration change
Filter Type	gaussdb.instance
Configure Rule Parameters	None

3.5.29.12 Backup Is Enabled for GaussDB for MySQL Instances

Rule Details

Table 3-142 Rule details

Parameter	Description
Rule Name	gaussdb-mysql-instance-enable-backup
Identifier	gaussdb-mysql-instance-enable-backup
Description	If the backup is disabled for a GaussDB for MySQL instance, this instance is noncompliant.
Tag	gaussdb
Trigger Type	Configuration change
Filter Type	gaussdb.instance
Configure Rule Parameters	None

3.5.29.13 Error Log Collection Is Enabled for GaussDB for MySQL Instances

Rule Details

Table 3-143 Rule details

Parameter	Description
Rule Name	gaussdb-mysql-instance-enable-errorlog
Identifier	gaussdb-mysql-instance-enable-errorlog
Description	If error log collection is not enabled for a GaussDB for MySQL instance, this instance is noncompliant.
Tag	gaussdb
Trigger Type	Configuration change
Filter Type	gaussdb.instance
Configure Rule Parameters	None

3.5.29.14 GaussDB for MySQL Support Slow Query Log Collection

Rule Details

Table 3-144 Rule details

Parameter	Description
Rule Name	gaussdb-mysql-instance-enable-slowlog
Identifier	gaussdb-mysql-instance-enable-slowlog
Description	If a GaussDB for MySQL instance does not support slow query log collection, this instance is noncompliant.
Tag	gaussdb nosql
Trigger Type	Configuration change
Filter Type	gaussdb.instance
Configure Rule Parameters	None

3.5.29.15 Error Log Collection Is Enabled for RDS Instances

Rule Details

Table 3-145 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

3.5.29.16 Error Log Collection Is Enabled for RDS Instances

Rule Details

Table 3-146 Rule details

Parameter	Description
Rule Name	rds-instance-enable-errorLog
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

3.5.29.17 RDS Instances Support Slow Query Logs

Rule Details

Table 3-147 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

3.5.29.18 Single-AZ Cluster Check

Rule Details

Table 3-148 Rule details

Parameter	Description
Name	rds-instance-multi-az-support
Identifier	rds-instance-multi-az-support
Description	If an RDS cluster is deployed in a single availability zone, this cluster is noncompliant.
Tag	rds
Trigger Type	Configuration change
Filter Type	rds.instances
Configure Rule Parameters	None

3.5.29.19 RDS Instances Do Not Have Public IPs

Rule Details

Table 3-149 Rule details

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

3.5.29.20 RDS Instances Use KMS Encryption

Rule Details

Table 3-150 Rule details

Parameter	Description
Rule Name	rds-instances-enable-kms
Identifier	rds-instances-enable-kms
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

3.5.29.21 RDS Instances Are in the Specified VPC

Rule Details

Table 3-151 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**: indicates the ID of a specified VPC. The value must be a string.

3.5.29.22 Both Error Logs and Slow Query Logs Are Collected for RDS Instances

Rule Details

Table 3-152 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

3.5.29.23 Flavor Check

Rule Details

Table 3-153 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

3.5.30 Cloud Search Service (CSS)

3.5.30.1 CSS Clusters Use Authority Verification

Rule Details

Table 3-154 Rule details

Parameter	Description
Rule Name	css-cluster-authority-enable
Identifier	css-cluster-authority-enable
Description	If a CSS cluster can be accessed without authority verification, this cluster is noncompliant.
Tag	css
Trigger Type	Configuration change
Filter Type	css.clusters
Configure Rule Parameters	None

3.5.30.2 The Snapshot Function Is Enabled for CSS Clusters

Rule Details

Table 3-155 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

3.5.30.3 Disk Encryption Is Enabled for CSS Clusters

Rule Details

Table 3-156 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

3.5.30.4 HTTPS Access Is Enabled for CSS Clusters

Rule Details

Table 3-157 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

3.5.30.5 CSS Clusters Are in Specified VPCs

Rule Details

Table 3-158 Rule details

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

3.5.30.6 Single-AZ CSS Cluster Check

Rule Details

Table 3-159 Rule details

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

3.5.30.7 A CSS Cluster Has at Least Two Instances

Rule Details

Table 3-160 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
Configure Rule Parameters	None

3.5.30.8 CSS Clusters Are Not Publicly Accessible

Rule Details

Table 3-161 Rule details

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

3.5.30.9 Security Mode Is Enabled for CSS Clusters

Rule Details

Table 3-162 Rule details

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

3.5.30.10 CSS Clusters Cannot Be Accessed by All Public IPs

Rule Details

Table 3-163 Rule details

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

3.5.30.11 Kibana Cannot Be Accessed by All Public IPs

Rule Details

Table 3-164 Rule details

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

3.5.31 Elastic Volume Service (EVS)

3.5.31.1 EVS Disk Type Check

Rule Details

Table 3-165 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.

3.5.31.2 Disks Are Used Within the Specified Time

Rule Details

Table 3-166 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.

3.5.31.3 Idle EVS Disk Check

Rule Details

Table 3-167 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

3.5.31.4 EVS Disks Are Encrypted

Rule Details

Table 3-168 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

3.5.31.5 Disk Encryption Are Enabled

Rule Details

Table 3-169 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

3.5.32 Cloud Certificate Manager (CCM)

3.5.32.1 Expiration Check for Private CAs

Rule Details

Table 3-170 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 range, 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.

3.5.32.2 Expiration Check for Private Certificates

Rule Details

Table 3-171 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.

3.5.33 Distributed Message Service (for Kafka)

3.5.33.1 SSL Is Required for DMS Kafka Access over Private Networks

Rule Details

Table 3-172 Rule details

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

3.5.33.2 SSL Is Required for DMS Kafka over Public Networks

Rule Details

Table 3-173 Rule details

Parameter	Description
Rule Name	dms-kafka-not-enable-public-ssl
Identifier	dms-kafka-not-enable-public-ssl
Description	If SSL is not required for accessing a DMS Kafka instance over a public network, this instance is noncompliant.
Tag	dms
Trigger Type	Configuration change
Filter Type	dms.kafkas
Configure Rule Parameters	None

3.5.33.3 DMS Kafka Instances Are Not Publicly Accessible

Rule Details

Table 3-174 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.kafkas
Configure Rule Parameters	None

3.5.34 Distributed Message Service (for RabbitMQ)

3.5.34.1 SSL Is Enabled for DMS RabbitMq Instances

Rule Details

Table 3-175 Rule details

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

3.5.35 Distributed Message Service (for RocketMQ)

3.5.35.1 SSL Is Enabled for DMS Reliability Instances

Rule Details

Table 3-176 Rule details

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

3.5.36 Organizations

3.5.36.1 The Current Account Has Been Added to an Organization

Rule Details

Table 3-177 Rule details

Parameter	Description
Rule Name	account-part-of-organizations
Identifier	account-part-of-organizations
Description	If the current account has not been added to any organizations or to a specified organization, this account is noncompliant.
Tag	organizations
Trigger Type	Periodic
Filter Type	organizations.account

Parameter	Description
Rule Parameter	domainId: The account ID an organization administrator. An empty string indicates any account ID.

3.5.37 Cloud Firewall (CFW)

3.5.37.1 CFW Instances Are Attached with Protection Policies

Rule Details

Table 3-178 Rule details

Parameter	Description
Rule Name	cfw-policy-not-empty
Identifier	cfw-policy-not-empty
Description	If a CFW instance is not attached with a protection policy, this instance is noncompliant.
Tag	cfw
Trigger Type	Configuration change
Filter Type	cfw.cfw_instance
Rule Parameter	None

3.6 Event Monitoring

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

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

NOTE

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

The following table lists supported events of Config.

Table 3-179 Config events supported by Cloud Eye

Event Source	Event Name	Event Level	Description	Solution	Impact
SYS.RMS	Noncompliance notification	Major	The evaluation result of a rule is noncompliant.	Modify noncompliant resource configurations.	None
SYS.RMS	Compliance notification	Info	The evaluation result of a rule changes from noncompliant to complaint.	None	None
SYS.RMS	Storing Config snapshots failed	Major	Config fails to store resource snapshots to OBS buckets.	Check related OBS bucket permissions.	Resource changes cannot be recorded.
SYS.RMS	Resource snapshots stored	Info	Config successfully stores resource snapshots to OBS buckets.	None	None
SYS.RMS	Storing resource history failed	Major	Config fails to store resource history to OBS buckets.	Check related OBS bucket permissions.	Resource history cannot be recorded.
SYS.RMS	Resource history stored	Info	Config successfully stores resource history to OBS buckets.	None	None

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

4 Conformance Packages

4.1 Overview

Functions

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

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

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

Constraints and Limitation

- 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.

Concepts

Sample template

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

Pre-defined conformance package

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

Custom conformance package

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

Compliance data

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

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

Figure 4-1 Compliance score formula:

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

Stack:

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

Status

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

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

- Exception: Deleting a conformance package failed.
- Updated: A compliance package is updated.
- Updating: A compliance package is being updated.
- Updating: A compliance package update is in progress.

Authorization

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

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

4.2 Managing Conformance Packages

4.2.1 Creating a Conformance Package

Scenarios

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

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

Constraints and Limitation

- Up to 50 conformance packages (including organization conformance packages) and 500 rules can be created in an account.
- To create or update a conformance package, you need to enable the resource recorder. For details, see **Configuring the Resource Recorder**.

Procedure

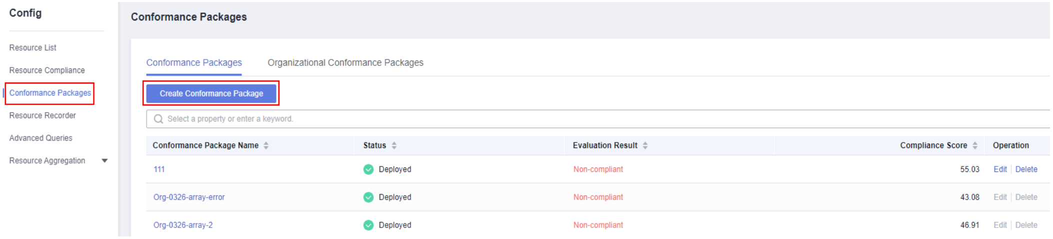
Step 1 Log in to the management console.

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
111	Deployed	Non-compliant	55.03	Edit | Delete
Org-0326-array-error	Deployed	Non-compliant	43.08	Edit | Delete
Org-0326-array-2	Deployed	Non-compliant	46.91	Edit | Delete

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

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

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

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

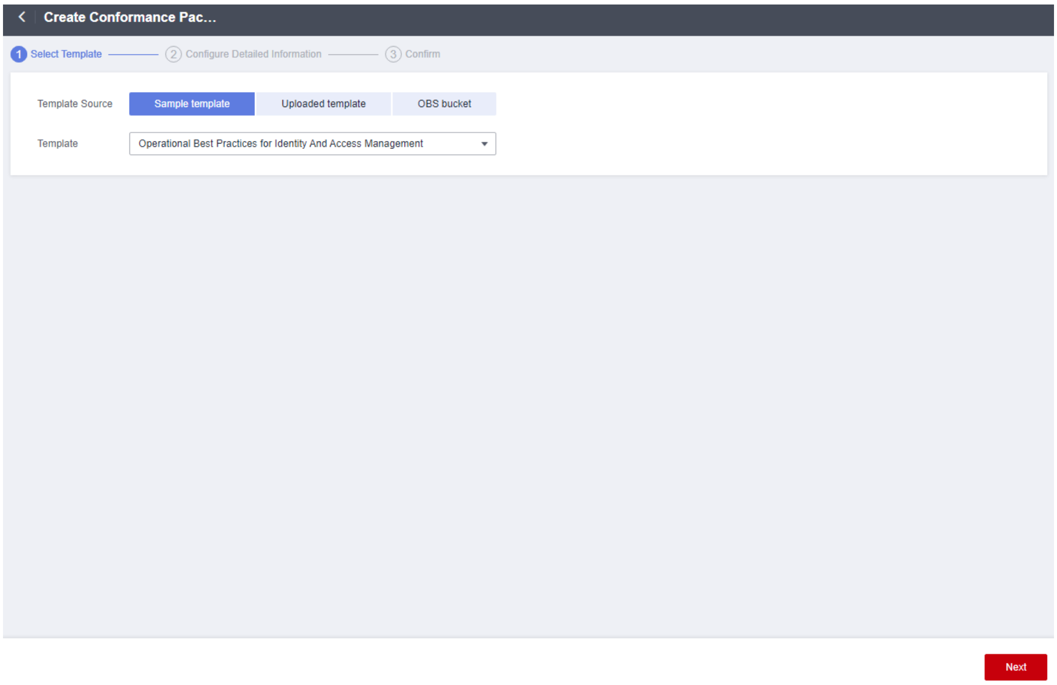
  Both the template file and content formats must be JSON. That is, the file name extension must be .tf.json. For details, see **custom conformance packages**.

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

  NOTE

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

Figure 4-3 Selecting a conformance package template



Create Conformance Pac...

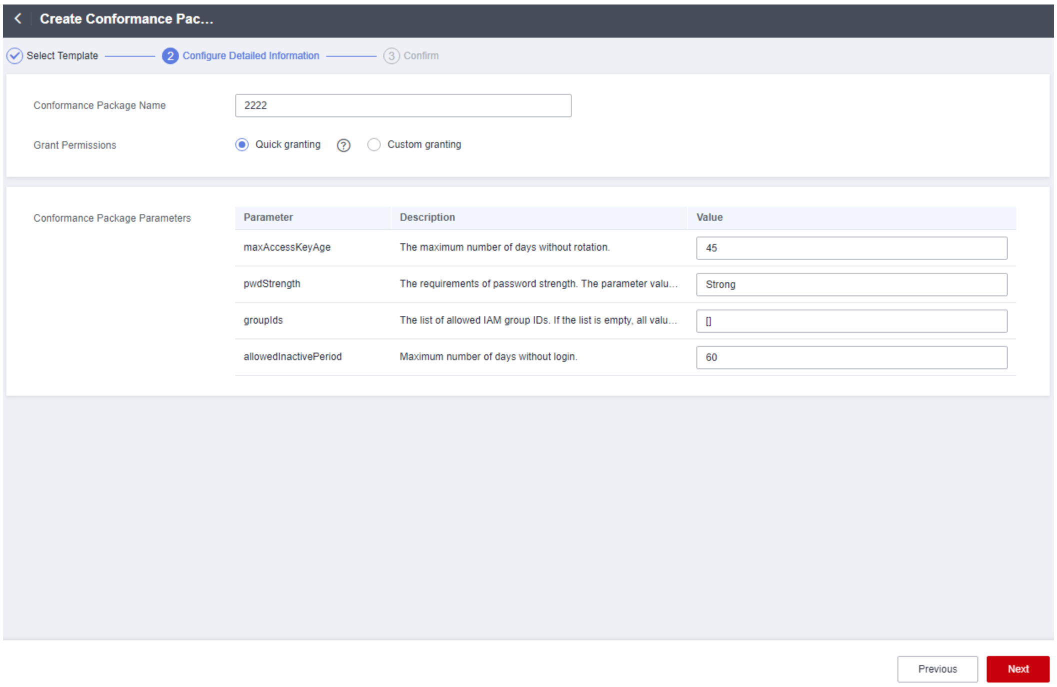
1 Select Template — 2 Configure Detailed Information — 3 Confirm

Template Source: Sample template | Uploaded template | OBS bucket

Template: Operational Best Practices for Identity And Access Management

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

Figure 4-4 Detailed information



Create Conformance Pac...

Select Template — 2 Configure Detailed Information — 3 Confirm

Conformance Package Name: 2222

Grant Permissions: ● Quick granting ○ Custom granting

Conformance Package Parameters

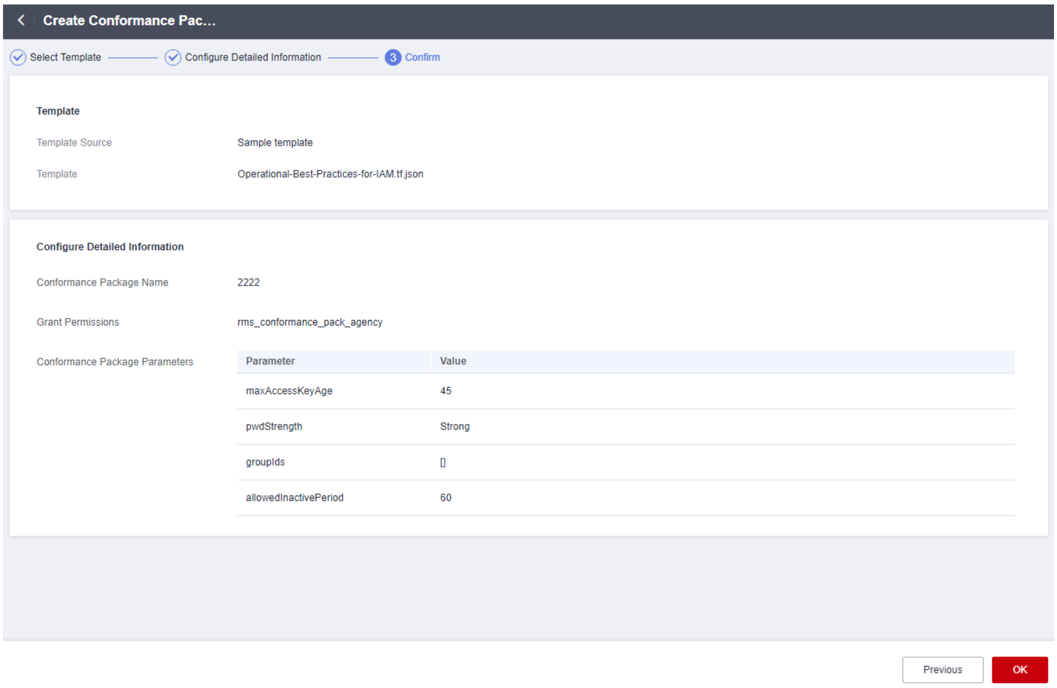
Parameter	Description	Value
maxAccessKeyAge	The maximum number of days without rotation.	45
pwdStrength	The requirements of password strength. The parameter valu...	Strong
groupIds	The list of allowed IAM group IDs. If the list is empty, all valu...	[]
allowedInactivePeriod	Maximum number of days without login.	60

Table 4-1 Package parameters

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

Step 7 On the confirm information page, confirm configuration and click **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: 2222

Grant Permissions: rms_conformance_pack_agency

Conformance Package Parameters

Parameter	Value
maxAccessKeyAge	45
pwdStrength	Strong
groupIds	[]
allowedInactivePeriod	60

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**.

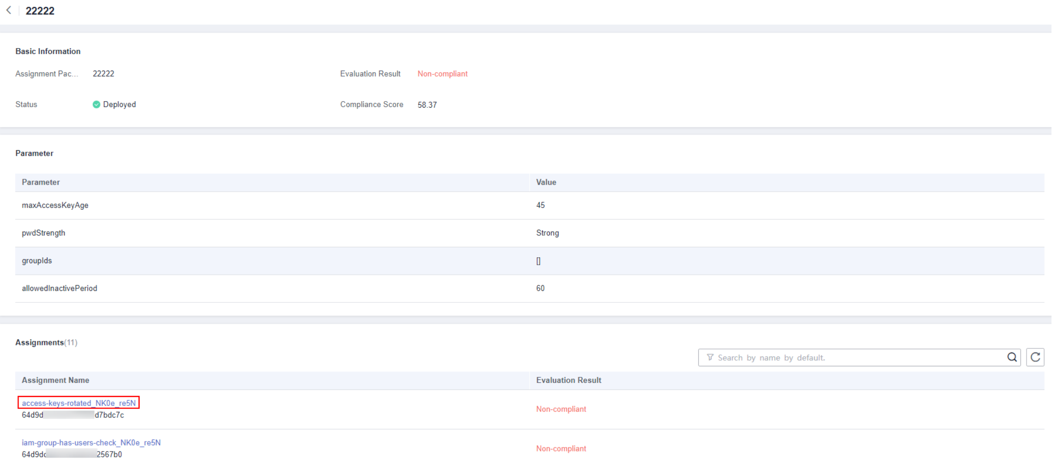
Step 4 View all the conformance packages created and their details, such as evaluation results, compliance scores, and status.

