Config

Getting Started

 Issue
 01

 Date
 2024-09-30





HUAWEI TECHNOLOGIES CO., LTD.

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

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

Trademarks and Permissions

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

Contents

1 Enabling the Resource Recorder	. 1
2 Filtering Resources	.4
3 Evaluating Resource Compliance	.8

1 Enabling the Resource Recorder

Scenarios

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

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.

This section describes how to enable and configure the resource recorder.

Preparations

- 1. If you already have a Huawei account, skip this step. If you do not have one, follow the following steps to create one:
 - a. Go to Huawei Cloud and click Sign Up.
 - b. Sign up for a Huawei account and enable Huawei Cloud services.

After your account is created, you will be directed to your personal information page.

- c. Complete real-name authentication by following the instructions in Individual Real-Name Authentication or Enterprise Real-Name Authentication.
- 2. Topping Up Your Account

Config is free of charge, but the SMN topic and the OBS bucket that you configured for the resource recorder will be charged. For details, see **SMN billing** and **OBS billing**.

Ensure your account has sufficient balance to avoid unavailability of the resource recorder and other functions of Config. For more details, see **Topping up an Account**.

Procedure

The following steps only involve mandatory parameters. For other parameters, you can keep the default configurations. For more details, see **Configuring the Resource Recorder**.

- **Step 1** Log in to the management console.
- **Step 2** Click in the upper left corner of the page. In the service list that is displayed, under **Management & Governance**, select **Config**.
- **Step 3** In the navigation pane on the left, choose **Resource Recorder**.
- **Step 4** Toggle on the resource recorder and in the displayed dialog box, click **OK**.

Config	Resource Recorder
Resource List Resource Compliance Conformance Packages	Resource Recorder Resource changes, helping you automate monitoring of massive resources.
Resource Recorder	×
Advanced Queries	Enable Resource Recorder
Resource Aggregation 🛛 🗸	After the resource recorder is enabled, it can record changes to your resource configurations, and you can disable it at any time. Are you sure you want to enable the resource recorder?

Step 5 Specify an OBS bucket.

Resource Dump		
When data dump is enabled, resource cha	ange information is saved to the specified	OBS bucket.
Your bucket Other users' bucket	ket	
bucket-example002 V (Opti	ional) Folder prefix	Q Create OBS Bucket

Select an OBS bucket from the current account or another account to store resource change messages and snapshots.

If there are no OBS buckets in the current account, create one first. For details, see **Creating a Bucket**.

Step 6 Configure an SMN topic.

Торіс				
Resource	changes and notifications can	be transmitted to an SMN topic. If you configure	an email address as the no	tification endpoint of an SMN topic, a large number of emails will be generated.
Your to	ic v	Q v	as-test-msg v	Q. Create Topic 🖻

Toggle on the SMN topic, select Your topic, and select a region and an SMN topic.

If there are no SMN topics available in the current account, create one first. For details, see **Creating a Topic**.

NOTE

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

Step 7 Grant permissions.

Grant Permissions

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

Quick granting

Quick granting will automatically create an agency named rms_tracker_agency to grant the required permissions for the resource recorder to work properly. The agency contains permissions, including the SMN Administrator for sending notifications and the OBS OperateAccess permission for writing data into an OBS bucket.

Custom granting

- Step 8 Click Save.
- Step 9 In the displayed dialog box, click OK.

----End

Related Information

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

- When configuring the resource recorder, if you select an OBS bucket or SMN topic from another account, you need to be authorized by the account. For details, see **Cross-Account Authorization**.
- If you select Custom granting to customize authorization for the resource recorder, you need to create an agency with IAM, and the agency must include either the permissions for sending notifications using an SMN topic or the permissions for writing data into an OBS bucket based on related configurations. To store resource changes and snapshots to an encrypted OBS bucket, you need the KMS Administrator permission. For details, see Storing Resource Change Notifications and Resource Snapshots to an Encrypted OBS Bucket. For details about how to create an agency, see .

2 Filtering Resources

Scenario

This section describes how to filter resources on the Config console. You can get details about resources, such as the region and state.

NOTE

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.

There is a delay in synchronizing 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.

Preparations

- 1. If you already have a Huawei account, skip this step. If you do not have one, follow the following steps to create one:
 - a. Go to Huawei Cloud and click Sign Up.
 - b. Sign up for a Huawei account and enable Huawei Cloud services.

After your account is created, you will be directed to your personal information page.

- c. Complete real-name authentication by following the instructions in Individual Real-Name Authentication or Enterprise Real-Name Authentication.
- 2. Topping Up Your Account

Config is free of charge, but the SMN topic and the OBS bucket that you configured for the resource recorder will be charged. For details, see **SMN billing** and **OBS billing**.

Ensure your account has sufficient balance to avoid unavailability of the resource recorder and other functions of Config. For more details, see **Topping up an Account**.

3. Enabling the Resource Recorder

To use the resource list, the resource recorder must be enabled.

Procedure

Step 1 Log in to the management console.

