

Config

Service Overview

Issue 01
Date 2023-10-25



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

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

Trademarks and Permissions



HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process*. For details about this process, visit the following web page:

<https://www.huawei.com/en/psirt/vul-response-process>

For vulnerability information, enterprise customers can visit the following web page:

<https://securitybulletin.huawei.com/enterprise/en/security-advisory>

Contents

1 What Is Config?	1
2 Function Overview	3
3 Billing	7
4 Permissions	8
5 Basic Concepts	14
6 Relationships with Other Services	16
7 Constraints and Limitations	18

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, Config may fail to aggregate resource data, collect resource data, and accurately evaluate your resources. For details about how to enable and configure the resource recorder, see [Configuring the Resource Recorder](#).

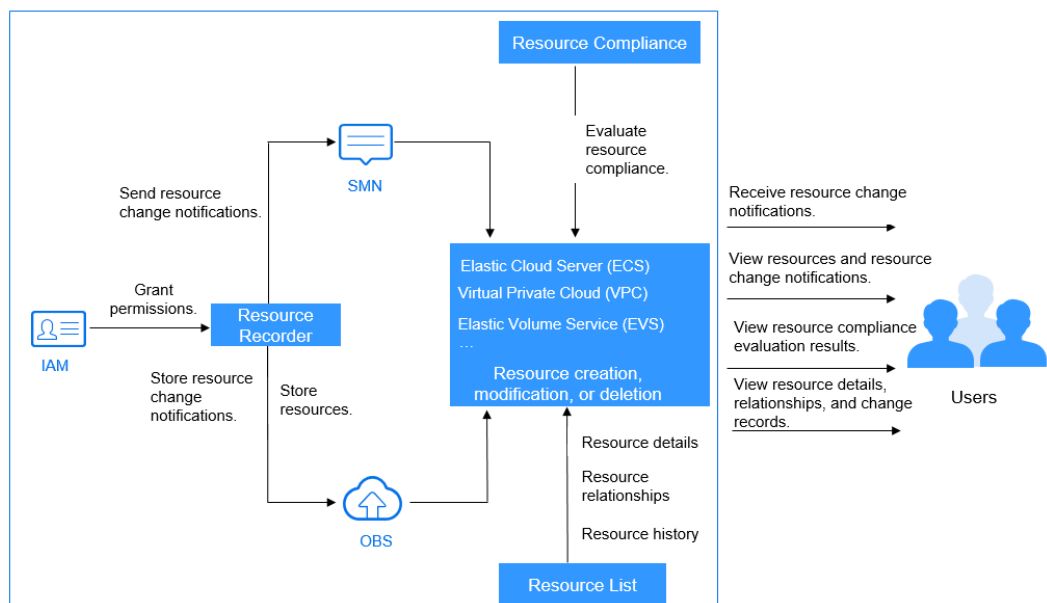
Architecture

Config provides you with resource information, such as resource inventory, details, relationships, and change records. It stores your resources every 24 hours and 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.
- **Displaying resource change records:** You can enable and configure the resource recorder to monitor resource changes continuously.
- **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 information:** Config will store your resource change information 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 against the rules to check whether they are compliant or not.
- **Advanced query:** You can create a custom query using ResourceQL syntax to query 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 these 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.

Figure 1-1 Config architecture



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. Sign in to the **management console**, click  in the upper left corner, and choose **Management & Governance > 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 **API Reference**.

2 Function Overview

Table 2-1 lists the common functions of Config.

Basic concepts help you better understand Config features.

Table 2-1 Common functions

Category	Function	Description
Resource list	Querying all resources	View all resources from the current account. Resource information, such as the resource name, region, service, resource type, and enterprise project, is displayed
	Querying details about a resource	You can query resource details from the current account, such as the resource name, creation time, and specifications.
	Filtering resources	You can set a filter criterion (resource name, resource ID, tag, or enterprise project) to quickly find out required 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.

Category	Function	Description
Resource Compliance	Adding a rule	You can add a rule to evaluate the compliance of your resources. You can set the compliance policy type and rule parameters.
	Evaluating resource compliance	You can click Evaluate in the Operation column to start the evaluation after a rule is added.
	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	You can click More > Modify in the Operation column to modify a rule as needed.
	Deleting a rule	You can delete a rule which is no longer used.
	Organization rules	If you are an organization administrator or a delegated administrator of Config, you can add organization rules, and this rule will apply to all member accounts in your organization.
Resource Recorder	Enabling the resource recorder	You can track resource changes only after the resource recorder is enabled.
	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 configurations of the resource recorder, such as the monitoring scope, notification topic, and data storage path.
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.

Category	Function	Description
	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 the conformance data in the rule list.
	Viewing aggregated resources	You can view all resources aggregated by the resource aggregator.
	Authorizing an aggregator account	Source accounts authorizes the aggregator account to collect resource configurations and compliance data from source accounts.
	Applying advanced queries to aggregators	Resource aggregation supports advanced queries. You can use ResourceQL to query configuration states of one or multiple aggregator account.
Conformance package	Creating conformance packages	You can use sample or custom templates to create and manage rules.
	Viewing conformance packages	You can view lists and details of conformance packages created.
	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.

