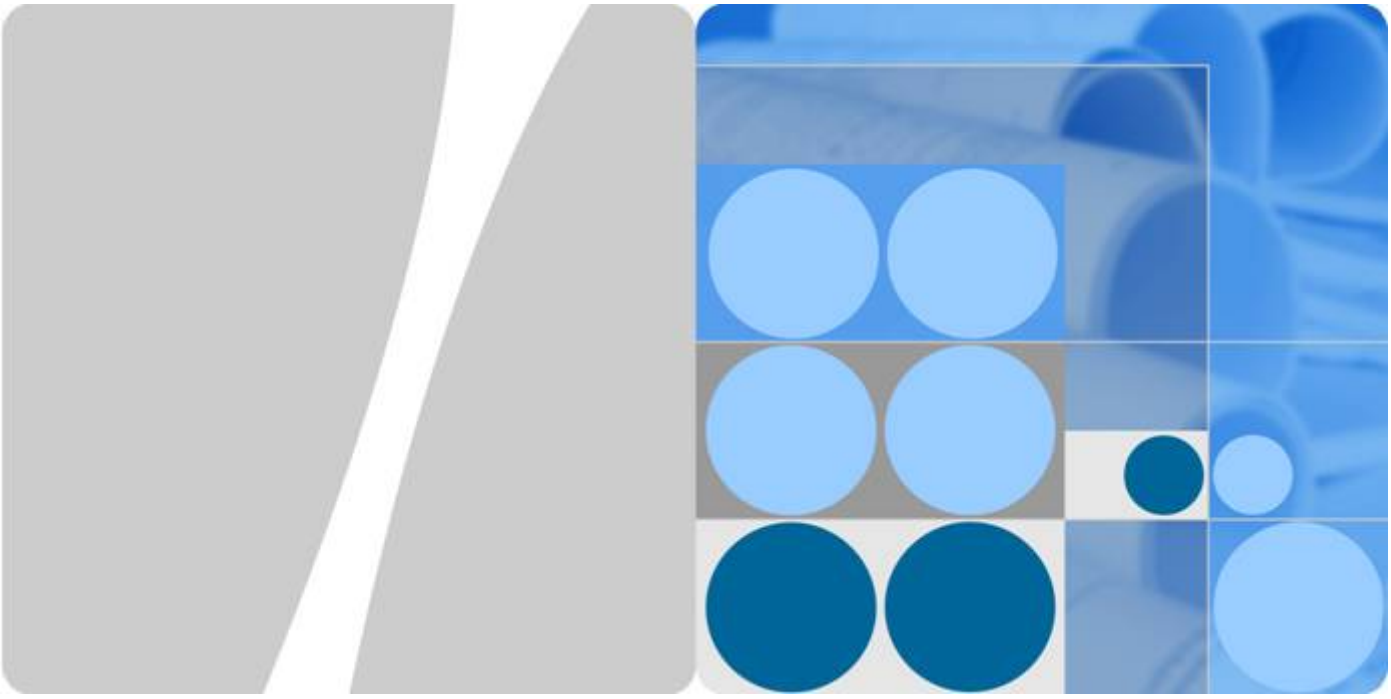


Config

User Guide

Date 2024-10-30

Contents

1 Service Overview

1.1 What Is Config?

Description

Config allows you to search for, record, and continuously evaluate your resource configurations to make sure that your resources are in expected status.

NOTICE

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

Architecture

Config provides you with resource information, such as resource inventory, details, relationships, and change records. It stores your resource data every 24 hours and notifications of your resource changes every 6 hours. It will also notify you when a change is made to your resources. In addition, it enables you to use Config rules to evaluate your resources.

- **Viewing resource details**: You can set multiple search options to query your resources on Config console.
- **Viewing resource relationships**: You can view relationships between resources on Config console.
- **Viewing resource change records**: You can enable and configure the resource recorder to continuously monitor resource changes.
- **Sending notifications**: Config will notify you when a change is made to your resources after you have enabled the resource recorder and configured a Simple Message Notification (SMN) topic.
- **Storing resource change notifications**: Config will store your resource change notifications every 6 hours after you have enabled the resource

recorder and configured an SMN topic and an Object Storage Bucket (OBS) bucket.

- **Storing resource snapshots**: Config will store your resource snapshots into the specified OBS bucket every 24 hours after you have enabled the resource recorder and configured an OBS bucket.
- **Evaluating resource compliance**: Config evaluates your resources using rules to check whether they are compliant or not.
- **Advanced query**: Allows you to customize queries with ResourceQL to search for your resources.
- **Resource aggregator**: 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 resource data.
- **Conformance package**: A conformance package is a collection of rules. You can use conformance packages to centrally create and manage rules, and query compliance data.

Access Methods

You can use either of the following methods to access Config.

- **Management Console**

  The console is a web-based UI, where you can perform operations easily. Log in to the management console, click  in the upper left corner, and choose **Management & Deployment** > **Config**.
- **Application Programming Interfaces (APIs)**

  To integrate Config into a third-party system for secondary development, you need to access the service by calling APIs. For details, see *Config API Reference*.

1.2 Function Overview

Table 1-1 lists common functions of Config.

To better understand Config functions, you can learn **basic concepts** first.

Table 1-1 Common functions

Category	Function	Description
Resource list	Querying all resources	You can view all resource information, including the resource name, region, service, resource type, and enterprise project, from the current account.
	Querying details about a resource	You can query resource details, such as the resource name, creation time, and specifications.

Category	Function	Description
	Filtering resources	You can set a filter criterion (resource name, resource ID, tag, or enterprise project) to quickly find out specific resources.
	Exporting resource information	You can export the information about required resources in an EXCEL file.
	Viewing resource compliance data	You can view compliance data of a resource.
	Viewing relationships of a resource	You can view relationships of a resource.
	Viewing change records of a resource	You can view change records of a resource.
Resource compliance	Adding a rule	You can add a rule to evaluate resource compliance. To add a rule, you need to set a policy and other related parameters.
	Evaluating resources	You can click **Evaluate** in the **Operation** column for a rule to evaluate the resources that are within the monitoring scope of the rule.
	Disabling a rule	You click **Disable** in the **Operation** column to disable a rule.
	Enabling a rule	If you want to use a disabled rule, you can enable it.
	Modifying a rule	If a rule does not meet your needs, you can change its configurations as needed.
	Deleting a rule	You can delete a rule which is no longer needed.
	Noncompliant resources	You can view and export noncompliant resources.
Resource recorder	Enabling the resource recorder	You can track resource changes only after the resource recorder is enabled.

Category	Function	Description
	Configuring the resource recorder	You can set the monitoring scope, select an SMN topic, and configure the data storage path (OBS bucket). Then you need to grant permissions to the resource recorder for using SMN to send notifications and storing resource snapshots in the OBS bucket.
	Modifying the resource recorder	You can modify resource recorder configurations, such as the monitoring scope, resource dump, data retention period, SMN topic, and permissions.
	Disabling the resource recorder	You can disable the resource recorder at any time.
Advanced Queries	Running an advanced query	You can use ResourceQL to query current configurations of your resources.
	Creating a query	You can add custom queries, so that you can directly run them later.
	Viewing a query	You can view the name, description, and SQL statement of a query.
	Modifying a query	If a custom query cannot meet your requirements, you can modify its name, description, and query statement.
	Deleting a query	If a custom query is no longer needed, you can delete it.
Resource Aggregation	Creating a resource aggregator	You can use resource aggregators to aggregate resource configurations and compliance data from multiple accounts or an organization.
	Viewing resource aggregators	You can view created resource aggregators and their details.
	Editing a resource aggregator	You can edit source accounts in a resource aggregator.
	Deleting a resource aggregator	If a resource aggregator is no longer used, you can delete it.
	Viewing aggregated rules	You can view all aggregated rules and their conformance data.

Category	Function	Description
	Viewing aggregated resources	You can view all resources aggregated by the resource aggregator.
	Authorizing an aggregator account	An aggregator account needs authorization from source accounts to collect resource configuration and compliance data from these accounts
	Applying advanced queries to aggregators	Resource aggregation supports advanced queries. You can use ResourceQL to query configuration states of resources from one or more source accounts.
Conformance package	Creating conformance packages	You can use example or custom templates to create and manage rules.
	Viewing conformance packages	You can view the conformance package list and details of each conformance package.
	Deleting conformance packages	You can delete conformance packages as needed. Rules included in a conformance package will be deleted automatically if the conformance package is deleted.
	Organization conformance packages	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.
CTS	Supported CTS operations	CTS records operations on Config for later query, audit, and backtrack.
	Viewing tracing logs	You can view or export Config operation records of the last seven days on CTS console.

1.3 Permissions

If you need to assign different permissions to employees in your enterprise, Identity and Access Management (IAM) is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you flexibly manage resource access.

You can create users using IAM and grant users permissions to implement access control. For example, if you want some of your employees to have the permissions for configuring the resource recorder, you can create IAM users for them and grant them with the required permissions.

If your account does not need individual IAM users for permissions management, skip this chapter.

Config Permissions

By default, new IAM users do not have permissions. You need to add a user to one or more groups and attach policies or roles to the user groups. Users in a group inherit permissions from the group, so that they can perform operations on cloud services based on the permissions.

Config is a global service. You do not need to repeat Config authorization for different regions or switch regions for accessing Config.

A user with Config read-only permissions can view all resources on the **Resource List** page.

You can grant permissions by using roles or policies.

- Roles: A coarse-grained authorization strategy that defines permissions by job responsibility. Only a limited number of service-level roles are available for authorization. When using roles to grant permissions, you must also assign other roles which the permissions depend on to take effect. However, roles are not an ideal choice for fine-grained authorization and secure access control.
- Policy: A type of fine-grained authorization method that defines permissions required to perform operations on specific cloud resources under certain conditions. Authorization using policies is more flexible and help you implement least privilege. Most policies define permissions based on APIs. API actions are the minimum granularity of permissions. For API actions supported by Config, see the **Permissions Policies and Supported Actions** section in *Config API Reference*.

Table 1-2 lists all the system-defined permissions supported by Config.

Table 1-2 System-defined permissions supported by Config.

Policy	Description	Dependencies
RMS ConsoleFullAccess	Grants full access to Config console. This policy grants you the permissions to perform all actions on the resource list, resource recorder, resource compliance, advanced queries, aggregators, and conformance packages.	RF FullAccess
RMS FullAccess	Grants full access to Config. This policy grants you the permissions to perform all actions on the resource list, resource recorder, resource compliance, advanced queries, aggregators, and conformance packages.	RF FullAccess

Policy	Description	Dependencies
RMS ReadOnlyAccess	Grants read-only access to Config. This policy grants you read access to the resource list, resource recorder, resource compliance, advanced queries, aggregators, and conformance packages.	None

NOTE

An IAM user or IAM Identity Center user may still be denied specific operations on resource recorders, rules, or conformance packages even if they have been granted the **RMS ConsoleFullAccess** permission. This is because specific operations require IAM agencies. To perform these operations, you need related IAM agencies. The following lists the details.

To create IAM agencies, you need the **iam:agencies:createAgency** and **iam:permissions:grantRoleToAgency** permissions. To grant the permission **iam:permissions:grantRoleToAgency**, specific actions need to be specified.

Table 1-3 lists the common operations and the system-defined permissions of Config. √ indicates that an operation is supported, and × indicates not supported.