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, parameters, and evaluation result of each rule.

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

Figure 4-6 Conformance package details page



22222

Basic Information

Assignment Pac... 22222

Evaluation Result Non-compliant

Status ● Deployed

Compliance Score 58.37

Parameter

Parameter	Value
maxAccessKeyAge	45
pwdStrength	Strong
groupIds	[]
allowedInactivePeriod	60

Assignments(11)

Search by name by default.

Assignment Name	Evaluation Result
access-keys-rotated_NK0e_re5N 64d9d[redacted]d7bdc7c	Non-compliant
iam-group-has-users-check_NK0e_re5N 64d9dc[redacted]2567b0	Non-compliant

NOTE

A conformance package may be in a status of:

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

----End

4.2.3 Modifying a Conformance Package

Scenario

This section describes how to modify or update a conformance package.

Procedure

Step 1 Log in to the management console.

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

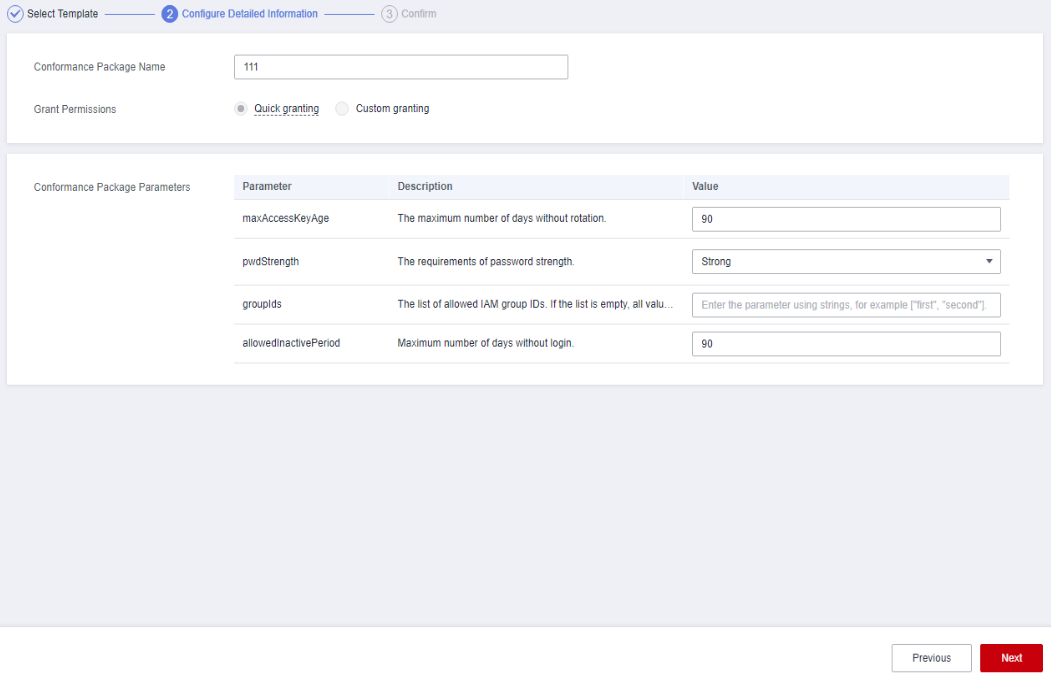
Step 3 On the left navigation pane, choose **Conformance Package**.

Step 4 Locate a target conformance package and click **Edit** in the **Operation** column to go the **Edit Conformance Package** page.

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**.

Figure 4-7 Modifying a conformance Package



Conformance Package Name: 111

Grant Permissions: ● Quick granting ○ Custom granting

Conformance Package Parameters

Parameter	Description	Value
maxAccessKeyAge	The maximum number of days without rotation.	90
pwdStrength	The requirements of password strength.	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 without login.	90

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**.

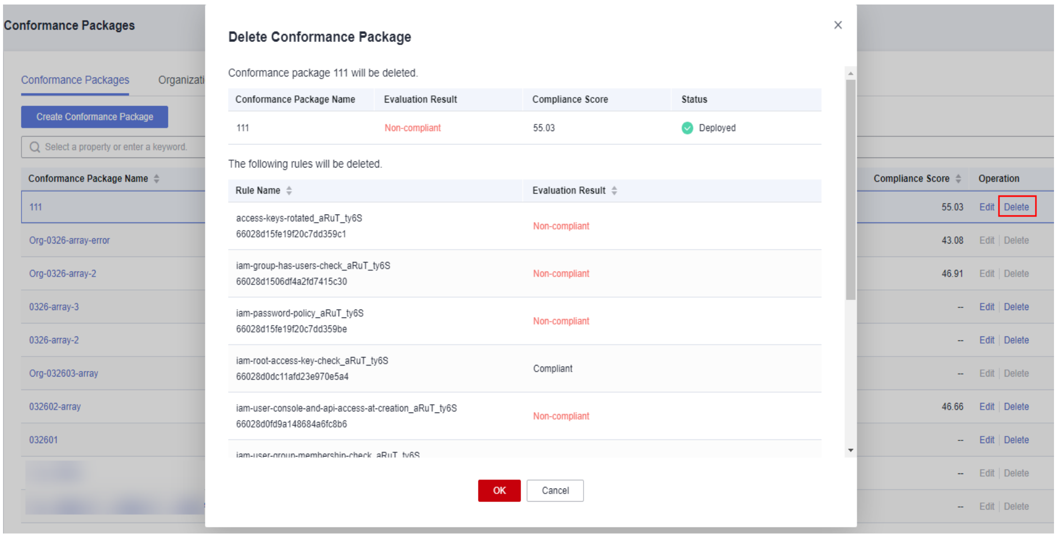
Step 3 On the left navigation pane, choose **Conformance Package**.

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



Delete Conformance Package

Conformance package 111 will be deleted.

Conformance Package Name	Evaluation Result	Compliance Score	Status
111	Non-compliant	55.03	✓ Deployed

The following rules will be deleted.

Rule Name	Evaluation Result
access-keys-rotated_aRuT_ty6S 66028d15fe19f20c7dd359c1	Non-compliant
iam-group-has-users-check_aRuT_ty6S 66028d1506df4a2fd7415c30	Non-compliant
iam-password-policy_aRuT_ty6S 66028d15fe19f20c7dd359be	Non-compliant
iam-root-access-key-check_aRuT_ty6S 66028d0dc11afd23e970e5a4	Compliant
iam-user-console-and-api-access-at-creation_aRuT_ty6S 66028d0fd9a148684a6fc8b6	Non-compliant
iam-user-group-membership-check_aRuT_ty6S	

----End

4.3 Organization Conformance Packages

4.3.1 Creating an Organization Conformance Package

Scenario

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

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

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

Restrictions and Limitations

- Up to 50 conformance packages (including organization conformance packages) and 500 rules can be created in an account.
- To create or update an organization conformance package, you need to enable the resource recorder. For details, see **Configuring the Resource Recorder**.
- The **Organization Conformance Package** tab is inaccessible for non-organization members on Config console.

Procedure

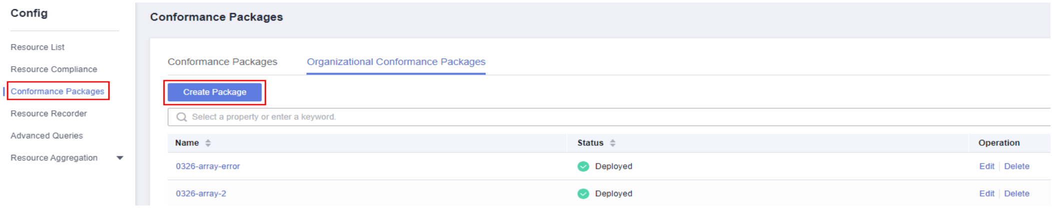
Step 1 Sign in to the Config console as an organization administrator or an agency administrator of Config.

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

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

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

Figure 4-9 Creating an organization conformance package



Name	Status	Operation
0326-array-error	Deployed	Edit | Delete
0326-array-2	Deployed	Edit | Delete

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

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

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

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

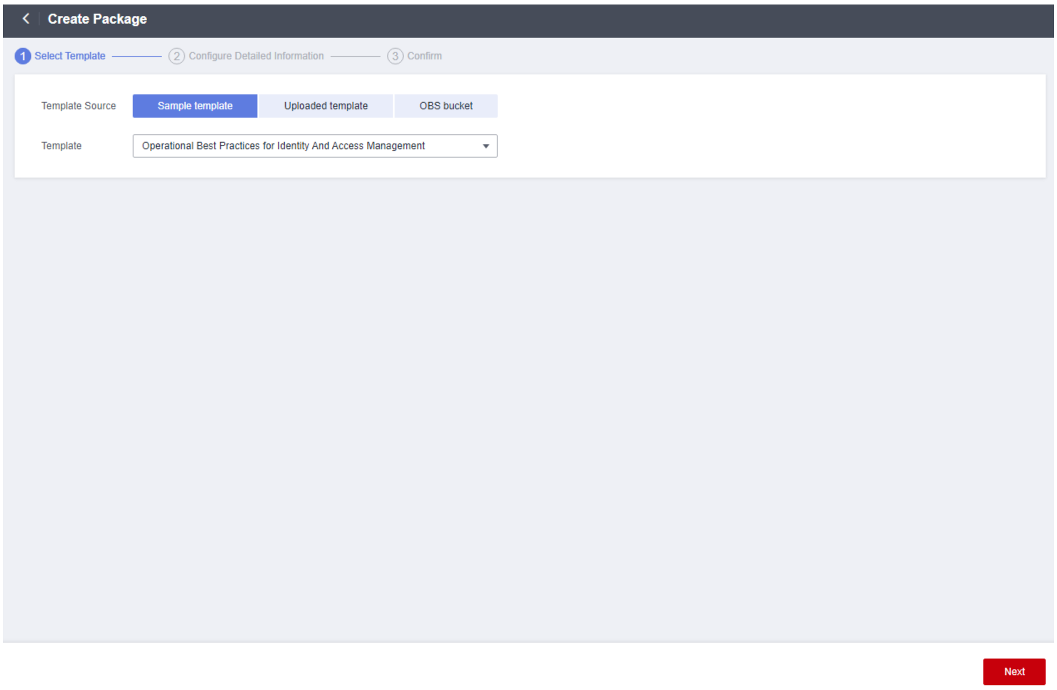
  Both the template file and content formats must be JSON. That is, the file name extension must be .tf.json. For details, see **custom conformance packages**.

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

  NOTE

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

Figure 4-10 Selecting a conformance package template

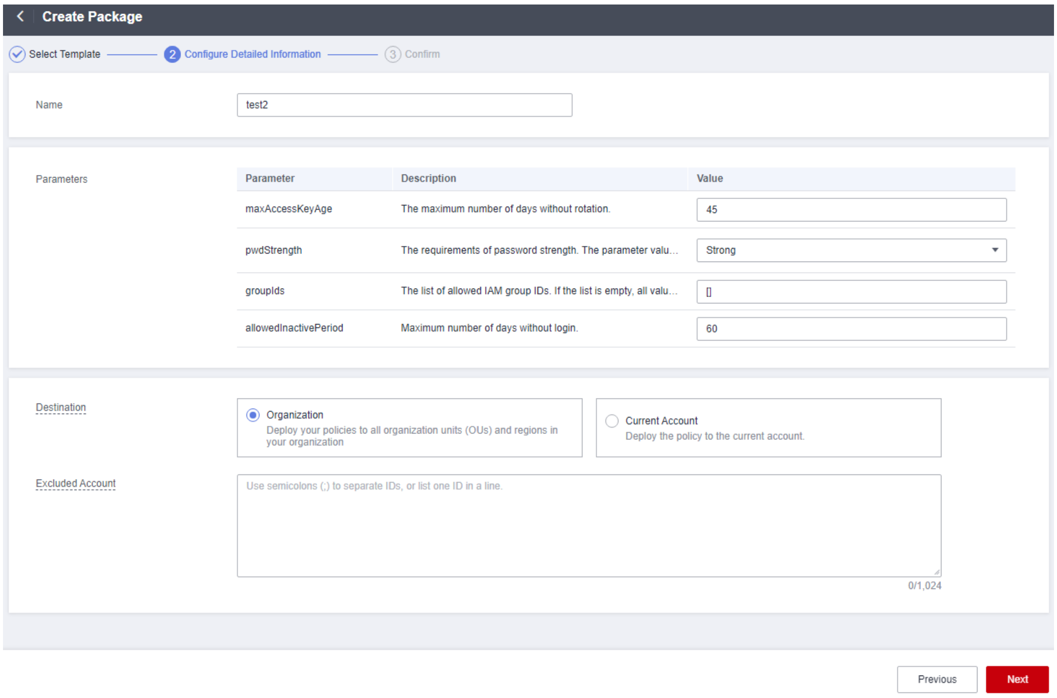


Template Source: Sample template | Uploaded template | OBS bucket

Template: Operational Best Practices for Identity And Access Management

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

Figure 4-11 Detailed information



Name: test2

Parameters

Parameter	Description	Value
maxAccessKeyAge	The maximum number of days without rotation.	45
pwdStrength	The requirements of password strength. The parameter valu...	Strong
groupIds	The list of allowed IAM group IDs. If the list is empty, all valu...	[]
allowedInactivePeriod	Maximum number of days without login.	60

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.

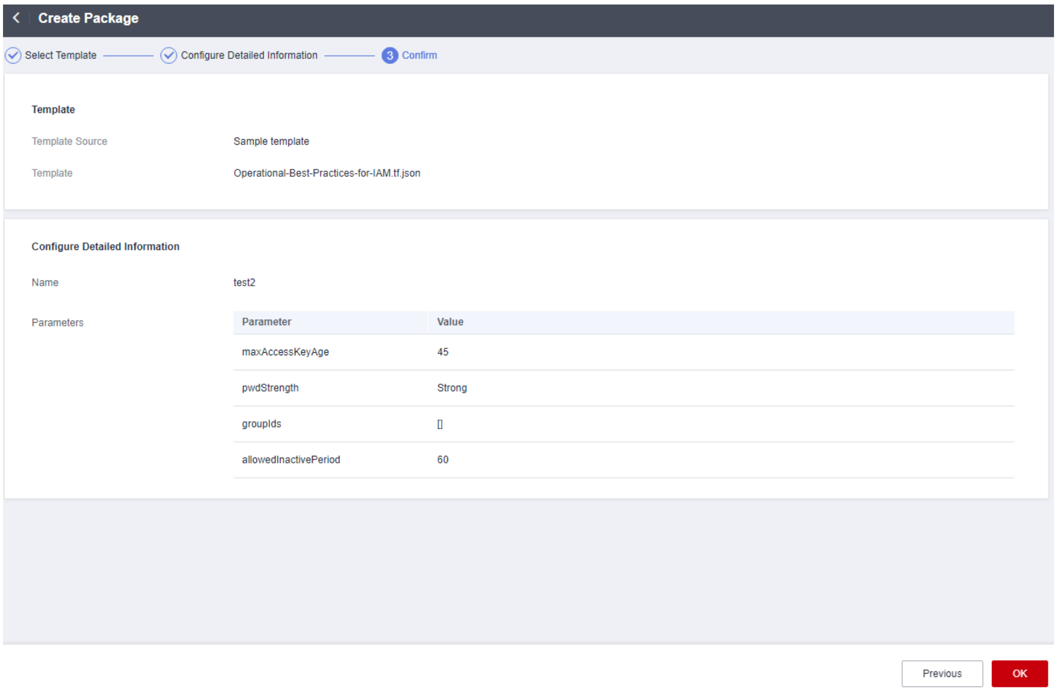
0/1,024

Table 4-2 Detailed information

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

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

Figure 4-12 Confirming configurations



Template

Template Source: Sample template

Template: Operational-Best-Practices-for-IAM.tf.json

Configure Detailed Information

Name: test2

Parameters

Parameter	Value
maxAccessKeyAge	45
pwdStrength	Strong
groupIds	[]
allowedInactivePeriod	60

NOTE

After an organization conformance package is created or updated, an evaluation will be automatically triggered.

----End

4.3.2 Viewing Organization Conformance Packages

Scenario

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

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

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

Viewing Organization Conformance Packages (for Administrators)

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

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

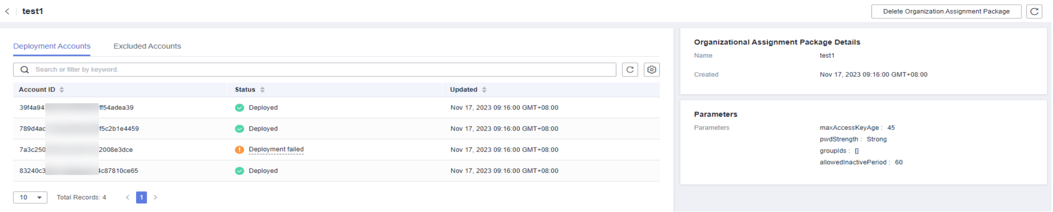
Step 3 On the left navigation pane, choose **Conformance Package**.

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

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

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

Figure 4-13 Organization conformance package details



test1
Delete Organization Assignment Package
Deployment Accounts
Excluded Accounts
Search or filter by keyword.

Account ID	Status	Updated
39f4a94[redacted]ff54adea39	Deployed	Nov 17, 2023 09:16:00 GMT+08:00
789d4ac[redacted]f5c2b1e4459	Deployed	Nov 17, 2023 09:16:00 GMT+08:00
7a3c250[redacted]2008e3dce	Deployment failed	Nov 17, 2023 09:16:00 GMT+08:00
83240c3[redacted]4c87810ce65	Deployed	Nov 17, 2023 09:16:00 GMT+08:00

10 Total Records: 4 1

Organizational Assignment Package Details

Name	test1
Created	Nov 17, 2023 09:16:00 GMT+08:00

Parameters

Parameters maxAccessKeyAge : 45
pwdStrength : Strong
groupIds : []
allowedInactivePeriod : 60

NOTE

The deployment status of an organization conformance package may be:

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

----End

Viewing Organization Conformance Packages (for Organization Members)

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

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

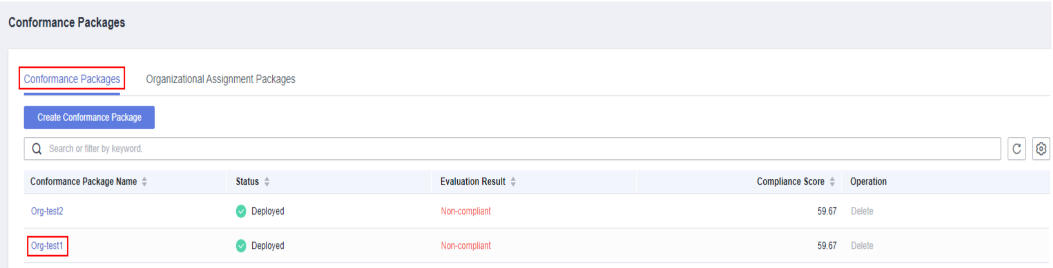
Step 3 On the left navigation pane, choose **Conformance Package**.

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, parameters, and evaluation result of each rule.

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

Figure 4-14 Viewing organization conformance packages (for organization members)



Conformance Packages

Conformance Packages
Organizational Assignment Packages
Create Conformance Package
Search or filter by keyword.

Conformance Package Name	Status	Evaluation Result	Compliance Score	Operation
Org-test2	Deployed	Non-compliant	59.67	Delete
Org-test1	Deployed	Non-compliant	59.67	Delete

NOTE

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

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

----End

4.3.3 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.