Category	Function	Description
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.

3 Billing

If you configure a resource recorder, the Simple Message Notification (SMN) resources or Object Storage Service (OBS) buckets used by the resource recorder will be charged. For details, see [Billing](#) for SMN and [Billing](#) for OBS.

If you configure user-defined compliance rules, FunctionGraph used by the user-defined compliance rules will be charged. For details, see [Billing Overview](#).

After Config is put into commercial use, you will be charged based on the number of resource changes recorded by the resource recorder and the number of rule executions.

Config will continue to be free for 2024. If it is billed later, we will notify you in advance.

4 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 Huawei Cloudaccount does not need individual IAM users for permissions management, skip this chapter.

IAM can be used free of charge. You pay only for the resources in your account. For more details, see [IAM Service Overview](#).

Config Permissions

By default, new IAM users do not have permissions. You need to add a user to one or more groups and attach permissions policies or roles to these 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. Your access will not be affected across different regions. So, users with related permissions can access Config and other global services in all regions.

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

- **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 4-1 lists all the system-defined permissions supported by Config.

Table 4-1 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
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 **RMSConsoleFullAccess** 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 4-2 lists the common operations and the system-defined permissions of Config. ✓ indicates that an operation is supported, and × indicates not supported.

Table 4-2 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	√	√	√
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	√	√	√

Operation	RMS ConsoleFullAccess	RMS FullAccess	RMS ReadOnlyAccess
Deleting organization rules	√	√	x
Viewing resource compliance evaluation results	√	√	√
Triggering a resource compliance evaluation	√	√	x
Updating compliance evaluation results	√	√	x
Running advanced queries	√	√	x
Creating advanced queries	√	√	x
Querying advanced queries	√	√	√
Listing advanced queries	√	√	√
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	√	√	√

Operation	RMS ConsoleFullAccess	RMS FullAccess	RMS ReadOnlyAccess
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
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

Operation	RMS ConsoleFullAccess	RMS FullAccess	RMS ReadOnlyAccess
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

5 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).

For details about supported resources and regions, see [Services and Regions Supported by Config](#).

Resource Relationship

A resource relationship indicates how your resources on the cloud platform are associated, for example, EVS disks attached to ECSs and ECSs contained in VPCs.

For details, see [Relationships with Supported Resources](#).

Resource Change Records

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

A record will be generated upon any property or relationship changes to a resource.

You can query the resource change records on the management console or by calling APIs.

Resource Recorder

The resource recorder tracks resource changes on the cloud platform. When a resource is created, modified, or deleted, or the resource relationship changes, an SMN message will be sent to notify you of the change. In addition, the resource change notifications and resource snapshots will be periodically stored into the configured OBS bucket.

Resource Compliance

You can add a rule to evaluate the compliance of your resources.

Advanced Query

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 these resource data.

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.

6 Relationships with Other Services

The following describes the relationships between Config and other services.

Table 6-1 Relationships between Config and other services

Service	Description	Function	Related Operation
SMN	You need to specify an SMN topic when you enable the resource recorder.	You will receive a notification if a change is made to your resource.	Configuring the Resource Recorder
OBS	You need to specify an OBS bucket when you enable the resource recorder.	<ul style="list-style-type: none"> 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. 	
IAM	Required agencies need to be assigned using IAM for configuring the resource recorder.	The agencies must contain the permissions for sending notifications with SMN topics and storing data into an OBS bucket.	
CTS	N/A	With CTS, you can record operations for Config for later query, audit, and backtrack.	Recording Config Operations in CTS

Service	Description	Function	Related Operation
FunctionGraph	N/A	You can use a FunctionGraph function configured for a custom policy to evaluate resource compliance.	Custom Policies
Resource Formation Service (RFS)	-	Conformance packages are created with RFS stacks. You cannot separately delete rules of a conformance package created with RFS stacks.	Conformance packages
Cloud Eye (CES)	-	Event monitoring allows you to query events and receive alarms when there are unexpected events. With event monitoring, resource compliance events are reported to Cloud Eye and alarms are generated when exceptional events occur.	Event Monitoring

7 Constraints and Limitations

The constraints on Config are as follows:

Table 7-1 Constraints and limitations on Config

Description	Limit
Retention duration of resource snapshots	24 hours
Retention duration of resource change messages	6 hours
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

Description	Limit
Maximum number of advanced queries in an account	200
Number of results returned for each advanced query	4,000
Retention period of resource configuration information	7 years

NOTICE

To get full functionality of Config, you need to enable the resource recorder. If the resource recorder is disabled, Config may fail to aggregate resource data, collect resource data, and accurately evaluate your resources. For details about how to enable and configure the resource recorder, see [Configuring the Resource Recorder](#).