Table 1-3 Common operations supported by system-defined permissions

Operation	RMS ConsoleFullAccess	RMS FullAccess	RMS ReadOnlyAccess
Querying all resources	√	√	√
Query details about a resource.	√	√	√
Filtering resources	√	√	√
Exporting resources	√	√	√
Viewing resource compliance data	√	√	√
Viewing relationships of a resource	√	√	√
Viewing resource change history	√	√	√
Querying the resource recorder	√	√	√

Operation	RMS ConsoleFullAccess	RMS FullAccess	RMS ReadOnlyAccess
Enabling, configuring, or modifying the resource recorder	√	√	x
Disabling the resource recorder	√	√	x
Querying a compliance policy	√	√	√
Modifying rules	√	√	x
Adding rules	√	√	x
Querying rules	√	√	√
Deleting rules	√	√	x
Creating organization rules	√	√	x
Modifying organization rules	√	√	x
Viewing organization rules	√	√	√
Deleting organization rules	√	√	x
Viewing resource compliance evaluation results	√	√	√
Triggering a resource compliance evaluation	√	√	x
Updating compliance evaluation results	√	√	x
Creating advanced queries	√	√	x
Querying advanced queries	√	√	√
Listing advanced queries	√	√	√

Operation	RMS ConsoleFullAccess	RMS FullAccess	RMS ReadOnlyAccess
Updating advanced queries	√	√	x
Deleting advanced queries	√	√	x
Creating a resource aggregator	√	√	x
Viewing a resource aggregator	√	√	√
Modifying a resource aggregator	√	√	x
Deleting a resource aggregator	√	√	x
Viewing aggregated rules	√	√	√
Viewing aggregated resources	√	√	√
Authorizing a resource aggregator account	√	√	x
Deleting authorization for an aggregator account	√	√	x
Deleting resource aggregation requests	√	√	x
Viewing resource aggregation requests	√	√	√
Running advanced queries to aggregators	√	√	x

Operation	RMS ConsoleFullAccess	RMS FullAccess	RMS ReadOnlyAccess
Viewing an authorization list	√	√	√
Creating conformance packages	√ (depends on RF FullAccess)	√ (depends on RF FullAccess)	x
Viewing conformance packages	√	√	√
Listing conformance packages	√	√	√
Deleting conformance packages	√ (depends on RF FullAccess)	√ (depends on RF FullAccess)	x
Updating conformance packages	√ (depends on RF FullAccess)	√ (depends on RF FullAccess)	x
Listing conformance package sample templates	√	√	√
Creating organization conformance packages	√	√	x
Viewing organization conformance packages	√	√	√
Listing organization conformance packages	√	√	√
Deleting organization conformance packages	√	√	x
Updating organization conformance packages	√	√	x

1.4 Basic Concepts

Resource

A resource is an entity that you can use on the cloud platform. A resource can be an Elastic Cloud Server (ECS), an Elastic Volume Service (EVS) disk, or a Virtual Private Cloud (VPC).

Resource Relationship

Resource relationships indicate how your cloud resources are associated. For example, a resource relationship can be described as an EVS disk attached to a cloud server or a cloud server deployed in a VPC.

Resource Change Records

Resource change records contain resource changes in a specific period of time.

A record will be generated if there is a change to resource relationships or attributes.

Resource attributes are key and value pairs that describe the characteristics of your resources. For example, a resource attribute can be the number of CPU cores of an ECS, the capacity of an EVS disk, or the password strength of an IAM user.

Resource Recorder

The resource recorder tracks changes to your cloud resources that are supported by Config. What changes are tracked depends on what a service reports to Config.

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

Resource Compliance

You can create rules to evaluate the compliance of your resources. You can view and export information of your noncompliant resources.

Advanced Query

The advanced query allows you to quickly query specific resources, helping you obtain resource details, analyze resources from multiple perspectives, and quickly export data reports.

Resource Aggregator

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 resource data.

Conformance Package

A conformance package is a collection of rules. Conformance packages allow you to centrally create and manage rules for compliance data query.

1.5 Relationships with Other Services

The following describes the relationships between Config and other services.

Table 1-4 Relationships between Config and other services

Service	Description	Function
SMN	You can specify an SMN topic when you enable the resource recorder. **NOTE** If you have configured an OBS bucket and you do not need notifications for resource changes, you do not need to configure an SMN topic.	You will receive a notification if a change is made to your resource.
OBS	You can specify an OBS bucket when you enable the resource recorder. **NOTE** If you have configured an SMN topic and you do not need an OBS bucket for resource dump, you do not need to configure an OBS bucket.	• The resource recorder stores resource change notifications into your specified OBS bucket every 6 hours (an SMN topic also needs to be specified). • The resource recorder stores your resource snapshots into the OBS bucket every 24 hours.

Service	Description	Function
IAM	• You need to assign Config related permissions when you configure the resource recorder. • You can use IAM to control users' access to Config.	• **Quick granting** automatically assigns Config the permissions to send notifications using the specified SMN topic and to write data into the specified OBS bucket. You can also choose **Custom granting** to modify the permission scope. • You can assign users system-defined or custom policies to decide which operations they can perform on Config.
CTS	CTS records operations on Config.	CTS helps you record operations on Config for later query, audit, and backtrack.
Resource Formation Service (RFS)	-	Conformance packages are created with RFS stacks. You cannot separately delete rules of a conformance package created with RFS stacks.

1.6 Constraints and Limitations

The constraints on Config are as follows:

Table 1-5 Constraints and limitations on Config

Description	Limit
Resource data synchronization period **NOTE** There is a delay in synchronizing resource data to Config. The delay varies depending on services. If the resource recorder is enabled, Config will update related data for resources that are included in the monitoring scope within 24 hours. If the resource recorder is disabled, Config will not update resource data.	24 hours
Retention duration of resource snapshots	24 hours
Retention duration of resource change notifications	6 hours

Description	Limit
Maximum number of rules (including organization rules) in an account	500
Maximum number of conformance packages (including organization conformance packages) in an account	50
Maximum number of resource aggregators (account specific) in an account	30
Maximum number of accounts a resource aggregator can collect.	30
Maximum number of accounts can be added, updated, or deleted in an account every seven days	1,000
Maximum number of resource aggregators (organization specific) in an account	1
Maximum number of times you can create resource aggregators (organization specific) for an account per day	One time
Maximum number of advanced queries in an account	200
Number of results returned for each advanced query	4,000
The default retention period for resource configurations	7 years (2,557 days)

NOTICE

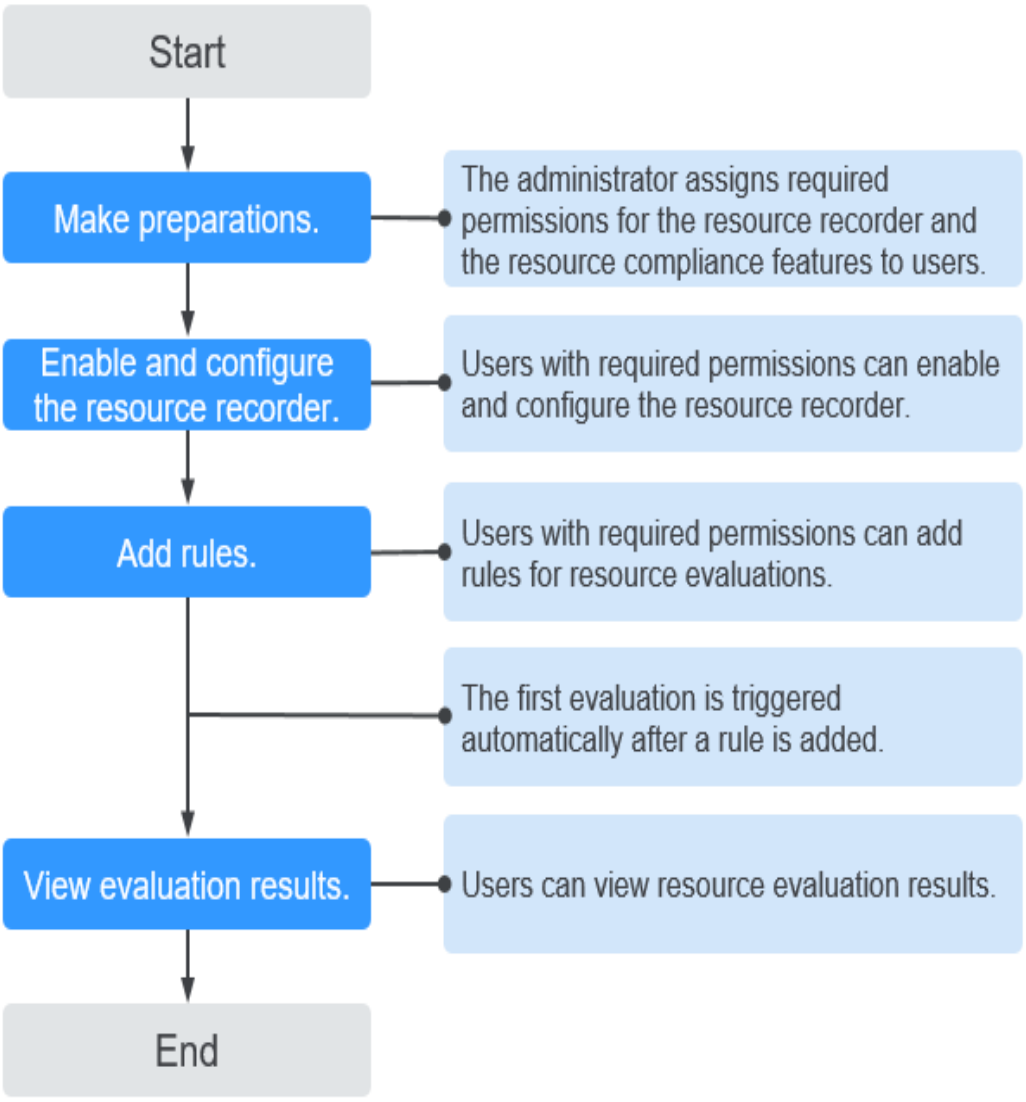
To get full functionality of Config, you need to enable the resource recorder. If the resource recorder is disabled, you may fail to update your resource data, create and use rules, or to aggregate resource data.

2 Getting Started

If you are new to Config, this section will help you quickly get familiar with main functions of this service. For more details about Config constraints, see **Constraints and Limitations**.

The following flowchart shows the operation process.

Figure 2-1 Getting started flowchart



Enabling the Resource Recorder

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

Step 1 Log in to the management console.

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

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

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

Step 5 Select the monitoring scope.

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

NOTE

The resource recorder is default to record all resources of Config.

Step 6 Specify an OBS bucket.

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

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

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

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

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

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

NOTE

After you specify an OBS bucket from the current or another account, Config will write an empty file named **ConfigWritabilityCheckFile** to the OBS bucket to verify whether resources can be written to the OBS bucket. If an error is reported, you can address the error based on **Why Is an Error Reported When Data Is Dumped to the OBS Bucket After the Resource Recorder Is Enabled?**.

Step 7 Specify a data retention period.

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

NOTE

The data retention period only applies to resource 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.

Step 8 (Optional) Configure an SMN topic.

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

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

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

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

Step 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 for writing data into an OBS bucket. The agency created by **quick granting** doesn't contain KMS permissions, so the resource recorder is unable to store resource change notifications and snapshots to an OBS bucket that is encrypted using KMS. If you need to use an encrypted bucket, you can add required permissions 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 Config. The agency must include either the permissions for sending notifications using an SMN topic or the permissions for writing data into an OBS bucket. To store resource changes and snapshots to an OBS bucket that is encrypted using KMS, you need the required permissions. For details, see **Storing Resource Change Notifications and Resource Snapshots to an Encrypted OBS Bucket**. For details about how to create an agency, see *Identity and Access Management User Guide*.