Procedure

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

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

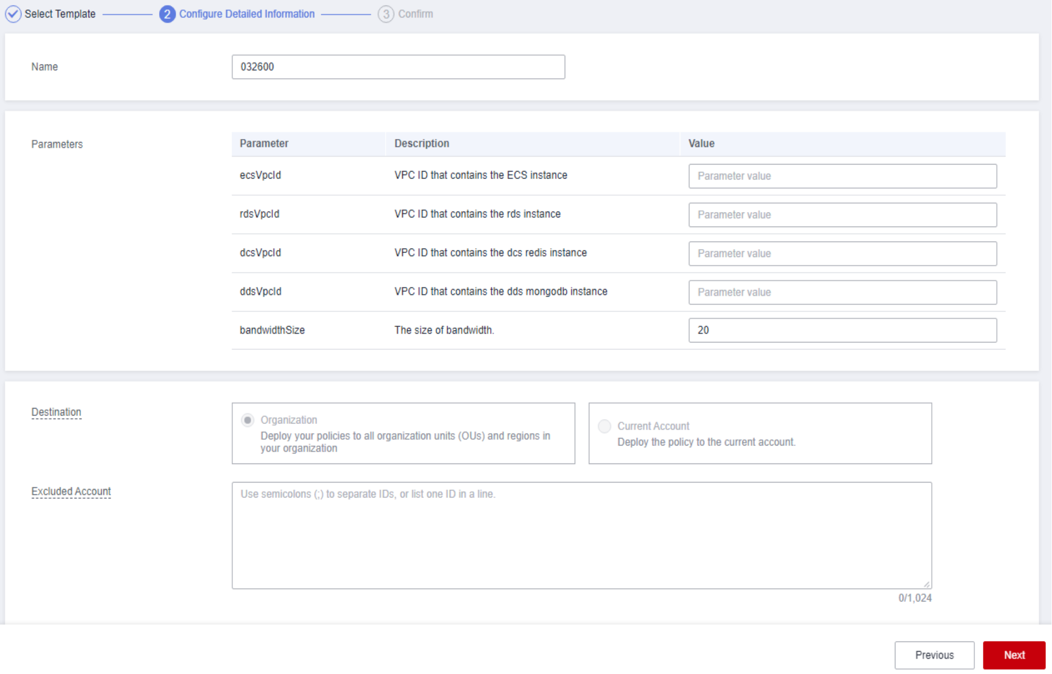
Step 3 On the left navigation pane, choose **Conformance Package**.

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

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**.

Figure 4-15 Modifying an organization conformance package



Name: 032600

Parameters

Parameter	Description	Value
ecsVpcId	VPC ID that contains the ECS instance	Parameter value
rdsVpcId	VPC ID that contains the rds instance	Parameter value
dcsVpcId	VPC ID that contains the dcs redis instance	Parameter value
ddsVpcId	VPC ID that contains the dds mongodb instance	Parameter value
bandwidthSize	The size of bandwidth.	20

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.

0/1,024

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 Organization Conformance Packages

Scenario

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

Procedure

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

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

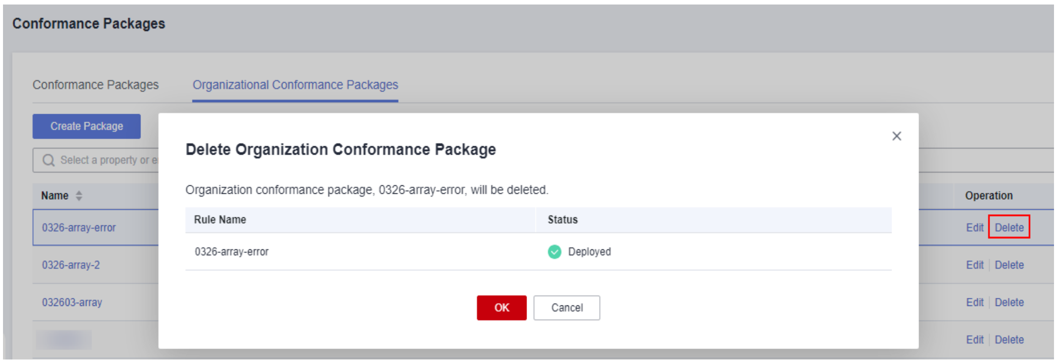
Step 3 On the left navigation pane, choose **Conformance Package**.

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

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

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

Figure 4-16 Deleting organization conformance packages



Delete Organization Conformance Package

Organization conformance package, 0326-array-error, will be deleted.

Rule Name	Status
0326-array-error	Deployed

----End

4.4 Custom Conformance Packages

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

Template Sections

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

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

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

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

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

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

```
{
  "resource": {
    "huaweicloud_rms_policy_assignment": {
      "AccessKeysRotated": {
        "name": "access-keys-rotated",
        "description": "An IAM users is noncompliant if the access keys have not been rotated for more than
maxAccessKeyAge number of days.",
        "policy_definition_id": "2a2938894ae786dc306a647a",
        "period": "TwentyFour_Hours",
        "parameters": {
          "maxAccessKeyAge": "${jsonencode(var.maxAccessKeyAge)}"
        }
      },
      "IamGroupHasUsersCheck": {
        "name": "iam-group-has-users-check",
        "description": "An IAM groups is noncompliant if it does not add any IAM user.",
        "policy_definition_id": "f7dd9c02266297f6e8c8445e",
        "policy_filter": {
          "resource_provider": "iam",
          "resource_type": "groups"
        },
        "parameters": {}
      },
      "IamPasswordPolicy": {
        "name": "iam-password-policy",
        "description": "An IAM users is noncompliant if password policy for IAM users matches the specified
password strength.",
        "policy_definition_id": "2d8d3502539a623ba1907644",
        "policy_filter": {
          "resource_provider": "iam",
          "resource_type": "users"
        },
        "parameters": {
          "pwdStrength": "${jsonencode(var.pwdStrength)}"
        }
      },
      "IamRootAccessKeyCheck": {
        "name": "iam-root-access-key-check",
        "description": "An account is noncompliant if the the root iam user have active access key.",
        "policy_definition_id": "66cac2ddc17b6a25ad077253",
        "period": "TwentyFour_Hours",
        "parameters": {}
      },
      "IamUserConsoleAndApiAccessAtCreation": {
        "name": "iam-user-console-and-api-access-at-creation",
        "description": "An IAM user with console access is noncompliant if access keys are setup during the
initial user setup.",
        "policy_definition_id": "a5f29eb45cddce8e6baa033d",
        "policy_filter": {
          "resource_provider": "iam",
          "resource_type": "users"
        },
        "parameters": {}
      },
      "IamUserGroupMembershipCheck": {
        "name": "iam-user-group-membership-check",
        "description": "An IAM user is noncompliant if it does not belong to any IAM user group.",
        "policy_definition_id": "846f5708463c1490c4eebd60",
        "policy_filter": {
          "resource_provider": "iam",
          "resource_type": "users"
        },
        "parameters": {
          "groupIds": "${jsonencode(var.groupIds)}"
        }
      },
      "IamUserLastLoginCheck": {
        "name": "iam-user-last-login-check",
        "description": "An IAM user is noncompliant if it has never signed in within the allowed number of
days.",
        "policy_definition_id": "6e4bf7ee7053b683f28d7f57",
        "period": "TwentyFour_Hours",
        "parameters": {
          "allowedInactivePeriod": "${jsonencode(var.allowedInactivePeriod)}"
        }
      },
      "IamUserMfaEnabled": {
        "name": "iam-user-mfa-enabled",
        "description": "An IAM user is noncompliant if it does not have multi-factor authentication (MFA) enabled.",
        "policy_definition_id": "b92372b5eb51330306cec9c2",
        "policy_filter": {
          "resource_provider": "iam",
          "resource_type": "users"
        },
        "parameters": {}
      },
      "IamUserSingleAccessKey": {
        "name": "iam-user-single-access-key",
        "description": "An IAM user with console access is noncompliant if iam user have multiple active access keys.",
        "policy_definition_id": "6deae3856c41b240b3c0bf8d",
        "policy_filter": {
          "resource_provider": "iam",
          "resource_type": "users"
        },
        "parameters": {}
      },
      "MfaEnabledForIamConsoleAccess": {
        "name": "mfa-enabled-for-iam-console-access",
        "description": "An IAM user is noncompliant if it uses a console password and does not have multi-factor authentication (MFA) enabled.",
        "policy_definition_id": "63f8301e47b122062a68b868",
        "policy_filter": {
          "resource_provider": "iam",
          "resource_type": "users"
        },
        "parameters": {}
      },
      "RootAccountMfaEnabled": {
        "name": "root-account-mfa-enabled",
        "description": "An account is noncompliant if the the root iam user does not have multi-factor authentication (MFA) enabled.",
        "policy_definition_id": "61d787a75cf7f5965da5d647",
        "period": "TwentyFour_Hours",
        "parameters": {}
      }
    }
  },
  "variable": {
    "maxAccessKeyAge": {
      "description": "The maximum number of days without rotation. ",
      "type": "string",
      "default": "90"
    },
    "pwdStrength": {
      "description": "The requirements of password strength. The parameter value can only be 'Strong', 'Medium', or 'Low'.",
      "type": "string",
      "default": "Strong"
    },
    "groupIds": {
      "description": "The list of allowed IAM group IDs. If the list is empty, all values are allowed.",
      "type": "list(string)",
      "default": []
    },
    "allowedInactivePeriod": {
      "description": "Maximum number of days without login.",
      "type": "number",
      "default": 90
    }
  },
  "terraform": {
    "required_providers": {
      "huaweicloud": {
        "source": "huawei.com/provider/huaweicloud",
        "version": "1.46.0"
      }
    }
  }
}
```

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

```
{
    "resource": {
        "huaweicloud_rms_policy_assignment": {
            "CustomPolicyAssignment": {
                "name": "customPolicy${var.name_suffix}",
"description": Custom rules. All resources are non-compliant.
                "policy_filter": {
                    "resource_provider": "obs",
                    "resource_type": "buckets"
                },
                "parameters": {},
                "custom_policy": {
                    "function_urn": "${var.function_urn}",
                    "auth_type": "agency",
                    "auth_value": {
                        "agency_name": "\"config_custom_policy_agency\""
                    }
                }
            }
        }
    },
    "variable": {
        "name_suffix": {
            "description": "",
            "type": "string"
        },
        "function_urn": {
            "description": "",
            "type": "string"
        }
    },
    "terraform": {
        "required_providers": {
            "huaweicloud": {
                "source": "huawei.com/provider/huaweicloud",
                "version": "1.46.0"
            }
        }
    }
}
```

4.5 Conformance Package Templates

4.5.1 Overview

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

The following sample templates are provided on Config console:

- **Compliance Package for Classified Protection of Cybersecurity Level 3 (2.0)**
- **Conformance Package for 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 for Enabling Public Access**
- **Conformance Package for Logging and Monitoring**
- **Conformance Package for Idle Asset Management**
- **Conformance Package for Architecture Reliability**
- **Conformance Package for Hong Kong Monetary Authority of China Requirements**
- **Conformance Package for ENISA Requirements**
- **Compliance Package for SWIFT CSP**
- **Compliance Package for Germany Cloud Computing Compliance Criteria Catalogue**
- **Compliance Package for PCI DSS**
- **Conformance Package for Healthcare Industry**

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

This section describes the background, applicable scenarios, and the compliance 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 4-3

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.	dds-instance-in-vpc	Deploy all DDS instances 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.	ecs-instance-in-vpc	Deploy all ECSs 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.	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.	dds-instance-in-vpc	Deploy all DDS instances within VPCs.

Guideline No.	Guideline Description	Config Rule	Solution
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.
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.

Guideline No.	Guideline Description	Config Rule	Solution
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.
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.

Guideline No.	Guideline Description	Config Rule	Solution
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.
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.

Guideline No.	Guideline Description	Config Rule	Solution
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 compliance rules and solutions included in the conformance package dedicated to the financial industry.

Table 4-4 Conformance package description

Rule Identifier	Cloud Service	Rule Content
access-keys-rotated	iam	If there is an access key that has not been rotated for longer than the specified time, the result 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.

Rule Identifier	Cloud Service	Rule Content
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 there is no tracker created for the specified OBS bucket, the result 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 in the current account, the result is noncompliant.
ecs-instance-in-vpc	ecs, vpc	If there is an ECS that is not within the specified VPC, the result is noncompliant.
ecs-instance-no-public-ip	ecs	If there is an ECS that is configured with a public IP, the result 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.

Rule Identifier	Cloud Service	Rule Content
function-graph-concurrency-check	fgs	If the number of concurrent requests of a 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 there is a user whose password does not meet the password complexity requirements, the result is noncompliant.
iam-root-access-key-check	iam	If the root access key is available, the result is noncompliant.
iam-user-group-membership-check	iam	If an IAM user is not added to any 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.
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 there is an MRS cluster that is not within the specified VPC, the result is noncompliant.

Rule Identifier	Cloud Service	Rule Content
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 is attached with a public IP, 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 cluster is deployed in a single availability zone, this cluster is noncompliant.
rds-instance-no-public-ip	rds	If an RDS instance is attached with an EIP, 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.
stopped-ecs-date-diff	ecs	If there is an ECS that has been stopped for longer than the time allowed, and no operations have been performed on it, the result 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 there is a network ACL that has not been associated with any subnets, the result is noncompliant.

Rule Identifier	Cloud Service	Rule Content
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 (**Source**: 0.0.0.0/0) and has no port specified, this security group is noncompliant.
vpn-connections-active	vpnaas	If the state of a VPN connection is not connected, the result is noncompliant.
waf-instance-policy-not-empty	waf	If no conditions are configured for a WAF protection rule, the result is noncompliant.

4.5.4 Conformance Package for Network Security

The following table lists the compliance rules and solutions included in the conformance package dedicated to network security.

Table 4-5 Conformance package description

Rule	Cloud Service	Description
access-keys-rotated	iam	If there is an AK/SK pair that has been used for a time longer than the specified time range, the result is noncompliant.
alarm-kms-disable-or-delete-key	ces, kms	If there are no alarm rules configured for disabling KMS or deleting keys, the result is noncompliant.
alarm-obs-bucket-policy-change	ces, obs	If there are no alarm rules configured for OBS bucket policy changes, the result is noncompliant.

Rule	Cloud Service	Description
alarm-vpc-change	ces, vpc	If no alarm rules are created for VPC changes, 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 the specified VPC, 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 there is no tracker created for the specified OBS bucket, the result 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 tracker in the current account, the result is noncompliant.
ecs-instance-in-vpc	ecs, vpc	If there is an ECS that is not within the specified VPC, the result is noncompliant.
ecs-instance-no-public-ip	ecs	If there is an ECS that is configured with a public IP, the result is noncompliant.
eip-unbound-check	vpc	If an EIP has not been attached to any resource, this EIP is noncompliant.

Rule	Cloud Service	Description
elb-tls-https-listeners-only	elb	If any listener of a load balancer is not configured with 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 there is a user whose password does not meet the password complexity requirements, the result is noncompliant.
iam-root-access-key-check	iam	If the root access key is available, the result is noncompliant.
iam-user-console-and-api-access-at-creation	iam	If there is a user who has a console password and whose AK/SK pair is created when this user is created, the result is noncompliant.
iam-user-group-membership-check	iam	If an IAM user is not added to any 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.
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 is attached with a public IP, 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 cluster is deployed in a single availability zone, this cluster is noncompliant.
rds-instance-no-public-ip	rds	If an RDS instance is attached with an EIP, 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.
stopped-ecs-date-diff	ecs	If there is an ECS that has been stopped for longer than the time allowed, and no operations have been performed on it, the result 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.

Rule	Cloud Service	Description
vpc-acl-unused-check	vpc	If there is a network ACL that has not been associated with any subnets, the result 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.

4.5.5 Conformance Package for Identity and Access Management

The following table lists the compliance rules and solutions included in the conformance package dedicated to Identity and Access Management.

Table 4-6 Conformance package description

Rule	Cloud Service	Description
access-keys-rotated	iam	If there is an AK/SK pair that has been used for a time longer than the specified time range, the result 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 there is a user whose password does not meet the password complexity requirements, the result is noncompliant.
iam-root-access-key-check	iam	If the root access key is available, the result is noncompliant.
iam-user-console-and-api-access-at-creation	iam	If there is a user who has a console password and whose AK/SK pair is created when this user is created, the result is noncompliant.

Rule	Cloud Service	Description
iam-user-group-membership-check	iam	If an IAM user is not added to any 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.
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.

4.5.6 Conformance Package for Cloud Eye

The following table describes the compliance rules and solutions in the sample template.

Table 4-7 Conformance package description

Rule	Cloud Service	Description
alarm-action-enabled-check	ces	If an alarm rule is not enabled, this rule is noncompliant.

Rule	Cloud Service	Description
alarm-kms-disable-or-delete-key	ces, kms	If there are no alarm rules configured for disabling KMS or deleting keys, the result is noncompliant.
alarm-obs-bucket-policy-change	ces, obs	If there are no alarm rules configured for OBS bucket policy changes, the result is noncompliant.
alarm-vpc-change	ces, vpc	If no alarm rules are created for VPC changes, the result is noncompliant.

4.5.7 Conformance Package for Compute Services

The following table describes the compliance rules and solutions in the sample template.

Table 4-8 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, the result is noncompliant.
as-multiple-az	as	If an AS group is deployed in a single AZ, this AS group is noncompliant.
ecs-instance-key-pair-login	ecs	If no key pairs are configured for an ECS, the ECS is noncompliant.

Rule	Cloud Service	Description
ecs-instance-no-public-ip	ecs	If there is an ECS that is configured with a public IP, the result is noncompliant.
ecs-multiple-public-ip-check	ecs	If there is an ECS that is configured with a public IP, the result 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 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 there is an ECS that has been stopped for longer than the time allowed, and no operations have been performed on it, the result 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.

4.5.8 Conformance Package for ECS

The following table describes the compliance rules and solutions in the sample template.

Table 4-9 Conformance package description

Rule	Cloud Service	Description
ecs-instance-key-pair-login	ecs	If no key pairs are configured for an ECS, this ECS is noncompliant.
ecs-instance-no-public-ip	ecs	If there is an ECS that is configured with a public IP, the result is noncompliant.
ecs-multiple-public-ip-check	ecs	If there is an ECS that is configured with a public IP, the result is noncompliant.
stopped-ecs-date-diff	ecs	If there is an ECS that has been stopped for longer than the time allowed, and no operations have been performed on it, the result is noncompliant.
volumes-encrypted-check	ecs, evs	If a mounted EVS disk is not encrypted, this disk is noncompliant.

4.5.9 Conformance Package for ELB

The following table describes the compliance rules and solutions in the sample template.

Table 4-10 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.

Rule	Cloud Service	Description
elb-tls-https-listeners-only	elb	If any listener of a load balancer is not configured with HTTPS, this load balancer is noncompliant.

4.5.10 Conformance Package for Management and Regulatory Services

The following table describes the compliance rules and solutions in the sample template.

Table 4-11 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 KMS or deleting keys, the result is noncompliant.
alarm-obs-bucket-policy-change	ces, obs	If there are no alarm rules configured for OBS bucket policy changes, the result is noncompliant.
alarm-vpc-change	ces, vpc	If no alarm rules are created for VPC changes, the result 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.

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 is no tracker in the current account, the result is noncompliant.
tracker-config-enabled-check	config	If the resource recorder has not been enabled, the result is noncompliant.

4.5.11 Conformance Package for RDS

The following table describes the compliance rules and solutions in the sample template.

Table 4-12 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 cluster is deployed in a single availability zone, this cluster is noncompliant.
rds-instance-no-public-ip	rds	If an RDS instance is attached with an EIP, this 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.

4.5.12 Conformance Package for AS

The following table describes the compliance rules and solutions in the sample template.

Table 4-13 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, the result is noncompliant.
as-multiple-az	as	If an AS group is deployed in a single AZ, this AS group is noncompliant.

4.5.13 Conformance Package for CTS

The following table describes the compliance rules and solutions in the sample template.

Table 4-14 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.

Rule	Cloud Service	Description
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 tracker in the current account, the result is noncompliant.

4.5.14 Conformance Package for AI and Machine Learning

The following table describes the compliance rules and solutions in the sample template.

Table 4-15 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 public IP is attached to a CCE cluster, this cluster is noncompliant.
cts-obs-bucket-track	cts	If there is no tracker created for the specified OBS bucket, the result 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 is attached with a public IP, this cluster 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.

4.5.15 Conformance Package for Autopilot

The following table describes the compliance rules and solutions in the sample template.