Step 10 Click **Save**.

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

----End

Adding a Rule

To create, modify, enable, or trigger a rule, the resource recorder must be enabled. If the resource recorder is disabled, you can only view, disable, and delete rules.

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

Step 2 Configure basic details, and click **Next**.

Table 2-1 Parameters of basic configurations

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

Parameter	Description
Rule Name	By default, the rule name is consistent with the predefined policy name. Rule names must be unique. A rule name can contain digits, letters, underscores (_), and hyphens (-) and cannot exceed 64 characters.
Description	By default, the rule description is the same as the selected predefined policy description. You can also customize the rule description. A rule description can contain any types of characters and cannot exceed 512 characters.

Step 3 On the displayed **Configure Rule Parameters** page, configure required parameters and click **Next**.

Table 2-2 Parameter descriptions

Parameter	Description
Trigger Type	Specifies the conditions under which rules are triggered. Possible values are: ● **Configuration change**: The rule is triggered when a specific cloud resource is changed. ● **Periodic execution**: The rule is triggered at a specific frequency. **NOTE** You cannot modify the **Trigger Type** of predefined policies. The **Trigger Type** varies depending on different predefined policies.
Filter Type	Specifies the resources to be evaluated. Possible types are: ● **Specific resources**: Resources of a specific type will be evaluated. ● **All resources**: All resources from your account will be evaluated. This parameter is mandatory only when **Trigger Type** is set to **Configuration change**.

Parameter	Description
Resource Scope	If you set **Filter Type** to **Specific resources**, you need to specify a resource scope. • **Service**: The service that the resource belongs to. • **Resource type**: The resource type • **Region**: The region where the resource resides. You only need to configure this parameter when **Trigger Type** is set to **Configuration change** and **Filter Type** is set to **Specific resources**. **NOTE** • You can specify a service and a resource type for **Resource Scope** only when **Trigger Type** is set to **Configuration change**. • You can specify a region for **Resource Scope** when **Trigger Type** is set to **Periodic execution** and the resources are not of the account type. You can check more predefined policies on Config console.
(Optional) Filter Scope	After you enable **Filter Scope**, you can filter resources by resource ID or tag. You can specify a specific resource for compliance evaluation. This parameter is optional for a rule whose trigger type is configuration change.
Execute Every	Indicates how often a rule is triggered. Available options: 1 hour, 3 hours, 6 hours, 12 hours, 24 hours. This parameter is mandatory only when **Trigger Type** is set to **Periodic execution**.
Configure Rule Parameters	Parameters of a built-in policy. For example, if you select the **required-tag-check** policy, you need to specify a tag, so that resources that do not have the tag will be determined as noncompliant. Some default policies, such as **volumes-encrypted-check**, do not require **Configure Rule Parameters**.
Tag	Tag of the rule. To add a tag, click **Add Tag** and enter a tag key and a tag value. You can add up to 20 tags to a rule. • A tag key cannot be empty. It can contain letters, digits, spaces, and special characters (_.:=+-@), but cannot start or end with a space or start with _sys_. A tag key can contain up to 128 characters. • A tag value cannot be empty. It can contain letters, digits, spaces, and special characters (_.:=+-@), but cannot start or end with a space. A tag value can contain up to 255 characters.

Step 4 On the **Confirm** page displayed, confirm the rule information and click **Submit**.

NOTE

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

----End

Viewing Evaluation Results

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

Step 1 Log in to the management console.

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

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

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

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

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

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

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.

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

Advanced Queries

Advanced Queries allow you to use ResourceQL to query how your resources in one or more regions are configured.

Advanced Queries allows you to filter and check your resources using ResourceQL.

ResourceQL is part of the Structured Query Language (SQL) SELECT syntax. It can perform attribute-based query and aggregation on the current resource data. 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, query EVS disks that are not attached to any ECS.

Resource Aggregator Overview

A resource aggregator enables you to aggregate resource configurations and compliance data from multiple accounts or an organization for centralized data query.

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

Conformance Package

A conformance package is a collection of rules. Config provides you with conformance packages to centrally create and manage rules, and query compliance data.

3 Resource List

3.1 Viewing Resources

3.1.1 Querying All Resources

Scenarios

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

NOTICE

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

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

Procedure

Step 1 Log in to the management console.

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

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

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

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

----End

3.1.2 Querying Details About a Resource

Scenarios

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

Procedure

Step 1 Log in to the management console.

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

Step 3 Click a resource name to view more details.

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

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

3.1.3 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 3-1 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.

Filter Criteria	Description
Resource Status	Resource status. A resource can be in either of the following states: ● **In use**: A resource is being used. ● **Deleted**: A resource has been deleted.
Tags	You can select a tag key and one or all values of this key to filter resources.
Enterprise Project	The enterprise project which resources belong to. If you select an enterprise project, resources in this enterprise project will be displayed. **NOTE** To filter resources by enterprise project, you need to enable Enterprise Center first. Filtering resources by enterprise project is only available to some users.

Procedure

Step 1 Log in to the management console.

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

Step 3 Filter resources by enterprise project, resource name, resource ID, resource status, enterprise project, or resource tag.

----End

3.1.4 Exporting the Resource List

Scenarios

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

Procedure

Step 1 Log in to the management console.

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

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

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

- If you do not set any search options, all your resources that are supported by Config will be exported.

- If you set search options to filter resources, only the search results will be exported. For details about how to filter resources, see **Filtering Resources**.

----End

NOTE

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

3.2 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 & Deployment**, click **Config**.

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

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

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

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

----End

3.3 Viewing Resource Relationships

Scenarios

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

Procedure

Step 1 Log in to the management console.

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

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

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

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

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

----End

NOTE

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

3.4 Viewing Resource Changes

Prerequisites

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

Scenarios

You can view resource changes over a time period. A record will be added to the resource timeline when the related service reports a resource attribute or relationship change to Config and the record will be retained for seven years by default.

Procedure

Step 1 Log in to the management console.

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

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

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

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

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

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

----End

4 Resource Recorder

4.1 Overview

Introduction

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

To be specific, the resource recorder:

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

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

Notes and Constraints

- When enabling and configuring the resource recorder, you must configure **Topic** or **Resource Dump**. To enable the resource recorder, you must configure either an SMN topic or an OBS bucket.
- To receive notifications of resource changes with the configured SMN topic, you not only have to create the topic, but also add subscription endpoints and request subscription confirmations for the topic.
- The resource recorder only updates data for the resources within the monitoring scope.
- By default, the resource configuration information is stored for seven years (2,557 days).
- There is a delay in synchronizing resource data to Config. The delay varies depending on services. If the resource recorder is enabled, Config will update

related data for resources that are included in the monitoring scope within 24 hours. If the resource recorder is disabled, Config will not update resource data.

NOTICE

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

4.2 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

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

Step 1 Log in to the management console.

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

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

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

Step 5 Select the monitoring scope.

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

NOTE

The resource recorder is default to record all resources of Config.

Step 6 Specify an OBS bucket.

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

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

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

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

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

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

NOTE

After you specify an OBS bucket from the current or another account, Config will write an empty file named **ConfigWritabilityCheckFile** to the OBS bucket to verify whether resources can be written to the OBS bucket. If an error is reported, you can address the error based on **Why Is an Error Reported When Data Is Dumped to the OBS Bucket After the Resource Recorder Is Enabled?**.

Step 7 Specify a data retention period.

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

NOTE

The data retention period only applies to resource 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.

Step 8 (Optional) Configure an SMN topic.

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

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

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

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

Step 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 for writing data into an OBS bucket. The agency created by **quick granting** doesn't contain KMS permissions, so the resource recorder is unable to store resource change notifications and snapshots to an OBS bucket that is encrypted using KMS. If you need to use an encrypted bucket, you can add required permissions 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 Config. The agency must include either the permissions for sending notifications using an SMN topic or the permissions for writing data into an OBS bucket. To store resource changes and snapshots to an OBS bucket that is encrypted using KMS, you need the required permissions. For details, see **Storing Resource Change Notifications and Resource Snapshots to an Encrypted OBS Bucket**. For details about how to create an agency, see *Identity and Access Management User Guide*.

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 navigation pane on the left, choose **Resource Recorder**.

Step 2 Click **Modify Resource Recorder**.

Step 3 Modify configurations.

Step 4 Click **Save**.

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

----End

Disabling the Resource Recorder

You can disable the resource recorder at any time.

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

Step 2 Toggle off the resource recorder.

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

----End

Cross-Account Authorization

- **Granting SMN topic permissions to another account**
  a. Log in to the management console with the authorizing account and go to the SMN console.
  b. Attach related SMN permissions to target accounts based on the "Configuring Topic Policies" section in the *Simple Message Notification User Guide*.
- **Granting OBS bucket permissions to another account**
  a. Log in to the management console with the authorizing account and go to the OBS console.
  b. Grant related OBS permissions to target accounts based on the "Creating a Custom Bucket Policy (JSON View)" in the *Object Storage Service User Guide*.

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

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

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

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

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

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

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

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

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

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

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

  a. Log in to the management console and go to the **Key Management Service** page on the Data Encryption Workshop (DEW) console.
  b. In the **Custom Keys** tab, click the alias of a target key to go to its details page and create a grant on it.
  c. Grant the account the permissions for using the key based on the "Creating a Grant" section in the *Data Encryption Workshop User Guide*.
     - Select **Account** for **User or Account** and enter an account ID.
     - Select **Create Data Key**, **Describe Key**, and **Decrypt Data Key** for **Granted Operations**.

4.3 Notifications

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

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

Config sends notifications when:

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

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

4.4 Storing Resource Snapshots

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

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

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

The following shows an example file name: 0926901ef980f2150fbdc001fdd23e80_Snapshot_regionid1_ResourceSnapshot_2024-07-22T221441Z_90decead-b69b-4522-a090-657d8c299d40_part-1.json.gz.

For more details, see Object Storage Service User Guide.

NOTE

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

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

4.5 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 confirmations for the topic.

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

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

The following shows an example name of a resource change notification file: 0926901ef980f2150fbdc001fdd23e80_Notification_regionid1_NotificationChunk_OBS_BUCKETS_2024-07-24T214735Z_2024-07-24T214759Z.json.gz

For more details, see Object Storage Service User Guide.

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

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

5 Resource Compliance

5.1 Rules

5.1.1 Adding a Rule with a Predefined Policy

Scenarios

You can create a rule to evaluate your resource compliance. When creating a rule, you can select a built-in 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

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

NOTICE

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

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

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

Procedure

Step 1 Log in to the management console.

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

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

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

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

Table 5-1 Parameters of basic configurations

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

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

Table 5-2 Parameter descriptions

Parameter	Description
Trigger Type	Specifies the conditions under which rules are triggered. Possible values are: • **Configuration change**: The rule is triggered when a specific cloud resource is changed. • **Periodic execution**: The rule is triggered at a specific frequency. **NOTE** You cannot modify the **Trigger Type** of predefined policies. The **Trigger Type** varies depending on different predefined policies.

Parameter	Description
Filter Type	Specifies the resources to be evaluated. Possible types are: • **Specific resources**: Resources of a specific type will be evaluated. • **All resources**: All resources from your account will be evaluated. This parameter is mandatory only when **Trigger Type** is set to **Configuration change**.
Resource Scope	If you set **Filter Type** to **Specific resources**, you need to specify a resource scope. • **Service**: The service that the resource belongs to. • **Resource type**: The resource type • **Region**: The region where the resource resides. You only need to configure this parameter when **Trigger Type** is set to **Configuration change** and **Filter Type** is set to **Specific resources**. **NOTE** • You can specify a service and a resource type for **Resource Scope** only when **Trigger Type** is set to **Configuration change**. • You can specify a region for **Resource Scope** when **Trigger Type** is set to **Periodic execution** and the resources are not of the account type. You can check more predefined policies on Config console.
(Optional) Filter Scope	After you enable **Filter Scope**, you can filter resources by resource ID or tag. You can specify a specific resource for compliance evaluation. This parameter is optional for a rule whose trigger type is configuration change.
Execute Every	Indicates how often a rule is triggered. Available options: 1 hour, 3 hours, 6 hours, 12 hours, 24 hours. This parameter is mandatory only when **Trigger Type** is set to **Periodic execution**.
Configure Rule Parameters	Parameters of a built-in policy. For example, if you select the **required-tag-check** policy, you need to specify a tag, so that resources that do not have the tag will be determined as noncompliant. Some default policies, such as **volumes-encrypted-check**, do not require **Configure Rule Parameters**.

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

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

NOTE

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

----End

5.1.2 Viewing a Rule

Scenario

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

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

NOTE

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

Procedure

Step 1 Log in to the management console.

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

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

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

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

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

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

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.

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

5.1.3 Triggering a Rule

Scenarios

Rules can be triggered automatically or manually.

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

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

Constraints and Limitations

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

NOTICE

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

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

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

Procedure

Step 1 Log in to the management console.

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

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

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

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

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

----End

5.1.4 Editing a Rule

Scenario

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

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

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

NOTE

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

Disabling a Rule

Step 1 Log in to the management console.

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

----End

Enabling a Rule

Step 1 Log in to the management console.

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

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

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

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

NOTE

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

----End

Modifying a Rule

Step 1 Log in to the management console.

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

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

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

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

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

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

NOTE

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

----End

Deleting a Rule

To delete a rule, you need to disable the rule first.

Step 1 Log in to the management console.

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

Step 5 Click **OK**.

----End

5.2 Organization Rules

5.2.1 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 to create an organization rule. This section describes how to create an organization rule with a built-in policy.

Constraints and Limitations

- You can add up to 500 rules in an account.
- The resource recorder must be enabled for adding, modifying, and triggering organization rules. If the resource recorder is disabled, you can only view and delete organization rules.
- The **Organization Rules** tab is inaccessible for a non-organization member.

NOTICE

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

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

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

Procedure

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

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

Table 5-3 Parameters of the basic configuration

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

Table 5-4 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**.
Resource Scope	If you set **Filter Type** to **Specific resources**, you need to specify a resource scope. • **Service**: The service to which a resource belongs. • **Resource type**: The resource type of the corresponding service. • **Region**: The region where the resource is located. This parameter is mandatory only when **Trigger Type** is set to **Configuration change**.
Filter Scope	After you enable **Filter Scope**, you can filter resources by resource ID or tag. You can specify a specific resource for compliance evaluation. This parameter is mandatory only when **Trigger Type** is set to **Configuration change**.
Execute Every	Indicates how often a rule is triggered. This parameter is mandatory only when **Trigger Type** is set to **Periodic execution**.
Rule Parameter	Parameters of a built-in policy. For example, if you select the **required-tag-check** policy, you need to specify a tag, so that resources that do not have the tag will be determined as noncompliant. Not all built-in policies require **Configure Rule Parameters**. For example, the rule, **volumes-encrypted-check**, does not require **Configure Rule Parameters**.

Parameter	Description
Destination	Specifies where the organization rule will be deployed. • **Organization**: A policy is deployed to all member accounts in an organization. • **Current Account**: A policy is deployed to the current account. When creating an organization rule, select **Organization**.
Excluded Account	Member accounts to which organization rules will not be deployed. This parameter is only required when **Destination** is set to **Organization**.

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

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**.

5.2.2 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 Log in to the management console.

Step 2 Click  in the upper left corner. Under **Management & Deployment**, 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.

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

NOTE

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

----End

Viewing Organization Rules Deployed to Member Accounts

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

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

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

NOTE

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

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

----End

5.2.3 Modifying an Organization Rule

Scenarios

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

NOTE

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

Procedure

Step 1 Log in to the management console.

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

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

5.2.4 Deleting an Organization Rule

Scenarios

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

Procedure

Step 1 Log in to the management console.

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

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

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

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

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

----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.

5.3 Viewing Noncompliant Resources

Scenarios

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

Procedure

Step 1 Log in to the management console.

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

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

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

Step 5 Click a resource name to view resource overview.

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

----End

5.4 Compliance Rule Concepts

5.4.1 Policy

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 a resource scope.

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

Table 5-5 Policy parameters (JSON)

Parameter	Description	Remarks
id	Policy ID	N/A
name	Policy name	A policy name can contain up to 64 characters.
display_name	Display name of a policy	A policy display name can contain up to 64 characters.
description	Policy description	Policy description can contain up to 512 characters.

Parameter	Description	Remarks
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		**builtin**: indicates the type of policies that are provided and maintained by Config.
policy_rule_type	Policy syntax	**Domain Specific Language (DSL)**: provided by Config to write policy expressions.

Parameter	Description	Remarks
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')}"
      }
    ]
  },
}
```

5.4.2 Rule

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

You can use a JSON expression to represent a rule, as shown in **Table 5-6**.

Table 5-6 Rule parameters (JSON)

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

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

Parameter	Description	Limitations	Remarks
created	Specifies the time when the rule was created.	N/A	**NOTE** The time is a UTC time in a fixed format complying with ISO-8601 (for example, **2018-11-14T08:59:14Z**).
updated	Specifies the time when the rule was updated.	N/A	
policy_definition_id	Specifies the ID of the compliance policy bound to the rule.	Its value must be a string with up to 64 characters. Only letters, digits, and hyphens (-) are allowed.	Policy ID
parameters	Specifies the values of rule parameters.	**parameters**: The value must be an object. ● **key**: The value must be a string including only letters and numbers. If the policy type of the rule is **Custom policy**, the value can have up to 1,024 characters. ● **value**: The value must be an object, and the value restrictions vary depending on the parameter type.	The compliance policy bound to the rule has corresponding parameters. The number, type, and value range of those parameters depend on the selected compliance policy.
tags	Tags added to a rule	-	● A tag key can contain up to 128 Unicode characters. ● A tag value can contain up to 255 Unicode characters.
created_by	The creator of a rule	-	A rule can be created by a user or a service with the required service-link agency.

NOTE

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

The following shows a predefined policy that is used to check whether ECSs in **regionid_1** have a specific tag (**env**: **production**).

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

5.4.3 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 5-7**.

Table 5-7 Evaluation result in JSON

Parameter	Description	Remarks
domain_id	Account ID	This parameter is used to distinguish users. **domain_id** will be provided in each evaluation result.
resource_id	Specifies the ID of the evaluated resource.	N/A
resource_name	Specifies the service type.	N/A
resource_provider	Specifies the service the resource belongs to.	N/A

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

The following JSON expression shows a non-compliant evaluation result:

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

6 Conformance Packages

6.1 Overview

Functions

A conformance package is a collection of rules. With conformance packages, you can evaluate resource compliance using multiple rules at the same time and centrally query conformance data.

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

If you are an organization administrator or a delegated administrator of Config, you can add organization conformance packages and 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 quickly create conformance packages quickly. Sample templates are scenario-based with appropriate compliance rules and parameters.

Pre-defined conformance package:

A pre-defined conformance package is created using a sample template. To deploy a pre-defined conformance package, you only need to configure a few parameters.

Custom conformance package:

A custom conformance package is created using a custom template. You can include both predefined and custom rules in a custom template. When you deploy a conformance package, you can upload a package template or use a package template stored in an OBS bucket. A custom template must be a JSON file. Other file formats, such as tf or zip, are not supported.

Compliance data

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

- Evaluation results for a conformance package: All rules in the conformance package are used for resource evaluation. If a resource is found to be noncompliant by any of the rules in the package, the evaluation result is noncompliant. If all resources are compliant, the evaluation result is compliant.
- Evaluation results for a rule: Each rule in the conformance package has an evaluation result. If a resource is found to be noncompliant, the result is noncompliant. If all resources are compliant, the result is compliant.
- Compliance score: The percentage of resources that are evaluated as compliant by a conformance package. A compliance score of 100 indicates that all resources evaluated are compliant. A score of 0 indicates that all resources evaluated are noncompliant.

  Figure 6-1 Compliance score formula:

$$\text{Score} = \frac{\sum_{\text{Rules}} \text{Compliant resource count}}{\sum_{\text{Rules}} \text{Total resource count}} \times 100\%$$

Stack:

A stack allows a rule to be created or deleted in a conformance package. .

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, a corresponding agency needs to be created for RFS.

- Quick authorization: This option creates the **rms_conformance_pack_agency** agency for RFS to create and delete a conformance package and to create, update and delete rules in a conformance package.
- Custom authorization: You can create an agency and perform custom authorization through IAM. The agency must contain required permissions for RFS to create, update, and delete rules..

6.2 Conformance Packages

6.2.1 Creating a Conformance Package

Scenarios

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

After a conformance package is created, the first evaluation using rules in the package will be automatically triggered. More evaluations will be triggered based on the specified trigger type of each rule. You can also manually trigger a rule for resource evaluation.

Constraints and Limitation

- Up to 50 conformance packages (including organization conformance packages) and 500 rules can be created in an account.
- To create or modify a conformance package, the resource recorder must be enabled. If the resource recorder is disabled, you can only view or delete conformance packages. For details, see **Configuring the Resource Recorder**.

Procedure

Step 1 Log in to the management console.

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

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

Step 4 Click **Create Conformance Package**.

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

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

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

  The template must be a JSON file with the name extension: .tf.json.

- OBS bucket: The location of the OBS bucket that stores the custom conformance package template. If your local template file exceeds 50 KB, upload it to an OBS bucket and enter the OBS URL when you need to select a package template.

  NOTE

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

Step 6 On the **Configure Detailed Information** page, configure required parameters and click **Next**.

Table 6-1 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 granting**: This option creates an **agency named rms_conformance_pack_agency** for RFS to create, update, and delete rules and to create and delete conformance packages. • **Custom granting**: You can create an agency and perform custom authorization through IAM. The agency must contain required permissions for RFS to create, update, or delete rules.
Parameters	Parameters of a conformance package are consistent with rules in the package.

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

NOTE

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

----End

6.2.2 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 & Deployment**, click **Config**.

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

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

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

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

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

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

6.2.3 Modifying a Conformance Package

Scenario

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

NOTE

To create or modify a conformance package, the resource recorder must be enabled. If the resource recorder is disabled, you can only view or delete conformance packages. For details, see **Configuring the Resource Recorder**.

Procedure

Step 1 Log in to the management console.

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

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

6.2.4 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 & Deployment**, 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.

----End

6.3 Organization Conformance Packages

6.3.1 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 modify an organization conformance package, the resource recorder must be enabled. If the resource recorder is disabled, you can only view or delete organization conformance packages. For details, see **Configuring the Resource Recorder**.
- The **Organization Conformance Package** tab is inaccessible for non-organization members on Config console.

Procedure

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

Step 2 Click  in the upper left corner. Under **Management & Deployment**, 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**.

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

The template must be a JSON file with the name extension: .tf.json.

- OBS bucket: The location of the OBS bucket that stores the custom conformance package template. If your local template file exceeds 50 KB, upload it to an OBS bucket and enter the OBS URL when you need to select a package template.

  NOTE

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

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

Table 6-2 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.
Destination	Specifies where an organization conformance package will be deployed. • **Organization** indicates that a conformance package will be deployed to all members in a specified organization. • **Current Account** indicates that a conformance package will be deployed to the current account. When creating an organization conformance package, select **Organization**.
Excluded Account	Member accounts to which organization conformance packages will not be deployed. This parameter is only required when **Destination** is set to **Organization**.

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

NOTE

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

----End

6.3.2 Viewing an Organization Conformance Package

Scenario

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

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

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

Viewing an Organization Conformance Package (for Administrators)

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

Step 2 Click  in the upper left corner. Under **Management & Deployment**, 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.

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 an Organization Conformance Package (for Organization Members)

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

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

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

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

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

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

NOTE

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

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

----End

6.3.3 Modifying an Organization Conformance Package

Scenario

You can modify the name or parameters of an organization conformance package at any time. If you fail to deploy an organization conformance package to some members in your organization, you can include these accounts in the **Excluded Account** area and then redeploy the package.

NOTE

To create or modify an organization conformance package, the resource recorder must be enabled. If the resource recorder is disabled, you can only view or delete organization conformance packages. For details, see **Configuring the Resource Recorder**.

Procedure

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

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

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

6.3.4 Deleting an Organization Conformance Package

Scenario

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

Procedure

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

Step 2 Click  in the upper left corner. Under **Management & Deployment**, 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.

----End

7 Advanced Queries

7.1 Overview

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

You can conveniently use ResourceQL and a query editor to search for and view your resources.

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

You can use Advanced Queries to:

- Manage inventory. For example, you can query ECSs with certain specifications.
- Check security compliance of your resources. For example, you can check if the configurations (public IPs attached or disks encrypted) of your resources meet security requirements.
- Optimize costs. For example, you can list all EVS disks that have not been attached to any ECS to avoid unnecessary expenditures.

NOTE

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

7.2 Restrictions

To prevent a single user from occupying resources for queries for too long, the following constrains are set on advanced queries:

- If the execution duration of a query statement exceeds 15 seconds, a timeout error will be returned.
- If the result set to be returned exceeds the size limit, an error will occur. Make sure that the data volume returned by each statement is within the size limit.

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

NOTICE

To get full functionality of advanced queries, you need to enable the resource recorder. The following describes how the resource recorder may affect your use of advanced queries.

- If you have never enabled the resource recorder, no resources can be queried with an advanced query.
- If you have enabled the resource recorder and a monitoring scope is specified, only resources within the monitoring scope can be queried with an advanced query.
- If you enable the resource recorder and disable it after a period of time, only resource data collected during the period when the resource recorder was enabled can be queried with an advanced query.

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

7.3 Creating a Custom Query

Scenarios

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

This section includes the following content:

- **Creating a Custom Query**
- **Using a Predefined Query**
- **Configuration Examples of Advanced Queries**

Creating a Custom Query

Step 1 Log in to the management console.

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

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

Step 4 Choose the **Custom Queries** tab and click **Create Query** in the upper right corner.

Step 5 In the **Query Editor**, enter the query statements.

On the left of the page, the Schema information is displayed. Schema information shows detailed resource attributes that are specified by the **properties** parameter

in the statement. For details about query statements, see **Configuration Examples of Advanced Queries**.

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

A query name can contain only digits, letters, underscores (_), and hyphens (-). It cannot exceed 64 characters.

Step 7 Click **OK**.

NOTE

There is a limit to how many custom queries you can create. If you exceed this limit, you will receive a notification: "The maximum number of custom queries has been reached." Although the query cannot be saved, you can still run the query and export the results.

Step 8 Click **Run** and then view the query results. Up to 4,000 query results can be displayed and exported.

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

----End

Using a Predefined Query

You can modify the name, description, and statement of a default query or a custom query and save it as a new query. The following procedure uses a default query as an example.

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

All default queries are displayed in a list.

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

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

Step 3 In the **Query Editor**, modify the query.

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

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

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

After a new query is created, the new query becomes a custom query and will be displayed in the custom query list.

----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 7-1 Parameter descriptions in table **resources**

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

Example quires are as follows:

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

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

- Example 2: List EVS disks with certain specifications.

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

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