Table 4-16 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 the **Security Mode** is not enabled for a CSS cluster, 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 there are no trackers created for the specified OBS bucket, the result 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 tracker in the current account, the result is noncompliant.

Rule	Cloud Service	Description
dcs-redis-no-public-ip	dcs	If a DCS Redis instance is configured with a public IP, 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 there is an ECS that is configured with a public IP, the result 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 is not configured with HTTPS, this load balancer is noncompliant.
iam-password-policy	iam	If there is a user whose password does not meet the password complexity requirements, the result 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.
rds-instance-no-public-ip	rds	If an RDS instance is attached with an EIP, this instance is noncompliant.

Rule	Cloud Service	Description
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 (**Source**: 0.0.0.0/0) and has no port specified, this security group is noncompliant.

4.5.16 Conformance Package for for Enabling Public Access

The following table describes the compliance rules and solutions in the sample template.

Table 4-17 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 not set to public network, this task is noncompliant.
drs-migration-job-not-public	drs	If the network type of a migration task is not set to public network, this 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.

Rule Identifier	Cloud Service	Description
ecs-instance-in-vpc	ecs, vpc	If there is an ECS that is not within the specified VPC, the result is noncompliant.
ecs-instance-no-public-ip	ecs	If there is an ECS that is configured with a public IP, the result 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 is attached with a public IP, this cluster is noncompliant.
rds-instance-no-public-ip	rds	If an RDS instance is attached with an EIP, this instance is noncompliant.

4.5.17 Conformance Package for Logging and Monitoring

The following table describes the compliance rules and solutions in the sample template.

Table 4-18 Conformance package description

Rule Identifier	Cloud Service	Description
alarm-action-enabled-check	ces	If an alarm rule is not enabled, this rule is noncompliant.
apig-instances-execution-logging-enabled	apig	If logging is not enabled for a dedicated API gateway, this gateway is considered non-compliant.

Rule Identifier	Cloud Service	Description
as-group-elb-healthcheck-required	as	If an AS group is not using Elastic Load Balancing health check, the result 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 there are no trackers created for the specified OBS bucket, the result 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 tracker in the current account, the result is noncompliant.
dws-enable-log-dump	dws	If the **Audit Log Dump** is not enabled for a DWS cluster, this cluster is noncompliant.
function-graph-concurrency-check	fgs	If the number of concurrent requests of a function is not within the specified range, this function is noncompliant.
multi-region-cts-tracker-exists	cts	If there are no trackers in any of the specified regions, the result is noncompliant.
rds-instance-logging-enabled	rds	If neither error logs nor slow query logs are collected for an RDS instance, this instance 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.

4.5.18 Conformance Package for Idle Asset Management

The following table describes the compliance rules and solutions in the sample template.

Table 4-19 Conformance package description

Rule Identifier	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.
eip-unbound-check	vpc	If an EIP has not been attached to any resource, this EIP is noncompliant.
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.
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.
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.

Rule Identifier	Cloud Service	Description
stopped-ecs-date-diff	ecs	If there is an ECS that has been stopped for longer than the time allowed, and no operations have been performed on it, the result is noncompliant.
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 there is a network ACL that has not been associated with any subnets, the result is noncompliant.

4.5.19 Conformance Package for Architecture Reliability

The following table describes the compliance rules and solutions in the sample template.

Table 4-20 Conformance package description

Rule Identifier	Cloud Service	Description
apig-instances-execution-logging-enabled	apig	If logging is not enabled for a dedicated API 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, the result 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 there are no trackers created for the specified OBS bucket, the result is noncompliant.

Rule Identifier	Cloud Service	Description
cts-tracker-exists	cts	If there is no tracker in the current account, the result is noncompliant.
dws-enable-kms	dws	If KMS encryption is not enabled for a DWS cluster, this cluster is noncompliant.
ecs-instance-in-vpc	ecs, vpc	If there is an ECS that is not within the specified VPC, the result is noncompliant.
function-graph-concurrency-check	fgs	If the number of concurrent requests of a function is not within the specified range, this function is noncompliant.
gaussdb-nosql-enable-disk-encryption	gaussdb nosql	If **Disk Encryption** is disabled for a GaussDB NoSQL instance, 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, the result 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 cluster is deployed in a single availability zone, this cluster is noncompliant.
rds-instances-enable-kms	rds	If KMS encryption is not enabled for an RDS instance, this instance is noncompliant.

Rule Identifier	Cloud Service	Description
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.
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 VPC connections.

4.5.20 Conformance Package for Hong Kong Monetary Authority of China Requirements

This section describes the background, applicable scenarios, and the compliance 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 No. in the following table are in consistent with the chapter No. in **HKMA.2022.08.31**.

Table 4-21 The conformance package for HAMA

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

Table 4-22 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	User API gateway logs to visualize users accessing APIs and obtain their access methods and activities.
2.8.1	AIs should ensure that appropriate up-to-date records are maintained in their premises and kept available for inspection by the HKMA.	cts-lts-enable	Use CTS to centrally collect and manage log events

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 4-23 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 4-24 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.

4.5.21 Conformance Package for ENISA Requirements

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

Background

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

Applicable Scenarios

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

Exemption Clauses

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

Compliance Rules

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

Table 4-25 Rules in the conformance package

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Guideline No.	Guideline Description	Rule	Solution
6_SECURE DEVICES: ENCRYPTION	Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferred over public networks, such as hotel or airport WiFi networks, ensure that data is encrypted, either by employing a Virtual Private Network (VPN) or accessing websites over secure connections using SSL/TLS protocol. Ensure their own websites are employing suitable encryption technology to protect client data as it travels over the Internet.	css-cluster-https-required	After HTTPS is enabled for a CSS cluster, communication is encrypted when you access this cluster. If HTTPS is disabled, HTTP protocol is used for cluster communication. In this case, data security cannot be ensured and public address is not allowed.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4.5.22 Compliance Package for SWIFT CSP

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

Background

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

Exemption Clauses

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

Compliance Rules

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

Table 4-26 Rules in the conformance package

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

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

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

4.5.23 Compliance Package for Germany Cloud Computing Compliance Criteria Catalogue

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

Background

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

Applicable Scenarios

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

Exemption Clauses

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

Rules

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

Table 4-27 Rules in this conformance package

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

Guideline No.	Rule	Solution
COS-03	vpc-sg-ports-check	Use security groups to control prot connections for VPCs.
COS-05	iam-user-mfa-enabled	Enable MFA for all IAM users to prevent account theft.
COS-05	mfa-enabled-for-iam-console-access	Enable MFA for all IAM users who can access Huawei Cloud management console. MFA enhances account security to prevent account theft and protect sensitive data.
COS-05	root-account-mfa-enabled	Enable MFA for root users. MFA enhances account security.
COS-05	ecs-instance-no-public-ip	Block public access to ECSs to protect sensitive data.
COS-05	mrs-cluster-no-public-ip	Block access to MRS clusters through public networks to protect sensitive data.
COS-05	rds-instance-no-public-ip	Block access to cloud databases from public networks to protect sensitive data.
COS-05	vpc-sg-restricted-common-ports	Configure security groups to control connections to common ports in a VPC.
COS-05	vpc-sg-restricted-ssh	Configure security groups to only allow connections to SSH port 22 of ECSs with specified IPs, so remote access to ECS can be secure.
COS-05	vpc-default-sg-closed	Use security groups to control access within a VPC. You can directly use the default security group for resource access control.
COS-05	vpc-sg-ports-check	Use security groups to control connections to specified ports.
CRY-02	apig-instances-ssl-enabled	Enable SSL for APIG REST APIs to authenticate API requests.
CRY-02	elb-predefined-security-policy-https-check	Ensure that your dedicated load balancers are configured with specified security policy to enhance service security.
CRY-02	css-cluster-https-required	After HTTPS is enabled for a CSS cluster, communication is encrypted when you access this cluster. If HTTPS is disabled, HTTP protocol is used for cluster communication. In this case, data security cannot be ensured and public address is not allowed.

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

Guideline No.	Rule	Solution
IDM-01	mrs-cluster-kerberos-enabled	Enable Kerberos for MRS clusters.
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 GaussDB NoSQL.
OPS-14	cts-support-validate-check	Enable file verification for CTS trackers to prevent log files from being modified or deleted after being stored.
OPS-14	cts-kms-encrypted-check	Enable trace file encryption for CTS trackers.
OPS-15	apig-instances-execution-logging-enabled	Enable CTS for your dedicated API gateways. APIG supports custom log analysis templates, which you can use to collect and manage logs and trace and analyze API request exceptions.
OPS-15	cts-lts-enable	Use LTS to centrally collect CTS data.

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 named system is created automatically. You can create multiple trackers for different regions to help make services better satisfy customer needs as well as legal or regulatory requirements.
OPS-15	cts-obs-bucket-track	Create at least one CTS tracker for each OBS bucket.
OPS-15	multi-region-cts-tracker-exists	Create CTS trackers for different regions where your services are deployed. When you enable CTS for the first time, a management tracker named system is created automatically. You can create multiple trackers for different regions to help make services better satisfy customer needs as well as legal or regulatory requirements.
PSS-05	iam-user-mfa-enabled	Enable MFA for all IAM users to prevent account theft.
PSS-05	mfa-enabled-for-iam-console-access	Enable MFA for all IAM users who can access Huawei Cloud management console. MFA enhances account security to prevent account theft and protect sensitive data.
PSS-05	root-account-mfa-enabled	Enable MFA for root users. MFA enhances account security.
PSS-07	iam-password-policy	Set thresholds for IAM user password strength.

4.5.24 Compliance Package for PCI DSS

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

Background

PCI DSS is an information security standard for safe payments worldwide. PCI DSS contains technical and operational baselines to ensure data security of paying accounts. Although specifically designed to focus on environments with payment card account data, PCI DSS can also help reduce payment threats and protect the people, processes, and technologies across the payment ecosystem. For more information about PCI DSS, see **PCI DSS: v3.2.1**.

Applicable Scenarios

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

Exemption Clauses

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

Rules

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

Table 4-28 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	Use security groups to control connections to specified ports.
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	vpc-sg-restricted-common-ports	Configure security groups to control connections to common ports in a VPC.
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	vpc-sg-restricted-ssh	Configure security groups to restrict connections to SSH port 22 of ECSs.

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

Guideline No.	Guideline Description	Rule	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	Enable trace file verification for CTS trackers to prevent logs 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	Use this rule to identify ECSs that allow access from multiple public IPs. ECSs that can be accessed by multiple public IPs may increase security risks.

Guideline No.	Guideline Description	Rule	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.
2.2	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.	iam-user-group-membership-check	Ensure each user is in at least one user group for permission management. Granting users more permissions than they need may violate the principles of least privilege and separation of duties.

Guideline No.	Guideline Description	Rule	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 named system is created automatically. You can create multiple trackers for different regions to help make services better satisfy customer needs as well as legal or regulatory requirements.

Guideline No.	Guideline Description	Rule	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	Configure security groups to control access to resources in a VPC using common 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	Configure security groups to restrict connections to SSH port 22.
2.3	Encrypt all non-console administrative access using strong cryptography.	apig-instances-ssl-enabled	Enable SSL for APIG REST APIs to authenticate API requests.
2.3	Encrypt all non-console administrative access using strong cryptography.	css-cluster-https-required	After HTTPS is enabled for a CSS cluster, communication is encrypted when you access this cluster. If HTTPS is disabled, HTTP protocol is used for cluster communication. In this case, data security cannot be ensured and public address is not allowed.

Guideline No.	Guideline Description	Rule	Solution
2.3	Encrypt all non-console administrative access using strong cryptography.	dws-enable-ssl	Enable SSL for DWS clusters to protect data.
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	Enable HTTPS for CSS clusters to ensure data security and allow access over public networks. After HTTPS is disabled, HTTP protocol is used for cluster communication. In this case, data security cannot be ensured and public IP address cannot be used.

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

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

Guideline No.	Guideline Description	Rule	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	Use security groups to control connections to specified ports.

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	Configure security groups to control connections to common ports in a VPC.
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	vpc-sg-restricted-ssh	Configure security groups to restrict connections to SSH port 24.
1.3.1	Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	css-cluster-in-vpc	Deploy all CSS clusters within VPCs.
1.3.1	Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	css-cluster-in-vpc	Deploy all CSS clusters within VPCs.
1.3.1	Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	drs-data-guard-job-not-public	Block public access to DRS real-time DR tasks.

Guideline No.	Guideline Description	Rule	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	Use security groups to control connections to specified ports.

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	Configure security groups to control connections to common ports in a VPC.
1.3.1	Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	vpc-sg-restricted-ssh	Configure security groups to restrict connections to SSH port 25.
1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.	css-cluster-in-vpc	Deploy all CSS clusters within VPCs.
1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.	css-cluster-in-vpc	Deploy all CSS clusters within VPCs.
1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.	drs-data-guard-job-not-public	Block public access to DRS real-time DR tasks.
1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.	drs-migration-job-not-public	Block public access to DRS real-time migration tasks.
1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.	drs-synchronization-job-not-public	Block public access to DRS real-time synchronization tasks.
1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.	ecs-instance-in-vpc	Deploy all ECSs within VPCs.
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	Use security groups to control connections to specified ports.
1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.	vpc-sg-restricted-common-ports	Configure security groups to control connections to common ports in a VPC.
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	Use security groups to control connections to specified ports.
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	Use security groups to control connections to specified ports.

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	Configure security groups to control connections to common ports in a VPC.
1.3.6	Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	vpc-sg-restricted-ssh	Configure security groups to restrict connections to SSH port 28.
10.2.1	Implement automated audit trails for all system components to reconstruct the following events: all individual user accesses to cardholder data.	apig-instances-execution-logging-enabled	Enable CTS for your dedicated API gateways. APIG supports custom log analysis templates, which you can use to collect and manage logs and trace and analyze API request exceptions.
10.2.1	Implement automated audit trails for all system components to reconstruct the following events: all individual user accesses to cardholder data.	cts-obs-bucket-track	Create at least one CTS tracker for each OBS bucket.
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 named system is created automatically. You can create multiple trackers for different regions to help make services better satisfy customer needs as well as legal or regulatory requirements.
10.2.2	Implement automated audit trails for all system components to reconstruct the following events: All actions taken by any individual with root or administrative privileges.	cts-tracker-exists	Ensure that a CTS tracker has been created for your account to record operations on the Huawei Cloud console.
10.2.2	Implement automated audit trails for all system components to reconstruct the following events: All actions taken by any individual with root or administrative privileges.	multi-region-cts-tracker-exists	Create CTS trackers for different regions where your services are deployed. When you enable CTS for the first time, a management tracker named system is created automatically. You can create multiple trackers for different regions to help make services better satisfy customer needs as well as legal or regulatory requirements.

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 named system is created automatically. You can create multiple trackers for different regions to help make services better satisfy customer needs as well as legal or regulatory requirements.
10.2.4	Implement automated audit trails for all system components to reconstruct the following events: Invalid logical access attempts.	apig-instances-execution-logging-enabled	Enable CTS for your dedicated API gateways. APIG supports custom log analysis templates, which you can use to collect and manage logs and trace and analyze API request exceptions.

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 named system is created automatically. You can create multiple trackers for different regions to help make services better satisfy customer needs as well as legal or regulatory requirements.

Guideline No.	Guideline Description	Rule	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 named system is created automatically. You can create multiple trackers for different regions to help make services better satisfy customer needs as well as legal or regulatory requirements.
10.2.6	Implement automated audit trails for all system components to reconstruct the following events: Initialization, stopping, or pausing of the audit logs.	cts-tracker-exists	Ensure that a CTS tracker has been created for your account to record operations on the Huawei Cloud console.

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 named system is created automatically. You can create multiple trackers for different regions to help make services better satisfy customer needs as well as legal or regulatory requirements.
10.2.7	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 named system is created automatically. You can create multiple trackers for different regions to help make services better satisfy customer needs as well as legal or regulatory requirements.
10.3.1	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 named system is created automatically. You can create multiple trackers for different regions to help make services better satisfy customer needs as well as legal or regulatory requirements.
10.3.1	Record at least the following audit trail entries for all system components for each event: User identification.	vpc-flow-logs-enabled	Enable flow logs for VPCs to help monitor network traffic, analyze network attacks, and optimize security group and ACL configurations.
10.5.2	Protect audit trail files from unauthorized modifications.	cts-kms-encrypted-check	Enable trace file encryption for CTS trackers.
10.5.3	Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	cts-lts-enable	Enable **Transfer to LTS** for CTS trackers.
10.5.5	Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	cts-support-validate-check	Enable trace file verification for CTS trackers to prevent logs from being modified or deleted.

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	Use security groups to control connections to specified ports.
2.2.2	Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	vpc-sg-restricted-common-ports	Configure security groups to control connections to common ports in a VPC.
2.2.2	Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	vpc-sg-restricted-ssh	Configure security groups to restrict connections to SSH port 29.

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

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

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

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

Guideline No.	Guideline Description	Rule	Solution
7.2.2	Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: Coverage of all system components	iam-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(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: Coverage of all system components	mrs-cluster-kerberos-enabled	Enable Kerberos for MRS clusters.
8.1.1	Assign all users a unique ID before allowing them to access system components or cardholder data.	iam-root-access-key-check	Grant IAM users only necessary permissions for performing specific operations. Granting users more permissions than they need may violate the principles of least privilege and separation of duties.
8.1.4	Remove/disable inactive user accounts within 90 days.	access-keys-rotated	Enable key rotation.

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.	apig-instances-ssl-enabled	Enable SSL for API Gateway REST APIs to authenticate API requests.
8.2.1	Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	elb-tls-https-listeners-only	Ensure that your load balancer listeners are configured with the HTTPS protocol.
8.2.1	Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	rds-instances-enable-kms	Enable KMS for RDS to encrypt data at rest.
8.2.1	Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	sfsturbo-encrypted-check	Enable KMS for SFS Turbo file systems.
8.2.1	Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	volumes-encrypted-check	Enable encryption for EVS to protect data.

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.

4.5.25 Conformance Package for Healthcare Industry

The following table describes the compliance rules and solutions in the sample template.

Table 4-29 Conformance package description

Rule Identifier	Cloud Service	Description
apig-instances-execution-logging-enabled	apig	If logging is not enabled for a dedicated API gateway, this gateway is considered non-compliant.
apig-instances-ssl-enabled	apig	If no SSL certificates are attached to a dedicated API gateway, this gateway is considered 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-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.

Rule Identifier	Cloud Service	Description
cts-obs-bucket-track	cts	If there are no trackers created for the specified OBS bucket, the result 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 tracker in the current account, the result is noncompliant.
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.
drs-migration-job-not-public	drs	If the network type of a migration task is not set to public network, this 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 the **Audit Log Dump** is not enabled for a DWS cluster, 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 there is an ECS that is not within the specified VPC, the result is noncompliant.
ecs-instance-no-public-ip	ecs	If there is an ECS that is configured with a public IP, the result is noncompliant.

Rule Identifier	Cloud Service	Description
eip-unbound-check	vpc	If an EIP has not been attached to any resource, this EIP is noncompliant.
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 is not configured with 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 GaussDB NoSQL instance, this instance is noncompliant.
gaussdb-nosql-enable-disk-encryption	gaussdb nosql	If **Disk Encryption** is disabled for a GaussDB NoSQL 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 there is a user whose password does not meet the password complexity requirements, the result is noncompliant.

Rule Identifier	Cloud Service	Description
iam-policy-no-statements-with-admin-access	iam	If there is an IAM policy or role that grants administrator permissions (the **Action** element is ***:*:***, ***:***, or *****), the result is noncompliant.
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 root access key is available, the result 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 is attached with a public IP, this cluster is noncompliant.
multi-region-cts-tracker-exists	cts	If there are no trackers in any of the specified regions, the result is noncompliant.

Rule Identifier	Cloud Service	Description
pca-certificate-authority-expiration-check	pca	If the validity period of a private CA is not within the specified range, this CA is noncompliant.
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 cluster is deployed in a single availability zone, this cluster is noncompliant.
rds-instance-no-public-ip	rds	If an RDS instance is attached with an EIP, this 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.