```
SELECT *
FROM resources
```

```
WHERE provider = 'obs'
 AND type = 'buckets'
 AND name LIKE '%figure%'
```

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

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

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

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

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

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

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

7.4 Viewing a Query

Scenarios

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

Procedure

Step 1 Log in to the management console.

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

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

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

View the query name and description in the query list.

Step 4 Locate the query and click its name.

The SQL statement details in the query are displayed.

----End

7.5 Modifying a Custom Query

Scenarios

You can follow the following procedure to modify the statement, name, and description of a custom query.

NOTE

You can modify the statement, name, and description of a predefined query and save it as a new custom query. For details, see **Using a Predefined Query**.

Procedure

Step 1 Log in to the management console.

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

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

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

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

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

Step 6 In the **Query Editor**, modify the query.

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

Step 7 Click **Save**.

Step 8 In the displayed dialog box, modify the query name and description and click **OK**.

A query name can contain only digits, letters, underscores (_), and hyphens (-). It cannot exceed 64 characters.

----End

7.6 Deleting a Query

Scenarios

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

NOTE

Default queries cannot be deleted.

Procedure

Step 1 Log in to the management console.

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

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

Step 4 Click **Custom Queries**.

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

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

----End

8 Resource Aggregation

8.1 Overview

Functions

A resource aggregator enables you to aggregate resource configurations and compliance data from multiple accounts or an organization for centralized data query.

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

NOTE

You can only use aggregators to query or view resource data from source accounts. If you need to modify or delete resources, go to related service consoles.

Setting Up An Aggregator

To collect resource data from source accounts, perform the following operations:

1. Create an aggregator. For more details, see **Creating a Resource Aggregator**.
2. Enable the resource recorder from every source account. For more details, see **Configuring the Resource Recorder**.
3. Authorize the aggregator account to collect resource configurations and compliance data from source accounts. For more details, see **Authorizing an Aggregator Account**.
4. View resource configurations and compliance data aggregated. For more details, see **Viewing Aggregated Rules** and **Viewing Aggregated Resources**.

Basic Concepts

Source Account

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

Aggregator

An aggregator is a kind of Config resource allowing you to collect resource configuration and compliance data from multiple resource accounts.

Aggregator Account

An aggregator account is an account used to create an aggregator.

Authorization

An aggregator account must gain authorization from source accounts for data collection. An organization aggregator, however, does not need authorization to collect data from members.

8.2 Restrictions

The following lists aggregator constrains:

- Up to 30 account specific aggregators can be created in an account.
- An aggregator can aggregate data from up to 30 source accounts.
- An account specific aggregator can add, update, and delete up to 1,000 source accounts every 7 days.
- Up to 1 organization specific aggregator can be created in an account.
- You can only create one organization within 24 hours. If you create and then delete an organization aggregator, creating an organization aggregator will not be supported within 24 hours of the creation.
- To aggregate data from source accounts, the resource recorder in each source account must be enabled. The following lists more detailed information:

NOTICE

The following provides more detailed information:

- If the resource recorder in a source account has not been enabled, neither resource nor compliance data can be aggregated.
- If a monitoring scope has been configured in a source account, only related data of the resources within the specified scope will be aggregated.
- If the resource recorder in a source account is enabled and then disabled, data aggregated from the source account will be deleted after the resource recorder is disabled.

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

8.3 Creating a Resource Aggregator

Scenarios

You can create an account specific or organization specific aggregator.

To aggregate data from a source account, an account aggregator must obtain related authorization. For details, see **Authorizing an Aggregator Account**.

NOTE

To create an organization aggregator, you need the following permissions for Organizations:

- organizations:organizations:get
- organizations:accounts:list
- organizations:delegatedAdministrators:list
- organizations:trustedServices:enable
- organizations:trustedServices:list

Procedure

Step 1 Log in to the management console.

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

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

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

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

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

NOTE

- An account specific aggregator can only aggregate data from accounts, so source account IDs must be specified.
- 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. 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

8.4 Viewing Resource Aggregators

Scenarios

You can view and search for all created resource aggregators and their details in the resource aggregator list.

NOTE

To view resource and compliance data aggregated by an organization aggregator, you need the following permissions:

- organizations:organizations:get
- organizations:delegatedAdministrators:list
- organizations:trustedServices:list

Procedure

Step 1 Log in to the management console.

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

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

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

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

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

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

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

On the details page, click a rule name in the **Non-compliant Rules** area to view details of this rule.

----End

8.5 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 Log in to the management console.

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

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

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

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

Step 5 On the **Edit Aggregator** page, edit the name and source accounts.

Step 6 Click **OK**.

----End

8.6 Deleting a Resource Aggregator

Scenarios

If a resource aggregator is no longer used, you can delete it.

Procedure

Step 1 Log in to the management console.

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

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

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

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

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

----End

8.7 Viewing Aggregated Rules

Scenarios

You can view and filter all compliance data aggregated by an aggregator. For example, you can filter rules by rule name, evaluation result, and account ID.

NOTE

To view compliance data aggregated by an organization aggregator, you need the following permissions:

- organizations:organizations:get
- organizations:delegatedAdministrators:list
- organizations:trustedServices:list

Procedure

Step 1 Log in to the management console.

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

Step 3 On the left navigation, choose **Resource Aggregation** > **Rules**.

Step 4 In the upper right corner, select an aggregator from the drop-down list.

In the rule list, click a target rule name to view rule details.

In the search box above the list, enter a rule name, evaluation result, or an account ID to filter compliance data.

----End

8.8 Viewing Aggregated Resources

Scenarios

You can view all resources aggregated by an aggregator. You can filter resource data by aggregator, resource name, account ID, and resource type. You can also view details of each resource.

NOTE

To view resource data aggregated by an organization aggregator, you need the following permissions:

- organizations:organizations:get
- organizations:delegatedAdministrators:list
- organizations:trustedServices:list

Procedure

Step 1 Log in to the management console.

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

Step 3 In the navigation pane, choose **Resource Aggregation** > **Resources**.

Step 4 In the upper left corner of the page, select a resource aggregator to be viewed. All resources aggregated by this aggregator will be displayed in a list. You can export all resource data.

In the search box above the list, enter the name, ID, or type of a resource to filter resource data.

In the resource list, click a target resource name to view resource details.

----End

8.9 Authorizing an Aggregator Account

Scenarios

To aggregate data from a source account, an aggregator account must obtain authorization from this source account. After the authorization, all aggregators created before or after the authorization with this aggregator account can aggregate data from this source account.

An organization specific aggregator can collect resource data of all member accounts in an organization without source account authorization.

This section describes the following topics:

- **Adding Authorization**
- **Accepting an Authorization**
- **Deleting an Authorization**

Adding an Authorization

You can use the **Add Authorization** function to authorize an aggregator account.

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Resource Aggregation** > **Authorizations**.

Step 4 Click **Add Authorization** in the upper right corner of the page.

Step 5 In the **Add Authorization** dialog box, enter the ID of the aggregator account which you want to authorize.

Step 6 Click **OK**.

After the authorization is complete, an authorization record will be displayed in the **Authorized** list.