Rule Identifier	Cloud Service	Description
stopped-ecs-date-diff	ecs	If there is an ECS that has been stopped for longer than the time allowed, and no operations have been performed on it, the result 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 there is a network ACL that has not been associated with any subnets, the result 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 (**Source**: 0.0.0.0/0) and has no port specified, 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** for the TCP 22 port, this security group is non-compliant.
vpn-connections-active	vpnaas	If the state of a VPN connection is not connected, the result is noncompliant.

5 Advanced Queries

5.1 Overview

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

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

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

You can use Advanced Queries to:

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

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 a long time, note the following restrictions:

- If the execution duration of a query statement exceeds15 seconds, a timeout error will be returned.
- If a query generates a large amount of data and an error is returned, you need to simplify the query statement.

- Only the first 4,000 records are returned for a single query.
- A single query statement can be used to perform a maximum of two join queries for tables.
- A maximum of 200 advanced queries can be created for each account.

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 is 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 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 Query**
- **Saving a Query**
- **Configuration Examples of Advanced Queries**

Creating a Query

Step 1 Sign in to Config console.

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

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

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

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

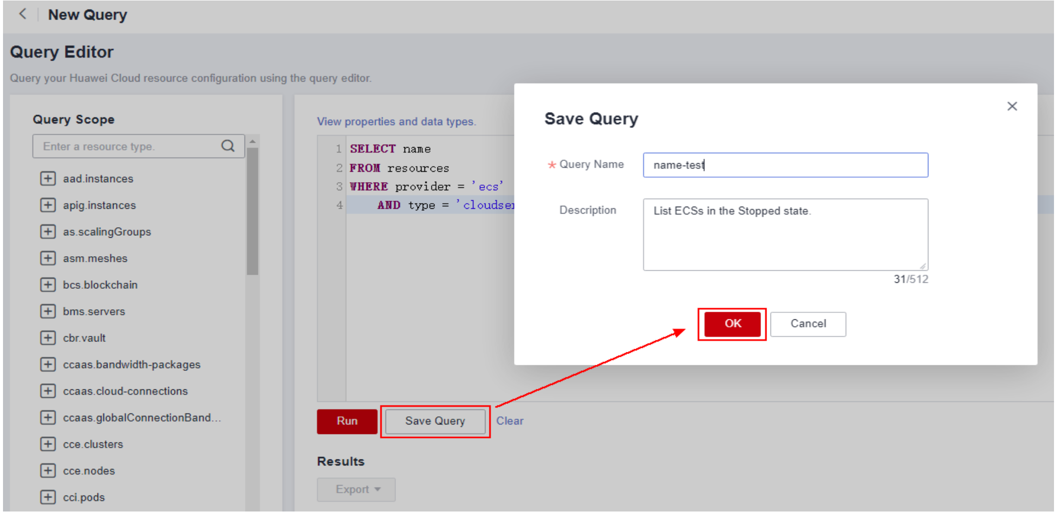
The Schema information used for advanced query is displayed on the left of the page. The properties parameter included in a request should be set to the Schema information which shows the detailed attributes of a cloud service resource. For details about the configuration example of the query statement,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

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

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

Step 7 Click **OK**.

Figure 5-1 Save Query



```
SELECT name
FROM resources
WHERE provider = 'ecs'
    AND type = 'cloudser
```

* Query Name: name-test

Description: List ECSs in the Stopped state.

31/512

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." You will still be able to run custom queries and export the results, but no more custom queries can be saved.

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

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

----End

Saving a Query

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

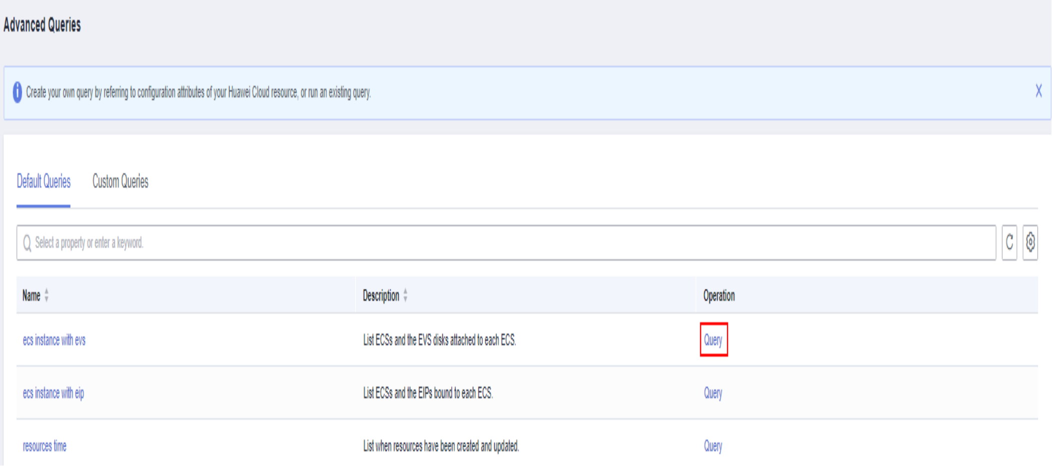
Step 1 Choose **Advanced Queries** > **Default Queries**.

All default queries are displayed in a list.

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

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

Figure 5-2 Default queries



Advanced Queries

Create your own query by referring to configuration attributes of your Huawei Cloud resource, or run an existing query.

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
resources time	List when resources have been created and updated.	Query

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

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

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

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

NOTE

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

----End

Configuration Examples of Advanced Queries

Advanced queries 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.

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

Example quires are as follows:

- Example 1: List ECSs in the **Stopped** state.

```
SELECT name
FROM resources
WHERE provider = 'ecs'
   AND type = 'cloudservers'
   AND properties.status = 'SHUTOFF'
```

- Example 2: List EVS disks with certain specifications.

```
SELECT *
FROM resources
WHERE provider = 'evs'
   AND type = 'volumes'
   AND properties.size = 100
```

- Example 3: List OBS buckets queried by fuzzy search.

```
SELECT *
FROM resources
WHERE provider = 'obs'
   AND 'type' = 'buckets'
   AND name LIKE '%figure%'
```

- Example 4: List ECSs and the EVS disks attached to each ECS.

```
SELECT ECS_EVS.id AS ecs_id, EVS.id AS evs_id
FROM (
   SELECT id, evs_id
   FROM (
   SELECT id, transform(properties.ExtVolumesAttached, x -> x.id) AS evs_list
   FROM resources
   WHERE provider = 'ecs'
      AND type = 'cloudservers'
   ) ECS
     CROSS JOIN UNNEST(evs_list) AS t (evs_id)
) ECS_EVS, (
   SELECT id
   FROM resources
   WHERE provider = 'evs'
      AND type = 'volumes'
```

```
    ) EVS
WHERE ECS_EVS.evs_id = EVS.id
```

- Example 5: List ECSs and the EIPs bound to each ECS.

```
SELECT ECS.id AS ECS_id, publicIpAddress AS ip_address
FROM (
    SELECT id, transform(properties.addresses, x -> x.addr) AS ip_list
    FROM resources
    WHERE provider = 'ecs'
        AND type = 'cloudservers'
) ECS, (
        SELECT name, properties.publicIpAddress
        FROM resources
        WHERE provider = 'vpc'
            AND type = 'publicips'
            AND properties.type = 'EIP'
            AND properties.status = 'ACTIVE'
    ) EIP
WHERE CONTAINS (ECS.ip_list, EIP.name)
```

- Example 6: List resources with a quantity greater than 100 in each region.

```
WITH counts AS (
    SELECT region_id, provider, type, count(*) AS number
    FROM resources
    GROUP BY region_id, provider, type
)
SELECT *
FROM counts
WHERE number > 100
```

For details about query statements, see **ResourceQL Syntax**.

5.4 Viewing a Query

Scenarios

You can view the name, description, and SQL statement of a query.

Procedure

Step 1 Sign in to Config console.

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

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

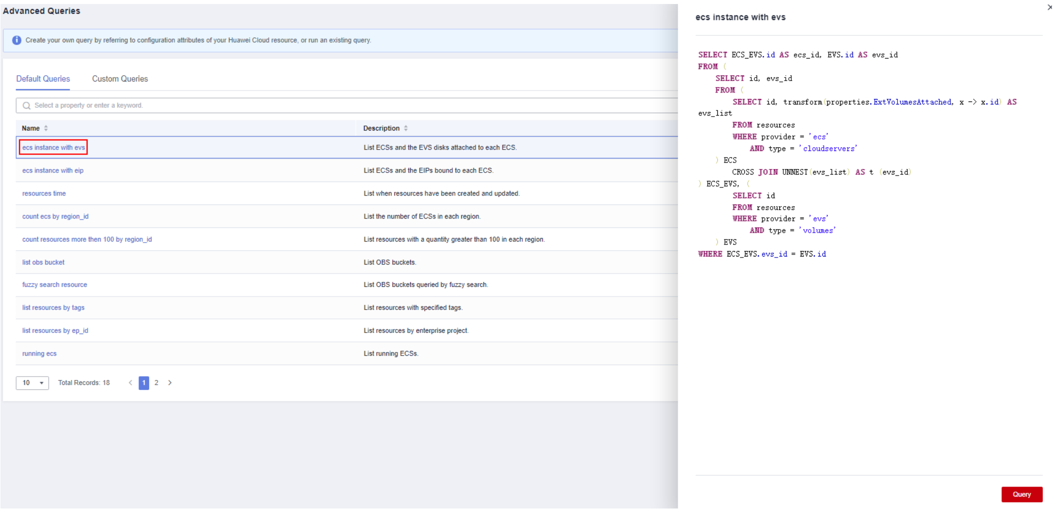
By default, the default query list is displayed. To view custom queries, click **Custom Queries**.

View the query name and description in the query list.

Step 4 Locate the query and click its name.

The SQL statement details in the query are displayed.

Figure 5-3 Viewing query details



Advanced Queries

Create your own query by referring to configuration attributes of your Huawei Cloud resource, or run an existing query.