----End

Accepting an Authorization

You can approve a pending authorization request to authorize an aggregator account.

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Resource Aggregation** > **Authorizations**.

Step 4 Click the **Pending Authorization** tab, locate the account ID that sends an authorization request to be processed in the list, and click **Authorize** in the **Operation** column.

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

After the authorization request is accepted, the authorization record is displayed in the **Authorized** list.

----End

Deleting an Authorization

You can revoke authorization from an aggregator account.

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Resource Aggregation** > **Authorizations**.

Step 4 Locate the authorization to be deleted in the list, and click **Delete** in the **Operation** column.

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

The authorization record will be moved to the **Pending Authorization** tab, and the authorization status will change to **Pending authorization**.

To authorize the aggregator account again, you can click **Authorize** in the **Operation** column in the **Pending Authorization** list.

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

8.10 Advanced Queries

Overview

Resource aggregation supports advanced queries. You can use ResourceQL to query configuration states of resources from one or more source accounts.

You can use ResourceQL and the query editor to customize queries for viewing and search for resources.

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

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

NOTE

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

Limitations

To prevent a single user from occupying resources for queries for too long, the following constrains are set on advanced queries:

- If the execution duration of a query statement exceeds 15 seconds, a timeout error will be returned.
- If the result set to be returned exceeds the size limit, an error will occur. Make sure that the data volume returned by each statement is within the size limit.
- Up to 4,000 records are returned for a single query.
- A single query statement can be used to perform a maximum of two join queries for tables.
- A maximum of 200 advanced queries can be created for each account.

NOTICE

To get full functionality of advanced queries, you need to enable the resource recorder. The following describes how the resource recorder may affect your use of advanced queries.

- If you have never enabled the resource recorder, no resources can be queried with an advanced query.
- If you have enabled the resource recorder and a monitoring scope is specified, only resources within the monitoring scope can be queried with an advanced query.
- If you enable the resource recorder and disable it after a period of time, only resource data collected during the period when the resource recorder was enabled can be queried with an advanced query.

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

Creating a Query

Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, choose **Resource Aggregation** > **Advanced Queries**.

Step 4 Choose the **Custom Queries** tab and click **Create Query** in the upper right corner.

Step 5 In the **Query Range** area on the right, select a target aggregator. In the text box below, enter the statement.

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

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

A query name can contain only digits, letters, underscores (_), and hyphens (-). It cannot exceed 64 characters.

Step 7 Click **OK**.

NOTE

There is a limit to how many custom queries you can create. If you exceed this limit, you will receive a notification: "The maximum number of custom queries has been reached." Although the query cannot be saved, you can still run the query and export the results.

Step 8 Click **Run** and then view the query results. Up to 4,000 query results can be displayed and exported.

Step 9 Click **Export** 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 **Using a Predefined Query**.
- To view the name, description, and query statements of a query, see **Viewing a Query**.
- To modify the query statement of a custom query, see **Modifying a Custom Query**.
- To delete a custom query, see **Deleting a Query**. Default queries cannot be deleted.

  NOTE

  To run an advanced query for an aggregator, you must specify this aggregator first.

Configuration Examples of Advanced Queries

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

Table 8-1 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

Parameter	Type	Description
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**.

9 Cloud Trace Service

9.1 Supported Config Operations

Scenarios

Cloud Trace Service (CTS) records operations on Config for your later query, audit, and backtrack.

Prerequisites

You have enabled CTS.

Key Operations Recorded by CTS

Table 9-1 Config operations supported by CTS

Operation	Resource Type	Event Name
Creating rules	policy	createPolicyAssignments
Deleting rules	policy	deletePolicyAssignment
Updating rules	policy	updatePolicyAssignment
Triggering rules	policy	runEvaluation
Disabling rules	policy	disablePolicyAssignment
Enabling rules	policy	enablePolicyAssignment
Creating or updating rule remediation configurations	policy	createOrUpdateRemediationConfiguration
Deleting rule remediation configurations	policy	deleteRemediationConfiguration

Operation	Resource Type	Event Name
Running remediation actions (manual)	policy	runRemediationExecution
Batch creating remediation exceptions	policy	batchCreateRemediationExceptions
Batch deleting remediation exceptions	policy	batchDeleteRemediationExceptions
Updating evaluation results	policyState	updatePolicyState
Configuring or modifying the resource recorder	trackerConfig	createOrUpdateTrackerConfig
Disabling the resource recorder	trackerConfig	deleteTrackerConfig
Creating advanced queries	storedQuery	createStoredQuery
Updating advanced queries	storedQuery	updateStoredQuery
Deleting advanced queries	storedQuery	deleteStoredQuery
Creating organization rules	organizationPolicyAssignments	createOrganizationPolicyAssignment
Updating organization rules	organizationPolicyAssignments	updateOrganizationPolicyAssignment
Deleting an organization rule	organizationPolicyAssignments	deleteOrganizationPolicyAssignment
Authorizing aggregator accounts	authorization	createAggregationAuthorization
Canceling aggregator account authorization	authorization	deleteAggregationAuthorization
Creating an aggregator	aggregator	createConfigurationAggregator
Deleting an aggregator	aggregator	deleteConfigurationAggregator
Updating an aggregator	aggregator	updateConfigurationAggregator
Deleting pending aggregation requests	aggregationRequests	deletePendingAggregationRequest
Creating a conformance package	conformancePacks	createConformancePack

Operation	Resource Type	Event Name
Deleting a conformance package	conformancePacks	deleteConformancePack
Updating conformance packages	conformancePacks	updateConformancePack
Creating organization conformance packages	organizationConformancePacks	createOrganizationConformancePack
Deleting organization conformance packages	organizationConformancePacks	deleteOrganizationConformancePack
Updating organization conformance packages	organizationConformancePacks	updateOrganizationConformancePack
Batch adding resource tags	policy	tagResource
Batch deleting resource tags	policy	unTagResource

9.2 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**

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 & Deployment > **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 section "Trace References" > "Trace Structure" and section "Trace References" > "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.

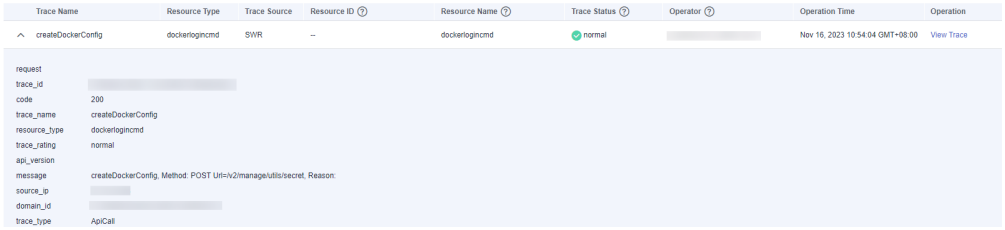
Viewing Real-Time Traces in the Trace List of the Old Edition

1. Log in to the management console.
2. Click  in the upper left corner and choose **Management & Deployment** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. Each time you log in to the CTS console, the new edition is displayed by default. Click **Go to Old Edition** in the upper right corner to switch to the trace list of the old edition.
5. Set filters to search for your desired traces. The following filters are available:
   - **Trace Type**, **Trace Source**, **Resource Type**, and **Search By**: Select a filter from the drop-down list.

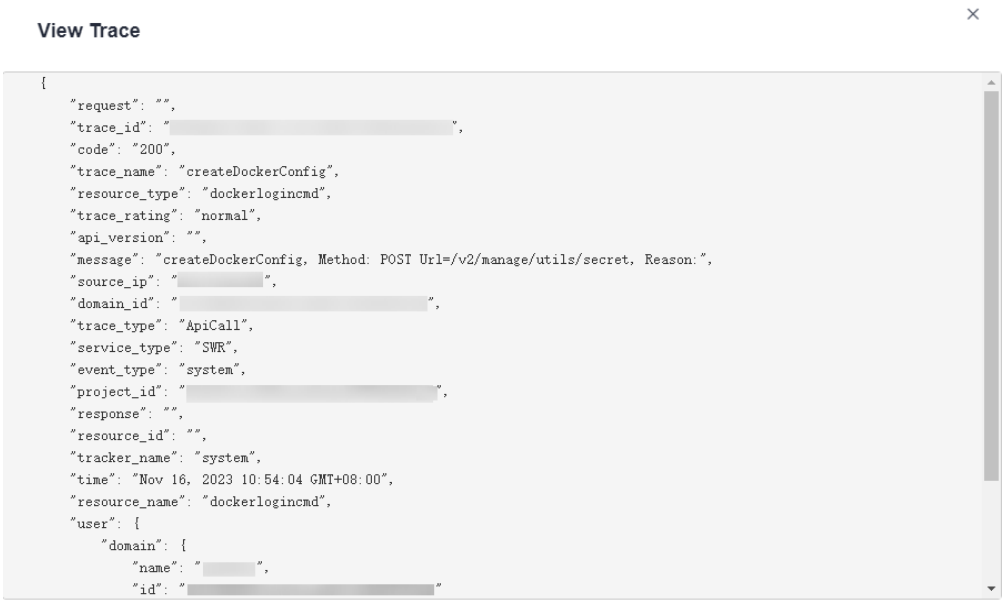
- If you select **Resource ID** for **Search By**, specify a resource ID.
- If you select **Trace name** for **Search By**, specify a trace name.
- If you select **Resource name** for **Search By**, specify a resource name.

– **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.



9. Click **View Trace** in the **Operation** column. The trace details are displayed.



10. For details about key fields in the trace structure, see section "Trace References" > "Trace Structure" and section "Trace References" > "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.

10 Appendix

10.1 Supported Services and Regions

To view services and regions supported by Config, log in to the console and click **Supported Services and Regions** in **Resource List** page. Supported services and regions are displayed.

10.2 Notification Models

10.2.1 Resource Change Notification Model

Resource Change Notification Model

Table 10-1 Parameters of the resource change notification model

Parameter	Type	Description
notification_type	String	The type of the notification. For a resource change notification, the notification type is **ResourceChanged**.
notification_creation_time	String	The time when the message was sent. The notification creation time is a UTC time (such as 2018-11-14T08:59:14Z) that complies with ISO8601.
domain_id	String	Account ID.
detail	Object	Notification details.

Table 10-2 detail parameters

Parameter	Type	Description
resource_id	String	Resource ID.
resource_type	String	Resource type.
event_type	Enum	Event type (**CREATE**, **UPDATE**, **DELETE**)
capture_time	String	The event capture time. The event capture time is a UTC time (such as 2018-11-14T08:59:14Z) that complies with ISO8601.
resource	Object	Resource details.

Table 10-3 resource

Parameter	Type	Description
id	String	Resource ID.
name	String	Resource name.
provider	String	Cloud service name.
type	String	Resource type.
region_id	String	The ID of the region where the resource resides.
project_id	String	IAM project ID.
project_name	String	IAM project name.
ep_id	String	Enterprise project ID.
ep_name	String	Enterprise project name.
checksum	String	The checksum.
created	String	Resource creation time. The resource creation time is a UTC time (such as 2018-11-14T08:59:14Z) that complies with ISO8601.

Parameter	Type	Description
updated	String	The time when the resource was last updated. The latest update time is a UTC time (such as 2018-11-14T08:59:14Z) that complies with ISO8601.
provisioning_state	String	Resource provisioning state.
tags	Map	Resource tags.
properties	Map	Resource attributes.

Notification Example of Resource Changes