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 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
```

----End

5.5 Modifying a Query

Scenarios

You can modify the statement of a custom query if needed.

NOTE

Default queries cannot be modified.

Procedure

Step 1 Sign in to Config console.

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

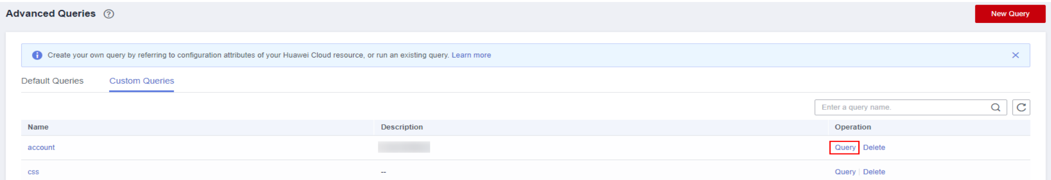
Step 3 In the left navigation, choose **Advanced Queries**.

Step 4 Click the **Custom Queries** tab.

Step 5 Locate the row that contains the query to be modified, and click **Query** in the **Operation** column.

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

Figure 5-4 Modifying a custom query



Create your own query by referring to configuration attributes of your Huawei Cloud resource, or run an existing query. Learn more

Name	Description	Operation
account	[redacted]	Query Delete
css	--	Query | Delete

Step 6 In the query editor, modify the query statement as prompted.

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**.

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

----End

5.6 Deleting a Query

Scenarios

You can delete a custom query if you no longer need it.

Preset queries cannot be deleted.

Procedure

Step 1 Sign in to Config console.

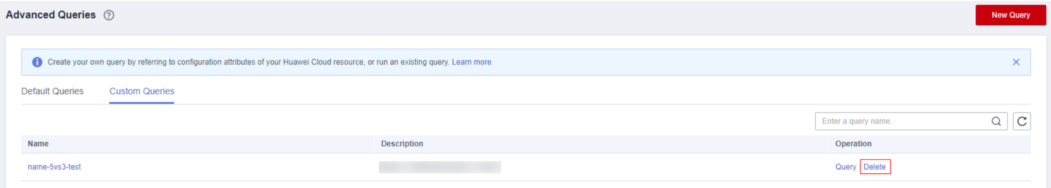
Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

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

Step 4 Click **Custom Queries**.

Step 5 Locate the custom query to be deleted and click **Delete** in the **Operation** column.

Figure 5-5 Deleting a custom query



Advanced Queries

Create your own query by referring to configuration attributes of your Huawei Cloud resource, or run an existing query. Learn more

Name	Description	Operation
name-5vs3-test	[redacted]	Query Delete

Step 6 In the dialog box that is displayed, click **OK**.

----End

6 Resource Aggregation

6.1 Overview

Functions

A resource aggregator enables you to aggregate resource configurations and compliance data from multiple accounts or an organization, so that you can centrally view or search for these resource data.

You can only view aggregated resources and their compliance data instead of modifying resource data. For example, you cannot use a resource aggregator to deploy rules or access snapshot files from a source account.

📖 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 from source accounts. For more details, see **Viewing Aggregated Rules** and **Viewing Aggregated Resources**.

Basic Concepts

Source Account

A source account is an account from which Config aggregates resource configurations and compliance data. A source account can be 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

Authorization refers to the permissions that an aggregator account needs to obtain from a source account to collect resource configuration and compliance data from the source account. Authorization is not required for an organization specific aggregator.

6.2 Restrictions

Usage limits for aggregators are as follows:

- Up to 30 account specific aggregators can be created in an account.
- An aggregator can aggregate data from up to 30 source accounts.
- An account specific aggregator can add, update, and delete up to 1,000 source accounts within 7 days.
- Up to 1 organization specific aggregator can be created in an account.
- You cannot create organization aggregators multiple times a day. For example, if you create and then delete an organization aggregator on the same day, creating another organization aggregator on the same day is not support.
- An aggregator can collect data from a source account only after the resource recorder has been enabled in the source account.

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 is enabled and then disabled after a period of time in a source account, related data aggregated by the aggregator will be deleted.

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 resource data from a source account to an aggregator account, authorization from the source account is required. For details, see **Authorizing a Resource Aggregator Account**.

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 Sign in to the Config console.

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

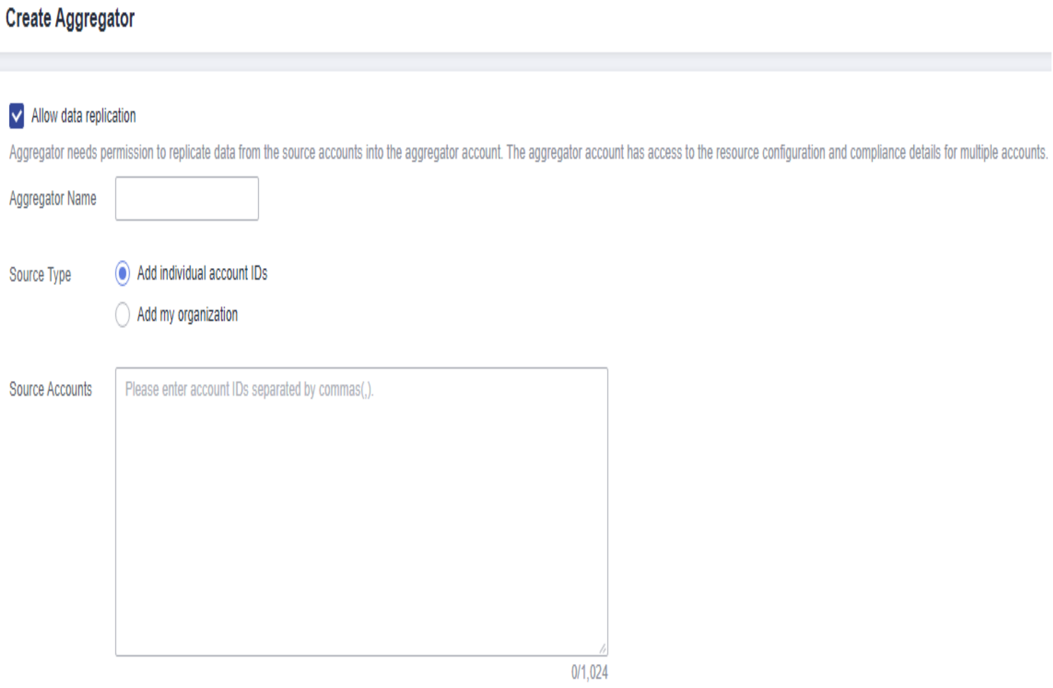
Step 3 In the left navigation, choose **Resource Aggregation** > **Aggregators**.

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

Step 5 On the **Create Aggregator** page, select **Allow data replication** and configure the aggregator name and source accounts.

If you select **Add individual account IDs** for **Source Type**, enter account IDs and separate them with commas (,). If you select **Add my organization**, the resource aggregator aggregates data of all member accounts in the organization without the need to specify individual account IDs.

Figure 6-1 Create Aggregator



Create Aggregator

☑ Allow data replication

Aggregator needs permission to replicate data from the source accounts into the aggregator account. The aggregator account has access to the resource configuration and compliance details for multiple accounts.

Aggregator Name

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 Sign in to the Config console.

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

Step 3 In the left navigation, choose **Resource Aggregation** > **Aggregators**.

Step 4 On the **Aggregators** page, view all resource aggregators created.

You can use the filter in the upper right corner of the list to search for the resource aggregator you want to view. Exact search by complete aggregator name is supported.

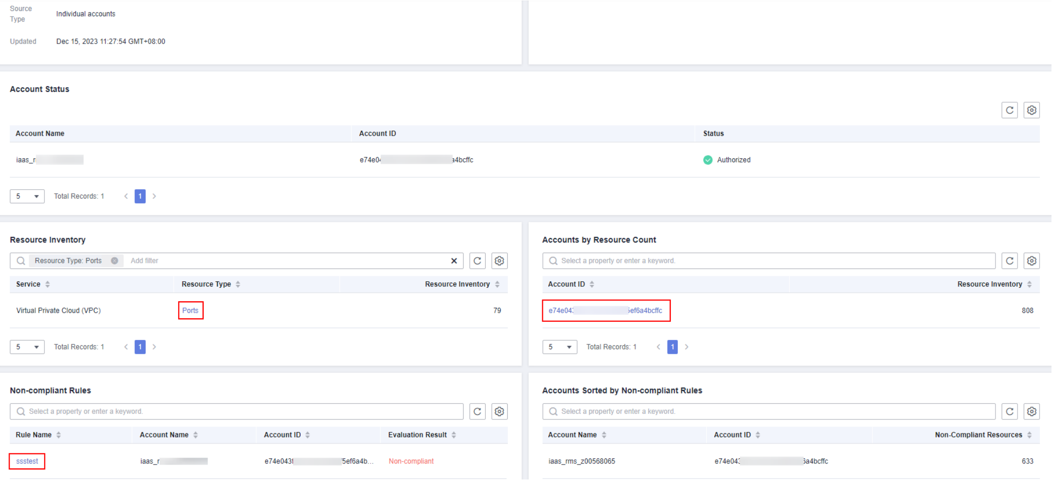
Step 5 Locate the aggregator you want to view and click its name.

Click a target resource type in the **Resource Inventory** area to view all aggregated resources of this resource type.

Click a target account ID in the **Accounts by Resource Count** area to view all aggregated resources from this account.

On the details page, click a rule name in the **Rule That Have Found Non-compliant** area.

Figure 6-2 Resource aggregator details page



Source Type: Individual accounts

Updated: Dec 15, 2023 11:27:54 GMT+08:00

Account Status

Account Name	Account ID	Status
iaas_r[redacted]	e74e0[redacted]a4bcffc	✓ Authorized

5 ▾ Total Records: 1 ‹ 1 ›

Resource Inventory

Resource Type: Ports ⊗ Add filter ✕

Service	Resource Type	Resource Inventory
Virtual Private Cloud (VPC)	Ports	79

5 ▾ Total Records: 1 ‹ 1 ›

Accounts by Resource Count

Select a property or enter a keyword.

Account ID	Resource Inventory
e74e04[redacted]ef6a4bcffc	808

5 ▾ Total Records: 1 ‹ 1 ›

Non-compliant Rules

Select a property or enter a keyword.

Rule Name	Account Name	Account ID	Evaluation Result
ssstest	iaas_r[redacted]	e74e043[redacted]5ef6a4b...	Non-compliant

Accounts Sorted by Non-compliant Rules

Select a property or enter a keyword.

Account Name	Account ID	Non-Compliant Resources
iaas_rms_z00568065	e74e04[redacted]a4bcffc	633

----End

6.5 Editing 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 Sign in to the Config console.

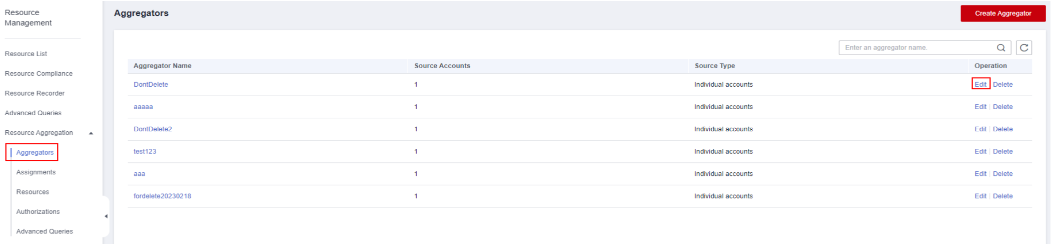
Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

Step 3 In the left navigation, choose **Resource Aggregation** > **Aggregators**.

Step 4 Locate the aggregator to be edited and click **Edit** in the **Operation** column.

Alternatively, in the upper right corner of the resource aggregator details page, click **Edit** to go to the **Edit Aggregator** page.

Figure 6-3 Editing a resource aggregator



Aggregator Name	Source Accounts	Source Type	Operation
DontDelete	1	Individual accounts	Edit Delete
aaaaa	1	Individual accounts	Edit | Delete
DontDelete2	1	Individual accounts	Edit | Delete
test123	1	Individual accounts	Edit | Delete
aaa	1	Individual accounts	Edit | Delete
fordelete20230218	1	Individual accounts	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 Sign in to the Config console.

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

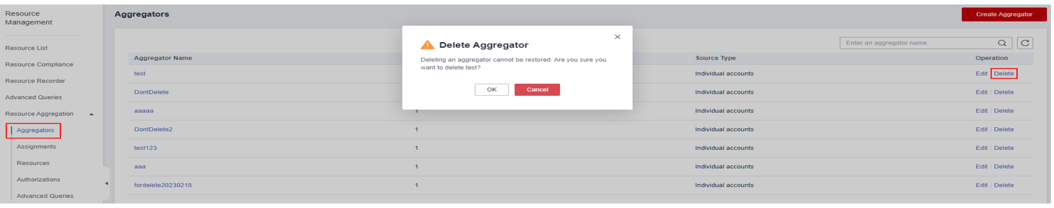
Step 3 In the left navigation, choose **Resource Aggregation** > **Aggregators**.

Step 4 In the resource aggregator list, locate the aggregator to be deleted and click **Delete** in the **Operation** column.

Alternatively, in the upper right corner of the resource aggregator details page, click **delete**.

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

Figure 6-4 Delete Aggregator



Aggregators

Delete Aggregator

Deleting an aggregator cannot be restored. Are you sure you want to delete test?

OK Cancel

Aggregator Name		Source Type	Operation
test		Individual accounts	Edit | Delete
DontDelete		Individual accounts	Edit | Delete
aaaaa	1	Individual accounts	Edit | Delete
DontDelete2	1	Individual accounts	Edit | Delete
test123	1	Individual accounts	Edit | Delete
aaa	1	Individual accounts	Edit | Delete
fordelete20230218	1	Individual accounts	Edit | Delete

----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 Sign in to the Config console.

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

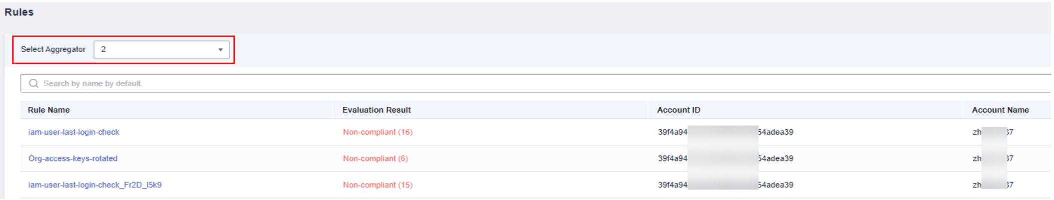
Step 3 On the left navigation, choose **Resource Aggregation** > **Rules**.

Step 4 In the upper right corner, select an aggregator from the drop-down list to view compliance data aggregated by this aggregator.

In the rule list, click a target rule name to view rule details.

In the search box above the list, enter a rule name, evaluation result, or account ID to filter compliance data.

Figure 6-5 Viewing aggregated rules



Rules

Select Aggregator: 2

Search by name by default.

Rule Name	Evaluation Result	Account ID	Account Name
iam-user-last-login-check	Non-compliant (16)	39f4a94[redacted]4adea39	zh[redacted]7
Org-access-keys-rotated	Non-compliant (6)	39f4a94[redacted]4adea39	zh[redacted]7
iam-user-last-login-check_Fr2D_I5k9	Non-compliant (15)	39f4a94[redacted]4adea39	zh[redacted]7

----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 Sign in to the Config console.

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

Step 3 In the navigation pane, choose **Resource Aggregation** > **Resources**.

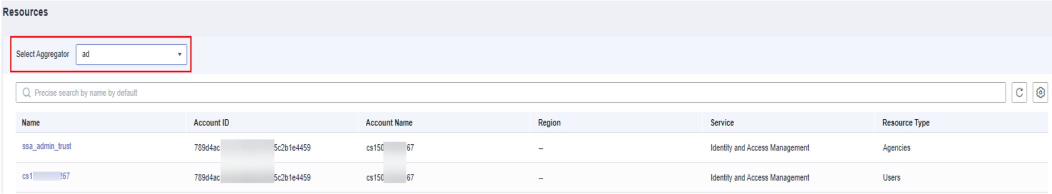
Step 4 In the upper left corner, select an aggregator.

All resources aggregated by the aggregator are displayed in a list.

In the search box above the list, enter a resource name, an account ID, or a resource type to filter resource data.

In the resource list, click a target resource name to view resource details.

Figure 6-6 Viewing aggregated resources



Resources

Select Aggregator: ad

Precise search by name by default

Name	Account ID	Account Name	Region	Service	Resource Type
ssa_admin_trust	789d4ac[redacted]5c2b1e4459	cs150[redacted]67	--	Identity and Access Management	Agencies
cs1[redacted]267	789d4ac[redacted]5c2b1e4459	cs150[redacted]67	--	Identity and Access Management	Users

----End

6.9 Authorizing an Aggregator Account

Scenarios

Before an aggregator account initiates aggregation requests, source accounts must grant this account the permissions to collect resource configurations and compliance data. There are no requirements on the order of adding authorization and creating an aggregator.

An organization specific aggregator can collect resource data of all member accounts in an organization without source account authorization.

Helpful links:

- **Adding Authorization**
- **Accepting an Authorization**
- **Deleting an Authorization**

Adding an Authorization

You can use the **Add Authorization** function to authorize an aggregator account.

Step 1 Sign in to the Config console.

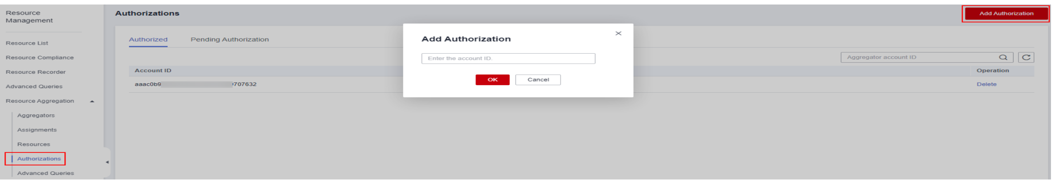
Step 2 Click ☰ in the upper left corner. Under **Management & Governance**, click **Config**.

Step 3 In the left navigation, choose **Resource Aggregation** > **Authorizations**.

Step 4 Click **Add Authorization** in the upper right corner of the page.

Step 5 In the **Add Authorization** dialog box, enter the ID of the aggregator account which you want to authorize.

Figure 6-7 Adding an authorization



Account ID	Operation
aaac0b9[redacted]707632	Delete

Step 6 Click **OK**.

After the authorization is complete, the authorization record is displayed in the **Authorized** list.

----End

Accepting an Authorization

You can approve a pending authorization request to authorize an aggregator account.

Step 1 Sign in to the Config console.

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

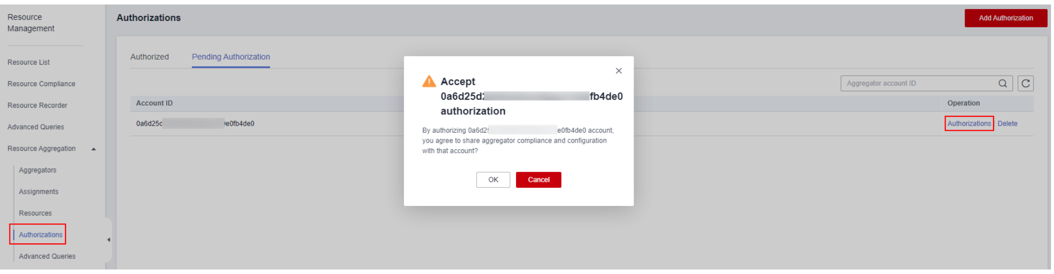
Step 3 In the left navigation, choose **Resource Aggregation** > **Authorizations**.

Step 4 Click the **Pending Authorization** tab, locate the account ID that sends an authorization request to be processed in the list, and click **Authorize** in the **Operation** column.

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

After the authorization request is accepted, the authorization record is displayed in the **Authorized** list.

Figure 6-8 Accepting an authorization



Account ID	Operation
0a6d25c[redacted]e0fb4de0	Authorizations Delete

Accept 0a6d25d[redacted]fb4de0 authorization

By authorizing 0a6d2[redacted]e0fb4de0 account, you agree to share aggregator compliance and configuration with that account?

----End

Deleting an Authorization

You can revoke authorization from an aggregator account.

Step 1 Sign in to the Config console.

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

Step 3 In the left navigation, choose **Resource Aggregation** > **Authorizations**.

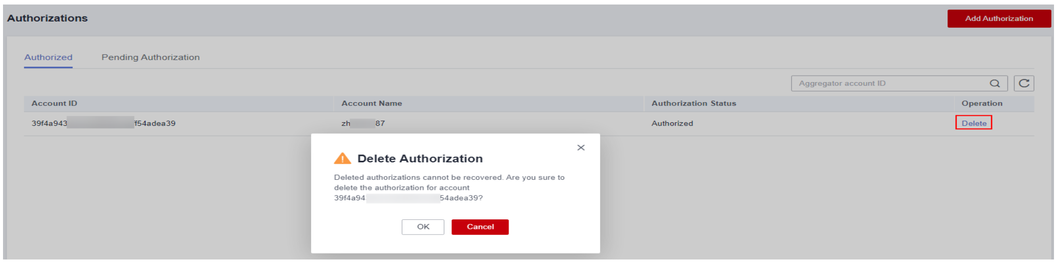
Step 4 Locate the authorization to be deleted in the list, and click **Delete** in the **Operation** column.

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

The authorization record 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 Deleting an authorization



Account ID	Account Name	Authorization Status	Operation
39f4a943[redacted]f54adea39	zh[redacted]87	Authorized	Delete

Delete Authorization

Deleted authorizations cannot be recovered. Are you sure to delete the authorization for account 39f4a94[redacted]54adea39?

Step 6 In the **Pending Authorization** list, locate the authorization, and click **Delete** in the **Operation** column. In the displayed dialog box, click **OK** to delete the authorization record completely.

NOTE

You can authorize an aggregator account again after revoking the authorization from this account.

----End

6.10 Advanced Queries

Overview

Resource aggregation supports advanced queries. You can use ResourceQL to query configuration states of one or multiple aggregator accounts.

You can create custom queries using **Query Editor**.

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

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

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 a long time, note the following restrictions:

- If the execution duration of a query statement exceeds15 seconds, a timeout error will be returned.
- If a query generates a large amount of data and an error is returned, you need to simplify the query statement.
- Only the first 4,000 records are returned for a single query.
- A single query statement can be used to perform a maximum of two join queries for tables.
- A maximum of 200 advanced queries can be created for each account.

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 is 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 left navigation, choose **Resource Aggregation** > **Advanced Queries**.

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

Step 5 On the **Query Range** area on the right, select the aggregator whose resource configuration needs to be queried. In the text box below, enter the query statement.

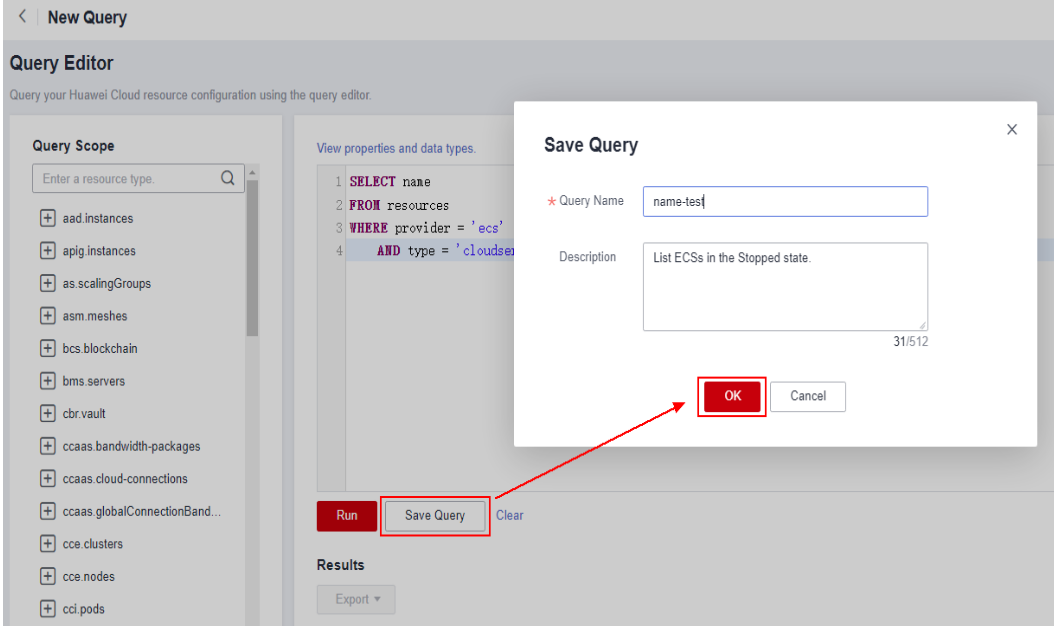
The Schema information used for advanced query is displayed on the left of the page. The properties parameter included in a request should be set to the Schema information which shows the detailed attributes of a cloud service resource. For details about the configuration example of the query statement,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

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

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

Step 7 Click **OK**.

Figure 6-10 Save Query



```
SELECT name
FROM resources
WHERE provider = 'ecs'
   AND type = 'cloudse
```

Query Name: name-test

Description: List ECSs in the Stopped state.

31/512

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." You will still be able to run custom queries and export the results, but no more custom queries can be saved.

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

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

----End

Other Operations

- You can modify the name, description, and query statement of a default query or an existing custom query. After you click **Save As**, a new query is generated. For details, see **Saving a 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 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.
provider	String	Cloud service name
type	String	Resource type
region_id	String	Region ID
project_id	String	Project ID
ep_id	String	Enterprise project ID
checksum	String	Resource checksum
created	Date	The time when the resource was created
updated	Date	The time when the resource was updated
provisioning_state	String	The result of an operation on resources.
tag	Array(Map<String,String>)	Resource tag
properties	Map<String,Object>	Resource attributes

Example quires are as follows:

- Example 1: Querying the names of stopped ECSs in a resource aggregator

```
SELECT domainId, name
FROM aggregator_resources
WHERE provider = 'ecs'
   AND type = 'cloudservers'
   AND properties.status = 'SHUTOFF'
```

- Example 2: Querying EVS disks of specified specifications in a resource aggregator

```
SELECT *
FROM aggregator_resources
WHERE provider = 'evs'
   AND type = 'volumes'
   AND properties.size = 100
```

- Example 3: Fuzzily querying OBS buckets in the resource aggregator

```
SELECT *
FROM aggregator_resources
WHERE provider = 'obs'
   AND 'type' = 'buckets'
   AND name LIKE '%figure%'
```

- Example 4: Querying the types of resources whose count is greater than 100 under each source account