```
{
  "detail": {
    "resource": {
      "id": "3e62c0e6-e779-469e-b0f2-35743f6229d1",
      "name": "ecs-51c8",
      "provider": "evs",
      "type": "volumes",
      "checksum": "b3bcc019cecbb701e324e0dcf2f283236685885236b49f5ba5ea2f5f788170a1",
      "created": "2020-08-12T07:14:41.638Z",
      "updated": "2020-08-12T07:14:44.423Z",
      "tags": {},
      "properties": {
        "shareable": false,
        "volumeType": "SATA",
        "metadata": {},
        "attachments": [],
        "replicationStatus": "disabled",
        "availabilityZone": "regionid1a",
        "bootable": "true",
        "userId": "059b5c937d80d3e41ff3c00a3c883d16",
        "volTenantAttrTenantId": "059b5e0a2500d5552fa1c00adada8c06",
        "size": "40",
        "encrypted": false,
        "volumeImageMetadata": {
          "virtualEnvType": "FusionCompute",
          "isregistered": "true",
          "imageSourceType": "uds",
          "minDisk": "40",
          "platform": "CentOS",
          "size": 0,
          "osVersion": "CentOS 7.5 64bit",
          "minRam": "0",
          "name": "CentOS 7.5 64bit",
          "checksum": "d41d8cd98f00b204e9800998ecf8427e",
          "osBit": "64",
          "osType": "Linux",
          "containerFormat": "bare",
          "supportXen": "true",
          "id": "e0adce3a-a4d2-4207-9018-69ce64b4426a",
          "supportKvm": "true",
          "diskFormat": "zvhd2",
          "imageType": "gold"
        },
        "links": [
          {
            "rel": "self",
```

```
            "href": "https://evs.regionid1a.xxxxxx.com/v2/059b5e0a2500d5552fa1c00adada8c06/os-vendor-volumes/3e62c0e6-e779-469e-b0f2-35743f6229d1"
          },
          {
            "rel": "bookmark",
            "href": "https://evs.regionid1a.xxxxxx.com/059b5e0a2500d5552fa1c00adada8c06/os-vendor-volumes/3e62c0e6-e779-469e-b0f2-35743f6229d1"
          }
        ],
        "volHostAttrHost": "regionid1a-pod01.regionid1a#0",
        "multiattach": false,
        "status": "available"
      },
      "region_id": "regionid1a",
      "project_id": "059b5e0a2500d5552fa1c00adada8c06",
      "project_name": "regionid1a",
      "ep_id": "0",
      "ep_name": "default",
      "provisioning_state": "Succeeded"
    },
    "resource_id": "3e62c0e6-e779-469e-b0f2-35743f6229d1",
    "resource_type": "evs.volumes",
    "event_type": "CREATE",
    "capture_time": "2020-08-12T07:15:15.116Z"
  },
  "notification_type": "ResourceChanged",
  "notification_creation_time": "2020-08-12T07:14:47.192Z",
  "domain_id": "059b5c937100d3e40ff0c00a7675a0a0"
}
```


10.2.2 Resource Relationship Change Notification Model

Resource Relationship Change Notification Model

Table 10-4 Parameters of the resource relationship change notification model

Parameters	Type	Description
notification_type	String	The type of a notification. For a resource relationship change notification, the notification type is **ResourceRelationChanged**.
notification_creation_time	String	The time when the message was sent. The notification creation time is a UTC time (such as 2018-11-14T08:59:14Z) that complies with ISO8601.
domain_id	String	Account ID.
detail	Object	Notification details.

Table 10-5 detail

Parameter	Type	Description
resource_id	String	Resource ID.
resource_type	String	Resource type.
event_type	Enum	Event type (**CHANGE**).
capture_time	String	The event capture time. The event capture time is a UTC time (such as 2018-11-14T08:59:14Z) that complys with ISO8601.

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"
}
```

10.2.3 Resource Snapshot Storage Notification Model

Resource Snapshot Storage Notification Model

Table 10-6 Parameters of the resource snapshot storage notification model

Parameter	Type	Description
notification_type	String	The type of a notification. For a resource snapshot storage notification, the notification type is **SnapshotArchiveCompleted**.
notification_creation_time	String	The time when the message was sent. The notification creation time is a UTC time (such as 2018-11-14T08:59:14Z) that complies with ISO8601.
domain_id	String	Account ID.
detail	Object	Notification details.

Table 10-7 detail

Parameter	Type	Description
snapshot_id	String	Resource snapshot ID.
region_id	String	The ID of the region where resource snapshots reside.
bucket_name	String	The name of the OBS bucket where resource snapshots are stored.
object_keys	Array of String	Path of the OBS object where resource snapshots are stored.

Notification Example of Resource Snapshot Storage

```
{
  "detail": {
    "snapshot_id": "474f85e6-72cd-442b-af4e-517120a5c669",
    "region_id": "regionid1a",
    "bucket_name": "test",
    "object_keys": [
      "RMSLogs/059b5c937100d3e40ff0c00a7675a0a0/Snapshot/
2020/8/11/059b5c937100d3e40ff0c00a7675a0a0_Snapshot_regionid1a_ResourceSnapshot_2020-08-10T170901_474f85e6-72cd-442b-af4e-517120a5c669_part-1.json.gz"
    ]
  },
  "notification_type": "SnapshotArchiveCompleted",
  "notification_creation_time": "2020-08-10T17:09:27.314Z",
  "domain_id": "059b5c937100d3e40ff0c00a7675a0a0"
}
```

10.2.4 Notification Model of Resource Change Notification Storage

Notification Model of Resource Change Notification Storage

Table 10-8 Parameters of the notification model of resource change notification storage

Parameter	Type	Description
notification_type	String	The type of a notification. For resource change notification storage, the notification type is **NotificationArchiveCompleted**.
notification_creation_time	String	The time when the message was sent. The notification creation time is a UTC time (such as 2018-11-14T08:59:14Z) that complies with ISO8601.

Parameter	Type	Description
domain_id	String	Account ID.
detail	Object	Notification details.

Table 10-9 detail parameters

Parameter	Type	Description
region_id	String	The ID of the region where resource change notifications are stored.
bucket_name	String	The name of the OBS bucket where resource change notifications are stored.
object_key	String	The path of an object in an OBS bucket for storing resource change notifications.

Notification Example of Resource Change Notification Storage

```
{
    "detail": {
        "region_id": "regionid1a",
        "bucket_name": "test",
        "object_key": "RMSLogs/059b5c937100d3e40ff0c00a7675a0a0/Notification/2020/12/10/
NotificationChunk/
059b5c937100d3e40ff0c00a7675a0a0_Notification_regionid1a_NotificationChunk_VPC_VPCS_2020-12-10T02
4612Z_2020-12-10T050621Z.json.gz"
    },
    "notification_type": "NotificationArchiveCompleted",
    "notification_creation_time": "2020-12-10T05:09:28.002Z",
    "domain_id": "059b5c937100d3e40ff0c00a7675a0a0"
}
```

10.3 Storage Models

10.3.1 Resource Snapshot Storage Model

Resource Snapshot Storage Model

Table 10-10 Resource snapshot storage model

Parameter	Type	Description
snapshot_id	String	Specifies the resource snapshot ID.

Parameter	Type	Description
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 10-11 Items parameters

Parameter	Type	Description
resource	Object	Specifies the resource.
relations	Array of Object	Specifies the item list of the resource relationship.

Table 10-12 resource parameters

Parameter	Type	Description
id	String	Specifies the resource ID.
name	String	Specifies the resource name.
provider	String	Specifies the cloud service name.
type	String	Specifies the cloud resource type.
region_id	String	Specifies the ID of the region where the resource is located.
project_id	String	Specifies the IAM project ID.
project_name	String	Specifies the IAM project name.
ep_id	String	Specifies the enterprise project ID.
ep_name	String	Specifies the enterprise project name.
checksum	String	Specifies the checksum.

Parameter	Type	Description
created	String	Specifies the time when the cloud resource was created. **created** is a UTC time in a fixed format complying with ISO-8601 (for example, **2018-11-14T08:59:14Z**).
updated	String	The time when the resource was last updated. **updated** is a UTC time in a fixed format complying with ISO-8601 (for example, **2018-11-14T08:59:14Z**).
provisioning_state	String	Specifies the result of an operation on resources. The value can be: • Succeeded: The operation is successful. • Failed: The operation fails. • Canceled: The operation is canceled. • Processing: The operation is in progress.
tags	Map	Specifies the cloud resource tags.
properties	Map	Specifies the cloud resource attributes.

Table 10-13 Relations parameters

Parameter	Type	Description
from_resource_id	String	Specifies the ID of the source resource.
to_resource_id	String	Specifies the ID of the associated resource.
from_resource_type	String	Specifies the type of the source resource.
to_resource_type	String	Specifies the type of the associated resource.
relation_type	String	Specifies the resource relationship type.

Resource Snapshot Storage Example


```
{
  "items": [
    {
      "resource": {
        "id": "c25ee8b3-c907-4cd4-9869-6c4b07c61a0b",
        "name": "rse-cdk-07-cdk-3sbz",
        "provider": "vpc",
        "type": "securityGroups",
        "region_id": "regionid1a",
        "project_id": "fc6d40abe7e54492b7c7aa5a29d6cbab",
        "project_name": "demo_project",
        "ep_id": "0",
        "ep_name": "default",
        "checksum": "4098715092c762b3eafe25be8eeda33a10b547033f9d59b6e18f5a960a1f805d",
        "updated": "2020-05-25T10:27:17.000Z",
        "created": "2020-05-25T10:27:17.000Z",
        "provisioning_state": "Succeeded",
        "tags": {},
        "properties": {}
      },
      "relations": [
        {
          "from_resource_id": "c25ee8b3-c907-4cd4-9869-6c4b07c61a0b",
          "to_resource_id": "0088a276-162b-4f07-aa40-f6ed8b801ca1",
          "from_resource_type": "vpc.securityGroups",
          "to_resource_type": "ecs.cloudservers",
          "relation_type": "isAssociatedWith"
        }
      ]
    }
  ],
  "snapshot_id": "6e40483d-5499-4440-a369-284e528f3d85",
  "snapshot_time": "2020-06-30T06:56:00.018Z"
}
```


10.3.2 Storage Model of Resource Change Notifications

Storage Model of Resource Change Notifications

Table 10-14 Storage model of resource change notifications

Parameter	Type	Description
notification_items	Array of Object	Resource change notifications.

Table 10-15 notification_items parameters

Parameter	Parameter Type	Description
notification_type	String	Notification type. For a resource change notification, the notification type is **ResourceChanged**.

Parameter	Parameter Type	Description
notification_creation_time	String	Notification sending time The notification sending time is a UTC time (such as 2018-11-14T08:59:14Z) that complies with ISO8601.
domain_id	String	Account ID.
detail	Object	Notification details.

Table 10-16 detail parameters

Parameter	Parameter Type	Description
resource_id	String	Resource ID.
resource_type	String	Resource type.
event_type	Enum	Event type (**CREATE**, **UPDATE**, **DELETE**)
capture_time	String	Event capture time. The event capture time is a UTC time (such as 2018-11-14T08:59:14Z) that complies with ISO8601.
resource	Object	Resource details.

Table 10-17 resource

Parameter	Type	Description
id	String	Resource ID.
name	String	Resource name.
provider	String	Service name.
type	String	Resource type.
region_id	String	The ID of the region where the resource resides.
project_id	String	IAM project ID.
project_name	String	IAM project name.
ep_id	String	Enterprise project ID.

Parameter	Type	Description
ep_name	String	Enterprise project name.
checksum	String	The checksum.
created	String	Resource creation time. The resource creation time is a UTC time (such as 2018-11-14T08:59:14Z) that complies with ISO8601.
updated	String	The time when the resource was last updated. The resource update time is a UTC time (such as 2018-11-14T08:59:14Z) that complies with ISO8601.
provisioning_state	String	Resource state.
tags	Map	Resource tags.
properties	Map	Resource attributes.