```
WITH counts AS (
    SELECT region_id, provider, type, count(*) AS number
    FROM aggregator_resources
    GROUP BY domain_id, provider, type
 )
 SELECT *
 FROM counts
 WHERE number > 100
```

For details about query statements, see **ResourceQL Syntax**.

7 Cloud Trace Service

7.1 Supported CTS Operations

Scenarios

Cloud Trace Service (CTS) records operations on Config for your later query, audit, and backtrack.

Prerequisites

You have enabled CTS.

Key Operations Recorded by CTS

Table 7-1 Config operations recorded by CTS

Operation	Resource Type	Event Name
Adding a rule	policy	createPolicyAssignments
Deleting a rule	policy	deletePolicyAssignment
Modifying a rule	policy	updatePolicyAssignment
Triggering a resource evaluation	policy	runEvaluation
Disabling a rule	policy	disablePolicyAssignment
Enabling a rule	policy	enablePolicyAssignment
Creating or modifying resource recorder configuration	trackerConfig	createOrUpdateTracker-Config
Deleting the resource recorder configuration	trackerConfig	deleteTrackerConfig

Operation	Resource Type	Event Name
Creating an advanced query	storedQuery	createStoredQuery
Updating an advanced query	storedQuery	updateStoredQuery
Deleting an advanced query	storedQuery	deleteStoredQuery
Updating a compliance evaluation result	policyState	updatePolicyState
Creating or updating an organization rule	organizationPolicyAssignments	createOrganizationPolicyAssignment
Deleting an organization rule	organizationPolicyAssignments	deleteOrganizationPolicyAssignment
Creating authorization	authorization	createAggregationAuthorization
Deleting authorization	authorization	deleteAggregationAuthorization
Creating an aggregator	aggregator	createConfigurationAggregator
Deleting an aggregator	aggregator	deleteConfigurationAggregator
Updating an aggregator	aggregator	updateConfigurationAggregator
Deleting a pending authorization request	aggregationRequests	deletePendingAggregationRequest
Creating a conformance package	conformancePacks	createConformancePack
Deleting a conformance package	conformancePacks	deleteConformancePack

7.2 Querying Real-Time Traces

Scenarios

After you enable CTS and the management tracker is created, CTS starts recording operations on cloud resources. After a data tracker is created, the system starts recording operations on data in OBS buckets. CTS stores operation records generated in the last seven days.

This section describes how to query and export operation records of the last seven days on the CTS console.

- **Viewing Real-Time Traces in the Trace List of the New Edition**
- **Viewing Real-Time Traces in the Trace List of the Old Edition**

Constraints

- Traces of a single account can be viewed on the CTS console. Multi-account traces can be viewed only on the **Trace List** page of each account, or in the OBS bucket or the **CTS/system** log stream configured for the management tracker with the organization function enabled.
- You can only query operation records of the last seven days on the CTS console. To store operation records for more than seven days, you must configure an OBS bucket to transfer records to it. Otherwise, you cannot query the operation records generated seven days ago.
- After performing operations on the cloud, you can query management traces on the CTS console 1 minute later and query data traces on the CTS console 5 minutes later.

Viewing Real-Time Traces in the Trace List of the New Edition

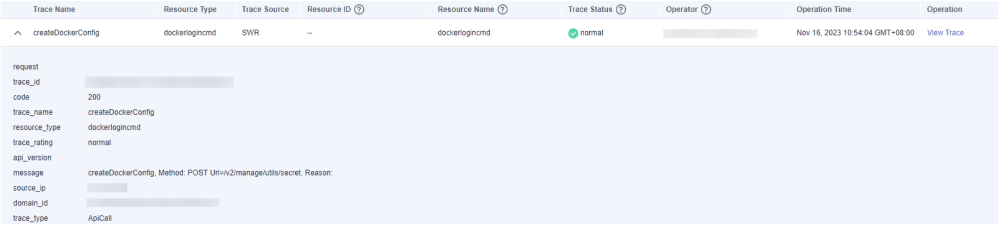
1. Log in to the management console.
2. Click ☰ in the upper left corner and choose **Management & Governance** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. On the **Trace List** page, use advanced search to query traces. You can combine one or more filters.
   - **Trace Name**: Enter a trace name.
   - **Trace ID**: Enter a trace ID.
   - **Resource Name**: Enter a resource name. If the cloud resource involved in the trace does not have a resource name or the corresponding API operation does not involve the resource name parameter, leave this field empty.
   - **Resource ID**: Enter a resource ID. Leave this field empty if the resource has no resource ID or if resource creation failed.
   - **Trace Source**: Select a cloud service name from the drop-down list.
   - **Resource Type**: Select a resource type from the drop-down list.
   - **Operator**: Select one or more operators from the drop-down list.
   - **Trace Status**: Select **normal**, **warning**, or **incident**.
     - **normal**: The operation succeeded.
     - **warning**: The operation failed.
     - **incident**: The operation caused a fault that is more serious than the operation failure, for example, causing other faults.
   - Time range: Select **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range.
5. On the **Trace List** page, you can also export and refresh the trace list, and customize the list display settings.

- Enter any keyword in the search box and 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 5000 records.
- Click ⟳ to view the latest information about traces.
- Click ⚙ to customize the information to be displayed in the trace list. If **Auto wrapping** is enabled (●), excess text will move down to the next line; otherwise, the text will be truncated. By default, this function is disabled.

6. For details about key fields in the trace structure, see **Trace Structure** and **Example Traces**.
7. (Optional) On the **Trace List** page of the new edition, click **Go to Old Edition** in the upper right corner to switch to the **Trace List** page of the old edition.

Viewing Real-Time Traces in the Trace List of the Old Edition

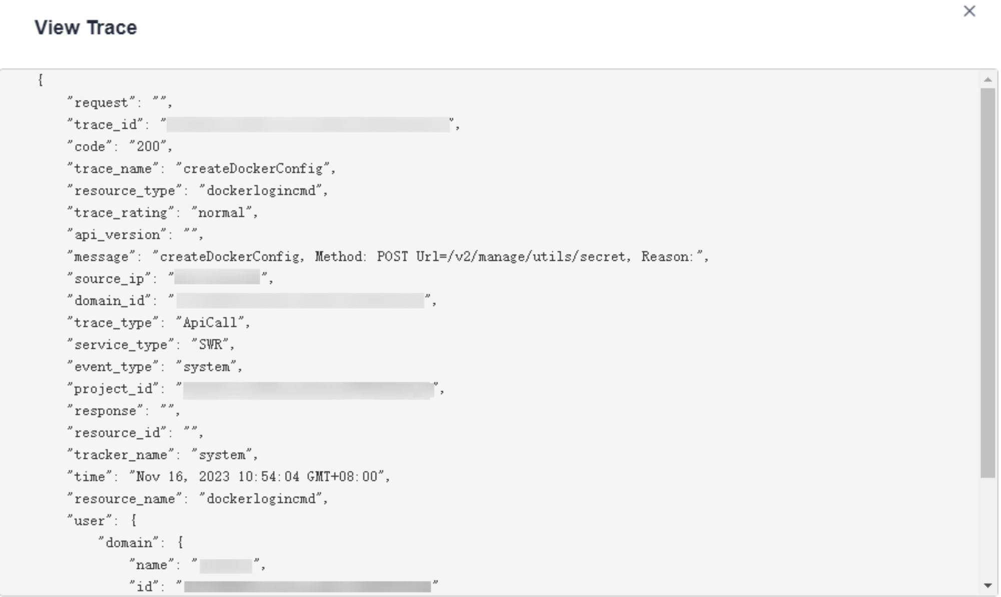
1. Log in to the management console.
2. Click ☰ in the upper left corner and choose **Management & Governance** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. Each time you log in to the CTS console, the new edition is displayed 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: You can query traces generated during any time range in the last seven days.
   - Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5000 records.
6. Click **Query**.
7. On the **Trace List** page, you can also export and refresh the trace list.
   - Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5000 records.
   - Click ⟳ to view the latest information about traces.
8. Click ⌄ on the left of a trace to expand its details.



	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.



```
{
    ”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 services and regions supported by Config, see **Supported Services and Regions**.

8.2 Relationships with Supported Resources

Table 8-1 Relationships with supported resources

Service	Resource Type	Relationship	Related Service	Related Resource Type
ECS	Cloud server	isContainedIn	VPC	VPC
			MRS	MRS
		isAttachedTo	VPC	Elastic IP
			EVS	Volume
		isAssociatedWith	VPC	Security group
			IMS	Image
BMS	Cloud server	isContainedIn	VPC	VPC
		isAttachedTo	EVS	Volume
		isAssociatedWith	VPC	Security group
			IMS	Image

Service	Resource Type	Relationship	Related Service	Related Resource Type
HECS	Hyper Elastic Cloud Server (HECS)	isContainedIn	VPC	VPC
		contains	VPC	Elastic IP
		isAttachedTo	EVS	volumes
		isAssociatedWith	VPC	Security group
			IMS	Image
AS	AS group	isContainedIn	VPC	VPC
		isAssociatedWith	VPC	Security group
DCS	Memcached instance	isContainedIn	VPC	VPC
		isAssociatedWith	VPC	Security group
	Node	isContainedIn	DCS	Redis instance
	Redis instance	isContainedIn	VPC	VPC
		contains	DCS	Node
		isAssociatedWith	VPC	Security group
ELB	Load balancer	contains	ELB	Listener
		isAttachedTo	VPC	Elastic IP
			ELB	Server group
			ELB	Server group
	Listener	Is contained in	ELB	Load balancer
		Is attached to	ELB	Server group
			ELB	Server group
	Server group	Contains	ELB	Server
		Is attached to	ELB	Load balancer

Service	Resource Type	Relationship	Related Service	Related Resource Type
			ELB	Listener
	Server group	Contains	ELB	Server
		Is attached to	ELB	Load balancer
			ELB	Listener
	Server	Is contained in	ELB	Server group
			ELB	Server group
VPC	VPC	contains	ECS	Cloud server
			BMS	Cloud server
			HECS	HECS
			AS	AS group
			DCS	Memcached instance
			DCS	Redis instance
			MRS	MRS
	Security group	isAssociatedWith	ECS	Cloud server
			BMS	Cloud server
			HECS	HECS
			AS	AS group
			DCS	Memcached instance
			MRS	mrs
			DCS	Redis instance
	Bandwidth	contains	VPC	publicips
	Elastic IP	isContainedIn	VPC	Bandwidth

Service	Resource Type	Relationship	Related Service	Related Resource Type
		isAttachedTo	ECS	Cloud server
			ELB	Load balancer
			MRS	MRS
			NAT Gateway	Public NAT gateway
EVS	Volume	isAttachedTo	ECS	Cloud server
			BMS	Cloud server
			HECS	HECS
IMS	Image	isAssociatedWith	ECS	Cloud server
			BMS	Cloud server
			HECS	HECS
NAT Gateway	Public NAT gateway	isAttachedTo	VPC	Elastic IP
GaussDB NoSQL	Instance	contains	GaussDB NoSQL	Node
	Node	isContainedIn	GaussDB NoSQL	Instance
GaussDB	Instance	contains	GaussDB	Node
	Node	isContainedIn	GaussDB	Instance
MRS	MRS	isContainedIn	VPC	VPC
		isAttachedTo	VPC	Elastic IP
		isAssociatedWith	VPC	Security group
		contains	ECS	Cloud server
CCE	Cluster	contains	CCE	Node
	Node	isContainedIn	CCE	Cluster

Service	Resource Type	Relationship	Related Service	Related Resource Type
Enterprise Router	Connection	isContainedIn	Enterprise Router	Instance
	Instance	contains	Enterprise Router	Connection
IAM	User group	contains	IAM	User
	User	isContainedIn	IAM	User group
RDS	Instance	contains	RDS	Node
	Node	isContainedIn	RDS	Instance
Config	Conformance package	Contains	Config	Rule
	Rule	Is contained in	Config	Conformance package

8.3 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)
Bare Metal Server (BMS)	BMSs (bms.servers)

Service	Resource type
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 (SFS)	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)
Document Database Service (DDS)	● Instances (dds.instances) ● Nodes (dds.nodes)
Cloud Search Service (CSS)	Clusters (css.clusters)

Service	Resource type
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)
IoT Device Access (IoTDA)	- Basic Instances (iotda.iotda) - Enterprise Instances (iotda.iotda_instance) - Standard Instances (iotda.iotda_standardinstance)
Global Accelerator (GA)	Accelerators (ga.accelerators)

Service	Resource type
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 Message Notification Models

Config send notifications when:

- Resources are created, modified, or deleted.
- Resource relationships change.
- Notifications of resource changes are stored.
- Resource snapshots are stored.

Notification Model of Resource Changes

Table 8-3 Parameter description

Parameter	Type	Description
notification_type	String	Specifies the message notification type.
notification_creation_time	String	Specifies the time when the message was sent. The time is a UTC time in a fixed format complying with ISO-8601 (for example, **2018-11-14T08:59:14Z**).
domain_id	String	Account ID
detail	Object	Specifies the message details.

Table 8-4 detail parameters

Parameter	Type	Description
resource_id	String	Specifies the resource ID.
resource_type	String	Specifies the resource type.
event_type	Enum	Specifies the event type. The value can be **CREATE**, **UPDATE**, or **DELETE**.
capture_time	String	Specifies the time when the event was captured. The time is a UTC time in a fixed format complying with ISO-8601 (for example, **2018-11-14T08:59:14Z**).
resource	Object	Specifies the resource details.

Table 8-5 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.

Parameter	Type	Description
region_id	String	Specifies the ID of the region where the resource is located.
project_id	String	Specifies the IAM project ID.
project_name	String	Specifies the IAM project name.
ep_id	String	Specifies the enterprise project ID.
ep_name	String	Specifies the enterprise project name.
checksum	String	Specifies the checksum.
created	String	Specifies the time when the cloud resource was created. The time is a UTC time in a fixed format complying with ISO-8601 (for example, **2018-11-14T08:59:14Z**).
updated	String	Specifies the last time when the cloud resource was updated. The time is a UTC time in a fixed format complying with ISO-8601 (for example, **2018-11-14T08:59:14Z**).
provisioning_state	String	Specifies the status of the operation that causes the resource change.
tags	Map	Specifies the cloud resource tag.
properties	Map	Specifies the cloud resource attribute.

Notification Example of Resource Changes

```
{
  "detail": {
    "resource": {
      "id": "3e62c0e6-e779-469e-b0f2-35743f6229d1",
      "name": "ecs-51c8",
      "provider": "evs",
      "type": "volumes",
      "checksum": "b3bcc019cecbb701e324e0dcf2f283236685885236b49f5ba5ea2f5f788170a1",
      "created": "2020-08-12T07:14:41.638Z",
      "updated": "2020-08-12T07:14:44.423Z",
      "tags": {},
      "properties": {
        "shareable": false,
        "volumeType": "SATA",
        "metadata": {},
        "attachments": [],
        "replicationStatus": "disabled",
        "availabilityZone": "regionid1a",
        "bootable": "true",
        "userId": "059b5c937d80d3e41ff3c00a3c883d16",
        "volTenantAttrTenantId": "059b5e0a2500d5552fa1c00adada8c06",
        "size": "40",
        "encrypted": false,
        "volumeImageMetadata": {
          "virtualEnvType": "FusionCompute",
          "isregistered": "true",
          "imageSourceType": "uds",
          "minDisk": "40",
          "platform": "CentOS",
          "size": 0,
          "osVersion": "CentOS 7.5 64bit",
          "minRam": "0",
          "name": "CentOS 7.5 64bit",
          "checksum": "d41d8cd98f00b204e9800998ecf8427e",
          "osBit": "64",
          "osType": "Linux",
          "containerFormat": "bare",
          "supportXen": "true",
          "id": "e0adce3a-a4d2-4207-9018-69ce64b4426a",
          "supportKvm": "true",
          "diskFormat": "zvhd2",
          "imageType": "gold"
        },
        "links": [
          {
            "rel": "self",
            "href": "https://evs.regionid1.xxxxxx.com/v2/059b5e0a2500d5552fa1c00adada8c06/os-vendor-
volumes/3e62c0e6-e779-469e-b0f2-35743f6229d1"
          },
          {
            "rel": "bookmark",
            "href": "https://evs."regionid1.xxxxxx.com/059b5e0a2500d5552fa1c00adada8c06/os-vendor-
volumes/3e62c0e6-e779-469e-b0f2-35743f6229d1"
          }
        ],
        "volHostAttrHost": ""regionid1a-pod01."regionid1#0",
        "multiattach": false,
        "status": "available"
      },
      "region_id": ""regionid1",
      "project_id": "059b5e0a2500d5552fa1c00adada8c06",
      "project_name": ""regionid1",
      "ep_id": "0",
      "ep_name": "default",
      "provisioning_state": "Succeeded"
    },
    "resource_id": "3e62c0e6-e779-469e-b0f2-35743f6229d1",
    "resource_type": "evs.volumes",
    "event_type": "CREATE",
    "capture_time": "2020-08-12T07:15:15.116Z"
  },
  "notification_type": "ResourceChanged",
  "notification_creation_time": "2020-08-12T07:14:47.192Z",
  "domain_id": "059b5c937100d3e40ff0c00a7675a0a0"
}
```

Notification Model of Resource Relationship Changes

Table 8-6 Parameter description

Parameter	Type	Description
notification_type	String	Specifies the message notification type.
notification_creation_time	String	Specifies the time when the message was sent. The time is a UTC time in a fixed format complying with ISO-8601 (for example, **2018-11-14T08:59:14Z**).
domain_id	String	Account ID
detail	Object	Specifies the message details.

Table 8-7 detail parameters

Parameter	Type	Description
resource_id	String	Specifies the resource ID.
resource_type	String	Specifies the resource type.
event_type	Enum	Specifies the event type (**CHANGE**).
capture_time	String	Specifies the time when the event was captured. The time is a UTC time in a fixed format complying with ISO-8601 (for example, **2018-11-14T08:59:14Z**).

Notification Example of Resource Relationship Changes

```
{
  "detail": {
    "resource_id": "f65b06d1-d63b-438a-93cc-bdd55b304f0a",
    "resource_type": "ecs.cloudservers",
    "event_type": "CHANGE",
    "capture_time": "2020-08-12T07:15:14.257Z"
  },
  "notification_type": "ResourceRelationChanged",
  "notification_creation_time": "2020-08-12T07:14:56.296Z",
  "domain_id": "059b5c937100d3e40ff0c00a7675a0a0"
}
```

Notification Model of Resource Snapshot Storage Completed

Table 8-8 Parameter description

Parameter	Type	Description
notification_type	String	Specifies the message notification type.
notification_creation_time	String	Specifies the time when the message was sent. The time is a UTC time in a fixed format complying with ISO-8601 (for example, **2018-11-14T08:59:14Z**).
domain_id	String	Specifies the tenant ID.
detail	Object	Specifies the message details.

Table 8-9 detail parameters

Parameter	Type	Description
snapshot_id	String	Specifies the resource snapshot ID.
region_id	String	Specifies the ID of the region where the resource snapshot is located.
bucket_name	String	Specifies the name of the OBS bucket where the resource snapshot is stored.
object_keys	Array of String	Specifies the resource snapshot path list.

Notification Example of Resource Snapshot Storage Completed

```
{
  "detail": {
    "snapshot_id": "474f85e6-72cd-442b-af4e-517120a5c669",
    "region_id": ""regionid1",
    "bucket_name": "test",
    "object_keys": [
      "RMSLogs/059b5c937100d3e40ff0c00a7675a0a0/Snapshot/2020/8/11/059b5c937100d3e40ff0c00a7675a0a0_Snapshot_"regionid1_ResourceSnapshot_2020-08-10T170901_474f85e6-72cd-442b-af4e-517120a5c669_part-1.json.gz"
    ]
  },
  "notification_type": "SnapshotArchiveCompleted",
  "notification_creation_time": "2020-08-10T17:09:27.314Z",
  "domain_id": "059b5c937100d3e40ff0c00a7675a0a0"
}
```

Notification Model of Resource Change Notification Storage Completed

Table 8-10 Parameter description

Parameter	Type	Description
notification_type	String	Specifies the message notification type.
notification_creation_time	String	Specifies the time when the message was sent. The time is a UTC time in a fixed format complying with ISO-8601 (for example, **2018-11-14T08:59:14Z**).
domain_id	String	Account ID
detail	Object	Specifies the message details.

Table 8-11 detail parameters

Parameter	Type	Description
region_id	String	Specifies the ID of the region where the resource snapshot is located.
bucket_name	String	Specifies the name of the OBS bucket where the resource snapshot is stored.
object_key	String	Specifies the resource snapshot path.

Notification Example of Resource Change Notification Storage Completed

```
{
    "detail": {
        "region_id": ""regionid1",
        "bucket_name": "test",
        "object_key": "RMSLogs/059b5c937100d3e40ff0c00a7675a0a0/Notification/2020/12/10/
NotificationChunk/
059b5c937100d3e40ff0c00a7675a0a0_Notification_"regionid2_NotificationChunk_VPC_VPCS_2020-12-10T02
4612Z_2020-12-10T050621Z.json.gz"
    },
    "notification_type": "NotificationArchiveCompleted",
    "notification_creation_time": "2020-12-10T05:09:28.002Z",
    "domain_id": "059b5c937100d3e40ff0c00a7675a0a0"
}
```

8.5 Resource Storage Models

Table 8-12 Parameter description

Parameter	Type	Description
snapshot_id	String	Specifies the resource snapshot ID.
items	Array of Object	Specifies the list of the resource snapshot items.
snapshot_time	String	Specifies the time when the resource snapshot was stored. **snapshot_time** is a UTC time in a fixed format complying with ISO-8601 (for example, **2018-11-14T08:59:14Z**).

Table 8-13 Resource snapshot items

Parameter	Type	Description
resource	Object	Specifies the resource.
relations	Array of Object	Specifies the item list of the resource relationship.

Table 8-14 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.

Parameter	Type	Description
ep_name	String	Specifies the enterprise project name.
checksum	String	Specifies the checksum.
created	String	Specifies the time when the cloud resource was created. **created** is a UTC time in a fixed format complying with ISO-8601 (for example, **2018-11-14T08:59:14Z**).
updated	String	Specifies the last time when the cloud resource was updated. **updated** is a UTC time in a fixed format complying with ISO-8601 (for example, **2018-11-14T08:59:14Z**).
provisioning_state	String	Specifies the result of an operation on resources. The value can be: ● Succeeded: The operation is successful. ● Failed: The operation fails. ● Canceled: The operation is canceled. ● Processing: The operation is in progress.
tags	Map	Specifies the cloud resource tag.
properties	Map	Specifies the cloud resource attribute.

Table 8-15 Resource relationship items

Parameter	Type	Description
from_resource_id	String	Specifies the ID of the source resource.
to_resource_id	String	Specifies the ID of the associated resource.
from_resource_type	String	Specifies the type of the source resource.

Parameter	Type	Description
to_resource_type	String	Specifies the type of the associated resource.
relation_type	String	Specifies the resource relationship type.

Resource Storage Example

```
{
  "items": [
    {
      "resource": {
        "id": "c25ee8b3-c907-4cd4-9869-6c4b07c61a0b",
        "name": "rse-cdk-07-cdk-3sbz",
        "provider": "vpc",
        "type": "securityGroups",
        "region_id": ""regionid1",
        "project_id": "fc6d40abe7e54492b7c7aa5a29d6cbab",
        "project_name": "demo_project",
        "ep_id": "0",
        "ep_name": "default",
        "checksum": "4098715092c762b3eafe25be8eeda33a10b547033f9d59b6e18f5a960a1f805d",
        "updated": "2020-05-25T10:27:17.000Z",
        "created": "2020-05-25T10:27:17.000Z",
        "provisioning_state": "Succeeded",
        "tags": {},
        "properties": {}
      },
      "relations": [
        {
          "from_resource_id": "c25ee8b3-c907-4cd4-9869-6c4b07c61a0b",
          "to_resource_id": "0088a276-162b-4f07-aa40-f6ed8b801ca1",
          "from_resource_type": "vpc.securityGroups",
          "to_resource_type": "ecs.cloudservers",
          "relation_type": "isAssociatedWith"
        }
      ]
    }
  ],
  "snapshot_id": "6e40483d-5499-4440-a369-284e528f3d85",
  "snapshot_time": "2020-06-30T06:56:00.018Z"
}
```

8.6 Models of Resource Change Notification Storage

Table 8-16 Parameter description

Parameter	Type	Description
notification_items	Array of Object	Specifies the list of resource change notifications.

Notification Model of Resource Changes

Table 8-17 Parameter description

Parameter	Type	Description
notification_type	String	Specifies the message notification type.
notification_creation_time	String	Specifies the time when the message was sent. The time is a UTC time in a fixed format complying with ISO-8601 (for example, **2018-11-14T08:59:14Z**).
domain_id	String	Account ID
detail	Object	Specifies the message details.

Table 8-18 detail parameters

Parameter	Type	Description
resource_id	String	Specifies the resource ID.
resource_type	String	Specifies the resource type.
event_type	Enum	Specifies the event type. The value can be **CREATE**, **UPDATE**, or **DELETE**.
capture_time	String	Specifies the time when the event was captured. The time is a UTC time in a fixed format complying with ISO-8601 (for example, **2018-11-14T08:59:14Z**).
resource	Object	Specifies the resource details.

Table 8-19 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.

Parameter	Type	Description
region_id	String	Specifies the ID of the region where the resource is located.
project_id	String	Specifies the IAM project ID.
project_name	String	Specifies the IAM project name.
ep_id	String	Specifies the enterprise project ID.
ep_name	String	Specifies the enterprise project name.
checksum	String	Specifies the checksum.
created	String	Specifies the time when the cloud resource was created. The time is a UTC time in a fixed format complying with ISO-8601 (for example, **2018-11-14T08:59:14Z**).
updated	String	Specifies the last time when the cloud resource was updated. The time is a UTC time in a fixed format complying with ISO-8601 (for example, **2018-11-14T08:59:14Z**).
provisioning_state	String	Specifies the status of the operation that causes the resource change.
tags	Map	Specifies the cloud resource tag.
properties	Map	Specifies the cloud resource attribute.

Example of Resource Change Notification Storage

```
{
    "notification_items": [
        {
            "detail": {
                "resource": {
                    "id": "ea05ef41-8bd6-4a9c-af39-244e1ec448eb",
                    "name": "as-group-test",
                    "provider": "as",
                    "type": "scalingGroups",
                    "checksum": "",
                    "region_id": ""regionid1",
                    "project_id": "068d54ceca00d5302f70c00aaf6a471c",
                    "project_name": "test",
                    "ep_id": "0",
                    "ep_name": "default"
                },
                "resource_id": "ea05ef41-8bd6-4a9c-af39-244e1ec448eb",
        "resource_type": "as.scalingGroups",
        "event_type": "DELETE",
        "capture_time": "2020-12-08T09:30:27.158Z"
      },
      "notification_type": "ResourceChanged",
      "notification_creation_time": "2020-12-08T09:30:27.272Z",
      "domain_id": "059b5c937100d3e40ff0c00a7675a0a0"
    }
  ]
}
```

8.7 DSL Syntax

DSL consists of a logical operator shown as shown below. A Boolean value is returned.

```
{
 <logical operator>: <condition> | [<condition>, ..., <condition>]
}
```

8.7.1 Logical Operators

Supported logical operators are:

- "not": <condition>
- "allOf": [<condition>, ..., <condition>]
- "anyOf": [<condition>, ..., <condition>]

not inverts the result of the condition.

allOf evaluates true only if all included conditions are true, and evaluates false as long as one included condition is false.

anyOf evaluates true as long as one included condition is true, and evaluates false if all included conditions are false.

allOf and **anyOf** both implement short-circuit evaluation. They evaluate the conditions in the subsequent list in sequence.

If the return result of a condition is false, **allOf** returns false and the subsequent conditions are not calculated.

If the return result of a condition is true, **anyOf** returns true and the subsequent conditions are not calculated.

8.7.2 Conditions

A condition can be a single judgment statement or a nested logical operator.

The judgment statement is used to determine whether a specific value meets a specific requirement. It returns a Boolean value and its format is as follows:

```
{
 "value": "...",
 "comparator": "...",
 "pattern": "..."
}
```

NOTE

- **value** can be a constant or an expression. Its value type depends on the selected comparison operator. Example: **true**, **1**, **"hello"**, or **"${resource().properties.metadata}"**
- **comparator**: specifies the comparison operator.
- **pattern** can be a constant or an expression.

The following comparators are supported:

- **equals** compares whether **value** is equal to **pattern**. **value** can be a string, an integer, or a Boolean, so is **pattern**.
- **notEquals**: Its result is opposite to the **equals** result.
- **equalsIgnoreCase** compares whether **value** is equal to **pattern** in case-insensitive mode. **value** must be a string, so is **pattern**.
- **like** performs fuzzy match of **value** and **pattern**. You can add an asterisk (*) to **pattern** to match zero or multiple random characters, or add a question mark (?) to **pattern** to match any random character. **value** must be a string, so is **pattern**.
- **notLike**: Its result is opposite to the **like** result.
- **likeIgnoreCase** performs fuzzy match of **value** and **pattern** in case-insensitive mode. **value** must be a string, so is **pattern**.
- **contains** determines whether **pattern** is a substring of **value**. **value** must be a string, so is **pattern**.
- **notContains**: Its result is opposite to the **contains** result.
- **in** determines whether **value** is in **pattern**. **Pattern** must be an array. **value** can be a string or an integer.
- **notIn**: Its result is opposite to the **in** result.
- **containsKey** determines whether **value** contains the key-value pattern. **value** must be an object. **pattern** must be a string.
- **notContainsKey**: Its result is opposite to the **containsKey** result.
- **less** determines whether **value** is smaller than **pattern**. **value** can be a string or an integer, so is **pattern**.
- **lessOrEquals** determines whether **value** is smaller than or equal to **pattern**. **value** can be a string or an integer, so is **pattern**.
- **greater** determines whether **value** is greater than **pattern**. **value** can be a string or an integer, so is **pattern**.
- **greaterOrEquals** determines whether **value** is greater than or equal to **pattern**. **value** can be a string or an integer, so is **pattern**.

The following is an example of nested logical operators in a condition:

```
{
  "not": {
    "anyOf": [
      {
        "value": "${resource().properties.metadata}",
        "comparator": "notContainsKey",
        "pattern": "systemEncrypted"
      },
      {
        "value": "${resource().properties.metadata.systemEncrypted}",
        "comparator": "equals",
        "pattern": "0"
      }
    ]
  }
}
```

8.7.3 Expressions

value and **pattern** can be a constant or an expression. An expression is contained in ${}. You can use the following functions in the expression.

Table 8-20 String functions

Function	Parameter	Returned Value	Description
base64()	string	string	Encodes a specific string using Base64.
base64ToString()	string	string	Decodes a Base64-encoded string.
concat()	string, string	string	Concatenates two strings.
contains()	string, string	bool	Determines whether parameter 2 is a substring of parameter 1.
empty()	string	bool	Determines whether a string is left blank.
endsWith()	string, string	bool	Determines whether parameter 1 ends with parameter 2.
indexOf()	string, string	int	Returns the position of parameter 2 when it appears for the first time in parameter 1. If parameter 2 does not appear, -1 is returned.
lastIndexOf()	string, string	int	Returns the position of parameter 2 when it appears for the last time in parameter 1. If parameter 2 does not appear, -1 is returned.
length()	string	int	Returns the length of a string.
replace()	string, string, string	string	Replaces parameter 2 in parameter 1 with parameter 3.
startsWith()	string, string	bool	Determines whether parameter 1 starts with parameter 2.
toLower()	string	string	Converts all letters in a string into lowercase letters.
toUpper()	string	string	Converts all letters in a string into uppercase letters.

Function	Parameter	Returned Value	Description
equals()	string, string	bool	Checks whether two strings are the same.
greater()	string, string	bool	Determines whether parameter 1 is greater than parameter 2.
greaterOrEquals()	string, string	bool	Determines whether parameter 1 is greater than or equal to parameter 2.
less()	string, string	bool	Determines whether parameter 1 is smaller than parameter 2.
lessOrEquals()	string, string	bool	Determines whether parameter 1 is no more than parameter 2.
split()	string, string	array	Returns the result of separating parameter 1 by parameter 2.
substring()	string, int, int	string	Obtains the substring of parameter 1. The start position of the substring is determined by parameter 2 and the length is determined by parameter 3.

Table 8-21 Numeric functions

Function	Parameter	Returned Value	Description
add()	int, int	int	Adds two integers.
max()	int, int	int	Uses the greater of the two integers.
min()	int, int	int	Uses the smaller of the two integers.
sub()	int, int	int	Calculates the result of parameter 1 minus parameter 2.
equals()	int, int	bool	Determines whether two integers are the same.
greater()	int, int	bool	Determines whether parameter 1 is greater than parameter 2.

Function	Parameter	Returned Value	Description
greaterOrEquals()	int, int	bool	Determines whether parameter 1 is greater than or equal to parameter 2.
less()	int, int	bool	Determines whether parameter 1 is smaller than parameter 2.
lessOrEquals()	int, int	bool	Determines whether parameter 1 is no more than parameter 2.

Table 8-22 Array functions

Function	Parameter	Returned Value	Description
concat()	array, array	array	Concatenates two arrays.
contains()	array, any	bool	Determines whether parameter 2 is in array parameter 1.
empty()	array	bool	Determines whether the array is left blank.
first()	array	any	Returns the first element in the array.
last()	array	any	Returns the last element in the array.
length()	array	int	Returns the number of elements in the array.

Table 8-23 Object functions

Function	Parameter	Returned Value	Description
contains()	object, string	bool	Determines whether parameter 1 contains key-value parameter 2.
getValue()	object, string	any	Obtains the value corresponding to the key-value parameter 2 in parameter 1.
empty()	object	bool	Determines whether the object is left blank.
length()	object	int	Returns the number of key-value pairs in the object.

Table 8-24 Logical functions

Function	Parameter	Returned Value	Description
if()	bool, any, any	any	Determines whether parameter 1 is true. If yes, parameter 2 is returned. If no, parameter 3 is returned.
and()	bool, bool	bool	Determines whether both parameter 1 and parameter 2 are true.
or()	bool, bool	bool	Determines whether at least one of parameter 1 and parameter 2 is true.
not()	bool	bool	Inverts the input Boolean value.

Table 8-25 Functions related to resource compliance

Function	Parameter	Returned Value	Description
resource()	None	object	Returns the structure of the current evaluated resource.
parameters()	string	any	Returns a parameter defined in the **parameters** section.

In addition to use function computing in expressions, you can use:

- a dot (.) to access a field in an object, for example, **resource().properties.metadata.systemEncrypted**.
- **CASE WHEN** statement

```
CASE WHEN condition1 THEN value1
    WHEN condition2 THEN value2
    ...
    ELSE defaultValue END
```

8.8 ResourceQL Syntax

8.8.1 Overview

ResourceQL provides SQL-like functions, allowing you to flexibly query your cloud resources.

```
SELECT name, created, updated FROM resources WHERE region_id = 'regionid1'
```

The statement is case insensitive. SELECT COUNT(*) and select CoUnT(*) are the same. Use single quotation marks to represent the literal of a string.

The following are data types supported by ResourceQL. For the array type, [] is used to index a position, and the number starts from 1.

Table 8-26 Supported data types

Type Name	Type
Integer	Int/Integer
Float	Float/Double
Boolean	Boolean
Array	Array
String	String

Type Name	Type
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 8-27 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.

aggregator_resources contains **domain_id** that indicates the account ID. The type of a domain ID is a string.

provider together with **type** represents a unique resource. **properties** also varies among different resources For example, if the **provider** is **ecs**, the **properties** of **cloudservers** contains 23 fields, while the **properties** of **vpc** contains three fields.

For details about the field types supported by the properties parameter, see **Creating a Query**. The field types supported by the properties parameter are also specified on the console when you create a new query.

For a specific resource type, you can use commas (.), a nesting method, to query the specific fields in **properties**. For example, if **properties** of an ECS contains the **status** and **addresses** fields, you can run the following statement to query the running ECS and its address:

```
SELECT name, created, updated, properties.addresses FROM resources
   WHERE provider = 'ecs' AND type = 'cloudservers' AND properties.status = 'ACTIVE'
```

8.8.2 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
```

8.8.3 Functions

ResourceQL supports the following functions.

Table 8-28 Mathematical operation functions

Function	Description
abs(x)	Returns the absolute value of x.
ceil/ceiling(x)	Returns *x* rounded up to the nearest integer.
floor(x)	Returns *x* rounded down to the nearest integer.
pow/power(x, p) → double	Returns *x* raised to the power of *p*.
round(x)	Returns *x* rounded to the nearest integer.
round(x, d)	Returns *x* rounded to *d* decimal places.
sign(x)	Returns the sign of *x*. ● **1** if the argument is greater than 0 ● **-1** if the argument is less than 0

Table 8-29 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.
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 8-30 Array functions

Function	Description
all_match(array(T), function(T, boolean)) → boolean	Returns whether all elements of an array match the given predicate.
any_match(array(T), function(T, boolean)) → boolean	Returns whether any elements of an array match the given predicate.
array_average(a) → double	Returns the average of all non-null elements of *a*.
array_distinct(a) → array	Removes duplicate values from array *a*.
array_duplicates(a) → array	Returns a set of elements that occur more than once in array *a*.
array_frequency(a) → map	Returns a map: keys are the unique elements in *array*, values are how many times the key appears.
array_has_duplicates(a) → boolean	Returns a boolean: whether *a* has any elements that occur more than once.
array_intersect(a, b) → array	Returns an array of the elements in the intersection of *a* and *b*, without duplicates.
array_join(x, delimiter) → string	Concatenates the elements of the given array using the delimiter.
array_join(x, delimiter[, null_replacement]) → string	Concatenates the elements of the given array using the delimiter and an optional string to replace nulls.
array_max/array_min(a)	Returns the maximum or minimum value of input array *a*.
array_position(a, element) → int	Returns the position of the first occurrence of the *element* in array *a* (or 0 if not found).
array_position(a, element, instance) → int	Returns the position of the first occurrence of the *element* in array *a*. If no matching element instance is found, **0** is returned. If *instance* > 0, returns the position of the *instance*-th occurrence of the *element* in array *a*. If *instance* < 0, return the position of the *instance*-to-last occurrence of the *element* in array *a*.
array_remove(a, element) → array	Removes all elements that equal *element* from array *a*.

Function	Description
array_sort(a) → array	Sorts and returns array *a*.
array_sort(array(T), function(<T, T>, int)) → array	Sorts and returns the *array* based on the given comparator *function*. The comparator will take two nullable arguments representing two nullable elements of the *array*. It returns **-1**, **0**, or **1** as the first nullable element is less than, equal to, or greater than the second nullable element.
array_sum(a)	Returns the sum of all non-null elements of *a*.
array_overlap(a, b) → boolean	Tests if arrays *a* and *b* have any non-null elements in common.
array_union(a, b) → array	Returns an array of the elements in the union of *a* and *b*, without duplicates.
array_except(x, y) → array	Returns an array of elements in **x** but not in **y**.
cardinality(a) → int	Returns the cardinality (size) of array *a*.
concat(a1, a2, ...) → array	Concatenates the arrays *a1*, *a2*, ... This function provides the same functionality as the SQL-standard concatenation operator (||).
contains(a, element) → boolean	Returns true if the array *a* contains the *element*.
element_at(a, index)	Returns element of *a* at given *index*. If *index* < 0, element_at accesses elements from the last to the first.
filter(array(T), function(T, boolean)) → array(T)	Constructs an array from those elements of *array* for which *function* returns true.
none_match(array(T), function(T, boolean)) → boolean	Returns whether no elements of an array match the given predicate.
reverse(a) → array	Returns an array which has the reversed order of array *a*.

Function	Description
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 8-31 Aggregate functions

Function	Description
arbitrary(x)	Returns an arbitrary non-null value of *x*, if one exists.
array_agg(x) → array	Returns an array created from the input *x* elements.
avg(x)→ double	Returns the average (arithmetic mean) of all input values.
bool_and/bool_or(x) → boolean	**bool_and** returns **TRUE** if every input value is **TRUE**, otherwise **FALSE**. **bool_or** returns **TRUE** if any input value is **TRUE**, otherwise **FALSE**.
coalesce(value1, value2, ...)	Returns the first non-null value in an argument list. Short-circuit evaluation will be used.
count(*)/count(x) → int	**count(*)** returns the number of input rows. **count(x)** returns the number of non-null input values.
greatest(value1, value2, ..., valueN)	Returns the largest of the provided values.
histogram(x) → map	Returns a map containing the count of the number of times each input value occurs.

Function	Description
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 8-32 Time functions

Function	Description
now() → date	Returns the current time.
date_diff(unit, timestamp1, timestamp2) → int	Returns timestamp2-timestamp1 expressed in terms of unit. The option of unit can be millisecond, second, minute, hour, day, week, month, quarter, or year.
date_parse(string, format) → timestamp	Parses a string into a timestamp using **format**.

9 Change History

Released On	Description
2023-12-30	This issue is the seventeenth official release, which incorporates the following change: Optimized **Predefined Policies**.
2023-11-24	This issue is the sixteenth official release. which incorporates the following changes: ● Added **Organization Conformance Packages**. ● Added the content in **Cross-Account Authorization** to explain that an encrypted OBS bucket can be specified when the resource recorder is configured.
2023-10-25	This issue is the fifteenth official release, Added the new feature **Conformance Packages**. A conformance package is a collection of rules. Config provides you with conformance packages to centrally create and manage rules, and query compliance data.
2023-10-11	This is the fourteenth official release. The following content is added: ● **Viewing Resource Compliance Data** ● **Viewing Noncompliant Resources**
2023-06-07	This issue is the thirteenth official release, which incorporates the following change: Changed the service name from Resource Management Service (RMS) to Config.

Copyright © Huawei Technologies Co., Ltd.

Released On	Description
2023-04-20	This issue is the twelfth official release, which incorporates the following changes: ● Added **Organization Rules**. ● Added **Viewing Aggregated Rules**. ● Added **Advanced Queries**.
2023-03-30	This issue is the eleventh official release, which incorporates the following changes: ● Added **Resource Aggregation**. ● The **My Resources** feature is renamed **Resource List**.
2023-02-17	This issue is the tenth official release, which incorporates the following change: Added **Event Monitoring**.
2022-12-30	This issue is the ninth official release, which incorporates the following changes: ● Added **Adding a Custom Rule**. ● Added **Example Functions (Python)**. ● Added **Events**.
2022-08-24	This issue is the eighth official release, which incorporates the following change: Added **Cross-account authorization**: Permissions on SMN topics and OBS buckets can be granted across accounts during resource recorder configuration.
2022-04-06	This issue is the seventh official release, which incorporates the following changes: ● Added **Advanced Queries**. ● Added **ResourceQL Syntax**.
2021-09-09	This issue is the sixth official release. Added **Why Can't I Delete Resources on the Resource List Page?**.
2021-07-16	This issue is the fifth official release, which incorporates the following change: Changed **Management & Deployment** to **Management & Governance** and **Computing** to **Compute** based on changes in the console product catalog.

Released On	Description
2020-12-28	This issue is the fourth official release, which added the following sections: ● **Cloud Trace Service** ● **Supported CTS Operations** ● **Querying Real-Time Traces**
2020-12-16	This issue is the third official release. Added **FAQs**.
2020-12-14	This issue is the second official release, which added the following sections: ● **Storing Resource Change Notifications** ● **Notification Model of Resource Change Notification Storage Completed** ● **Models of Resource Change Notification Storage**
2020-11-30	This issue is the first official release. ● **Resource List** : You can view, filter, and export resources. You can also view resource relationships and resource history. ● **Resource Recorder**: You can enable, configure, and modify the resource recorder. ● **Resource Compliance**: You can add, trigger, and modify rules.