Example of Resource Change Notification Storage

```
{
   "notification_items": [
      {
         "detail": {
            "resource": {
               "id": "ea05ef41-8bd6-4a9c-af39-244e1ec448eb",
               "name": "as-group-test",
               "provider": "as",
               "type": "scalingGroups",
               "checksum": "",
               "region_id": "regionid1a",
               "project_id": "068d54ceca00d5302f70c00aaf6a471c",
               "project_name": "test",
               "ep_id": "0",
               "ep_name": "default"
            },
            "resource_id": "ea05ef41-8bd6-4a9c-af39-244e1ec448eb",
            "resource_type": "as.scalingGroups",
            "event_type": "DELETE",
            "capture_time": "2020-12-08T09:30:27.158Z"
         },
         "notification_type": "ResourceChanged",
         "notification_creation_time": "2020-12-08T09:30:27.272Z",
         "domain_id": "059b5c937100d3e40ff0c00a7675a0a0"
      }
   ]
}
```

10.4 ResourceQL Syntax

10.4.1 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 10-18 Supported data types

Type Name	Type
Integer	Int/Integer
Float	Float/Double
Boolean	Boolean
Array	Array
String	String
Dictionary	Object
Timestamp	Date

All your cloud resources are included in a table. The table name is fixed to **resources**. The resources under your aggregator account forms a table. The table name is fixed to **aggregator_resources**. Each row in the table records a piece of data. The conventions of each column are as follows.

Table 10-19 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.

aggregator_resources contains **domain_id** that indicates the account ID. The type of a domain ID is a string.

provider and **type** represent a unique resource. For different resources, **properties** varies. For example, for an ECS, the **provider** and **type** are **ecs** and **cloudservers**, and the **properties** contains **flavor**. For a VPC, the **provider** and **type** are **vpc** and **publicips**, and the **properties** contains **bandwidth**.

You can obtain resource attributes that can be included in the **properties** element for each resource on Config console or by calling the related API. For more details, see **How Can I Obtain Resource Attributes Reported to Config?**

properties supports nested queries. The following shows an example of how to query the **addresses** parameter under **properties** for the running ECS.

```
SELECT name, created, updated, properties.addresses FROM resources
    WHERE provider = 'ecs' AND type = 'cloudservers' AND properties.status = 'ACTIVE'
```

10.4.2 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
```

10.4.3 Functions

ResourceQL supports the following functions.

Table 10-20 Mathematical operation functions

Function	Description
abs(x)	Returns the absolute value of x.

Function	Description
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 10-21 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.

Function	Description
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 10-22 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.

Function	Description
array_join(x, delimiter[, null_replacement]) → string	Concatenates the elements of the given array using the delimiter and an optional string to replace nulls.
array_max/array_min(a)	Returns the maximum or minimum value of input array *a*.
array_position(a, element) → int	Returns the position of the first occurrence of the *element* in array *a* (or 0 if not found).
array_position(a, element, instance) → int	Returns the position of the first occurrence of the *element* in array *a*. If no matching element instance is found, **0** is returned. If *instance* > 0, returns the position of the *instance*-th occurrence of the *element* in array *a*. If *instance* < 0, return the position of the *instance*-to-last occurrence of the *element* in array *a*.
array_remove(a, element) → array	Removes all elements that equal *element* from array *a*.
array_sort(a) → array	Sorts and returns array *a*.
array_sort(array(T), function(<T, T>, int)) → array	Sorts and returns the *array* based on the given comparator *function*. The comparator will take two nullable arguments representing two nullable elements of the *array*. It returns **-1**, **0**, or **1** as the first nullable element is less than, equal to, or greater than the second nullable element.
array_sum(a)	Returns the sum of all non-null elements of *a*.
array_overlap(a, b) → boolean	Tests if arrays *a* and *b* have any non-null elements in common.
array_union(a, b) → array	Returns an array of the elements in the union of *a* and *b*, without duplicates.
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*.

Function	Description
concat(a1, a2, ...) → array	Concatenates the arrays *a1*, *a2*, ... This function provides the same functionality as the SQL-standard concatenation operator (||).
contains(a, element) → boolean	Returns true if the array *a* contains the *element*.
element_at(a, index)	Returns element of *a* at given *index*. If *index* < 0, element_at accesses elements from the last to the first.
filter(array(T), function(T, boolean)) → array(T)	Constructs an array from those elements of *array* for which *function* returns true.
none_match(array(T), function(T, boolean)) → boolean	Returns whether no elements of an array match the given predicate.
reverse(a) → array	Returns an array which has the reversed order of array *a*.
sequence(start, stop, step)	Generates a sequence of timestamps from *start* to *stop*, incrementing by *step*. It is similar to the range() function in Python, which returns a sequence of numbers, starting from 0 by default, and increments by 1 (by default), and stops before a specified number.
shuffle(a) → array	Generates a random permutation of given array *a*.
slice(a, start, length) → array	Subsets array *a* starting from index *start* (or starting from the end if *start* is negative) with a length of *length*.
transform(array(T), function(T, S)) → array(S)	Returns an array that is the result of applying *function* to each element of *array*.

Table 10-23 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.

Function	Description
avg(x) → double	Returns the average (arithmetic mean) of all input values.
bool_and/bool_or(x) → boolean	**bool_and** returns **TRUE** if every input value is **TRUE**, otherwise **FALSE**. **bool_or** returns **TRUE** if any input value is **TRUE**, otherwise **FALSE**.
coalesce(value1, value2, ...)	Returns the first non-null value in an argument list. Short-circuit evaluation will be used.
count(*)/count(x) → int	**count(*)** returns the number of input rows. **count(x)** returns the number of non-null input values.
greatest(value1, value2, ..., valueN)	Returns the largest of the provided values.
histogram(x) → map	Returns a map containing the count of the number of times each input value occurs.
least(value1, value2, ..., valueN)	Returns the smallest of the provided values.
max/min(x, n=1)	Returns *n* largest or smallest values of all input values of *x*.
max_by/min_by(x, y, n=1)	Returns *n* values of *x* associated with the *n* largest of all input values of *y* in descending order of *y*, or return *n* values of *x* associated with the *n* smallest of all input values of *y* in ascending order of *y*.
geometric_mean(x) → double	Returns the geometric mean of all input values.
set_agg(x) → array	Returns an array created from the distinct input *x* elements.
set_union(x) → array	Returns an array of all the distinct values contained in each array of the input.
sum(x)	Returns the sum of all input values.
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 10-24 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**.

11 FAQs

11.1 Resource List

Why Can't I Delete Resources on the Resource List Page?

On the **Resource List** page, you can only view resources and export resource details. To delete a resource, you need to click **View Details** in the **Operation** column to go to the corresponding service page.

Why Does Resource Information Remain Unchanged on the Resource List Page After a Change Has Been Made to My Resources?

One possible reason is that there was a delay in synchronizing related resource information to Config.

Another reason may be the disabled resource recorder. If the resource recorder was disabled, Config would not update resource data. If the resource recorder is enabled, Config will update related data for resources that are included in the monitoring scope within 24 hours.

It may also be that the resource change was not reported to Config. The services are not supposed to report all resource data to Config, just some of it. For example, IAM is not supposed to report secret access keys (SKs) to Config, and Config will not display SK data.

11.2 Resource Compliance

How Many Rules Can I Add?

You can add up to 500 rules in an account.

What is the Configure Rule Parameters for When I Add a Rule?

Parameters for **Configure Rule Parameters** vary depending on the policy selected. For example, if you select the predefined policy, **required-tag-check**, you will need to specify a key and value pair for **Configure Rule Parameters**.

For a predefined policy, the parameters that you need to configure for **Configure Rule Parameters** are also predefined. You can set different values as needed.

Why There Are No Related Evaluation Results After I Add iam-password-policy and iam-user-mfa-enabled Policies?

Config evaluates all resources on the resource list Page. Check whether related resources are displayed on the resource list page. If not, check whether the resource recorder has been enabled. The resource recorder must be enabled before Config can evaluate any resources for you. For resources that are not recorded, disable corresponding rules to avoid being confused and avoid unnecessary expenditures.

11.3 Resource Recorder

Are Resource Snapshots and Resource Change Notifications Stored into the Same OBS Bucket?

Yes, they are stored into the same OBS bucket.

If you specified an OBS bucket and an SMN topic when you configured the resource recorder, resource snapshots and resource change notifications are periodically stored in the OBS bucket.

How Often Are Resource Snapshots and Resource Change Notifications Stored, Respectively?

After you enable the resource recorder and specify an SMN topic and an OBS bucket, Config will store your resource snapshots to the OBS bucket every 24 hours and your resource change notifications every 6 hours.

Do I Need to Configure Both Topic and Resource Dump When I Enable and Configure the Resource Recorder?

No. However, you need to configure either **Topic** or **Resource Dump**. To enable the resource recorder, you must configure either an SMN topic or an OBS bucket.

Why Are There No Notifications of Resource Changes Even When the Resource Recorder Has Been Enabled?

The possible causes are as follows:

- You didn't specify an SMN topic when you configured the resource recorder. To receive resource change notifications, modify the resource recorder to configure an SMN topic.
- You did not add subscriptions or request subscription confirmations for the specified SMN topic. For details, see the *Simple Message Notification User Guide*.
- Resource changes were not reported to Config.
- There was a delay in synchronizing or sending the notification.

Why Are Resource Change Notifications Not Stored into the Configured OBS Bucket?

To store resource change notifications, you need to configure both an SMN topic and an OBS bucket.

To make an SMN topic effective, you not only need to create a topic, but add subscription endpoints and request subscription confirmation.

Why Do I Receive a Notification When I Did Nothing with a Resource?

If you have specified an effective SMN topic when you enabled the resource recorder, Config will send notifications of resource changes that are resulted from both user operations and non-user operations. For more details, see **Notifications**. You are advised to use HTTPS instead of SMS messages or emails to receive notifications from Config.

How Can I Obtain Resource Attributes Reported to Config?

You can obtain resource attributes reported to Config in either of the following ways:

- Go to Config console and open the **Query Editor**. Resource attributes that are reported to Config are displayed on the left side of the **Query Editor**. The following procedure shows how to open the **Query Editor**.
  a. Log in to the management console.
  b. Click  in the upper left corner of the page. In the service list that is displayed, under **Management & Deployment**, select **Config**.
  c. In the navigation pane on the left, choose **Advanced Queries**.
  d. On the **Default Queries** tab, click **Query** in the **Operation** column of any rows.
  e. View resource attributes on the left side of the **Query Editor**. You can also enter a resource type to search for resource attributes.
- Alternatively, you can call the the querying schema API (GET /v1/resource-manager/domains/{domain_id}/schemas) to obtain resource attributes. In the response, the **type** field indicates the resource type, and the **schema** field indicates resource attributes that are reported to Config. For more details, see *Config API Reference*.

Why Is an Error Reported When Data Is Dumped to the OBS Bucket After the Resource Recorder Is Enabled?

If the message "Failed to write the ConfigWritabilityCheckFile file to the OBS bucket because the OBS bucket or the IAM agency is invalid" is displayed, the possible reasons are as follows:

1. The IAM agency assigned to the resource recorder does not contain the permission, **obs:object:PutObject**.
2. If an OBS bucket from the current account was used, the reason may be that the bucket policy explicitly denies the **PutObject** action from the IAM agency. If an OBS bucket from another account was used, the reason may be that the

bucket policy does not explicitly allow the **PutObject** action from the IAM agency. For more details, see **Cross-Account Authorization**. .

3. You used an encrypted OBS bucket, but the agency assigned to the resource recorder did not contain related KMS permissions. For more details, see **Storing Resource Change Notifications and Resource Snapshots to an Encrypted OBS Bucket**.

12 Change History

Released On	Description
2024-10-30	This issue is the first official release.