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

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

source List							G Feedbac
 Resource List m To view your res After you add, up Data will not be If no data is available 	any not list all of your resources. Supported Ser sources and their billing details, go to Billing Cer pdate, or delete resources, there is some delay updated for resources that are not recorded by liable, check whether the resource recorder is al	rices and Regions ther ⁽²⁾ before the changes are displayed. Please the resource recorder. ready enabled or whether your resources	check again later. are within the monitoring scope of the resou	rce recorder. You can also go to manage	ment console to view your resources.		
Only display	cloud services and regions that contain resource	es 💩 Supported Services and Regions					
Service	All (1,012)	Virtual Private Cloud (VPC) (315)	Identity and Access Managem (150)	Application O&M Management (124)	Log Tank Service (LTS) (78)	Elastic Load Balance (ELB) (42)	
	Cloud Backup and Recovery ((35)	Domain Name Service (DNS) (28)	Data Encryption Workshop (D (26)	Image Management Service (I (23)	VPC Endpoint (23)	Object Storage Service (OBS) (22)	
	Resource Formation Service (19)	Config (16)	Elastic Volume Service (EVS) (15)	Cloud Eye Service (15)	Simple Message Notification ((15)	Host Security Service (14)	
	FunctionGraph (11)	Elastic Cloud Server (ECS) (7)	Cloud Trace Service (CTS) (5)	EventGrid (5)	Enterprise Router (ER) (5)	Cloud Container Engine (CCE) (4)	
	Cloud Container Instance (CCI) (3)	Auto Scaling (AS) (2)	NAT Gateway (2)	Key Pair Service (KPS) (2)	Content Delivery Network (CDN) (1)	Application Service Mesh (1)	
	CodeArts Pipeline (1)	Direct Connect (1)	CodeArts (1)	ModelArts (1)			
Region	All	CN North-Beijing4 (224)	CN North-Ulangab1 (44)	CN East-Shanghai1 (280)	CN East-Qingdao (7)	CN East2 (6)	
	CN South-Guangzhou (112)	CN South-Guangzhou-Invitati (30)	CN Southwest-Gulyang1 (26)	CN-Hong Kong (13)	AP-Bangkok (10)	AP-Singapore (26)	
	AP-Jakarta (6)	ME-Riyadh (5)	AF-Cairo (5)	AF-Johannesburg (8)	TR-Istanbul (7)	LA-Mexico City1 (8)	
	LA-Mexico City2 (5)	LA-Sao Paulo1 (7)	LA-Santiago (5)				
Selected	Service: All	Region: All					
Export Resource	Info						
Q Search by nam	ne by default.						00
Name	Region	Resource status	Service	Resource Type	Enterprise Project	Operation	
CCE.	61e5-8 CN East-Shanghai1	O In use	Application O&M Manag	ement alarmRule	default	View Details	

Step 3 Set filters (service, resource type, and region) to search for resources. For global services, you do not need to set the region.

Resource List							G Feedback
 Resource List ma To view your reso After you add, upi Data will not be u If no data is available 	y not list all of your resources. Supported Serv- urces and their billing details, go to Billing Cer date, or delete resources, there is some delay I pdated for resources that are not recorded by t able, check whether the resource recorder is all	vices and Regions ther C before the changes are displayed. Please ch he resource recorder. ready enabled or whether your resources ar	neck again later. re within the monitoring scope of the resou	rce recorder. You can also go to manage	ment console to view your resources.		
Only display cl	loud services and regions that contain resource	es 🙆 Supported Services and Regions					
Service	All (1,012) Cloud Backup and Recovery ((35) Resource Formation Service (19) FunctionGraph (11) Cloud Container Instance (CCI) (3) CodeArts Pipeline (1)	Virtual Private Cloud (VPC) (315) Domain Name Service (DNS) (28) Config (16) Elastic Cloud Server (ECS) (7) Auto Scaling (AS) (2) Direct Connect (1)	Identity and Access Managem (150) Data Encryption Workshop (D (26) Elastic Volume Service (EVS) (15) Cloud Trace Service (CTS) (5) NAT Gateway (2) CodeArts (1)	Application 0.8M Management (124) Image Management Service (1 (23) Cloud Eye Service (15) EventGrid (5) Key Pair Service (KPS) (2) ModelArts (1)	Log Tank Service (LTS) (78) VPC Endpoint (23) Simple Message Notification ((15) Enterprise Router (ER) (5) Content Delivery Network (CDN) (1)	Elastic Load Balance (ELB) (42) Object Storage Service (OBS) (22) Host Security Service (14) Cloud Container Engine (CCE) (4) Application Service Mesh (1)	
Resource Type	Vaults (13)	Backup (3)	Policy (19)				
Selected	Service: Cloud Backup and Recovery (C	BR) Resource Type: Vaults	Region: CN North-Beijing4	CN Soun-Guangzhoù (3)	CN Sournvest-Gulyang1 (2)	ER-Mexico City2 (1)	
Export Resource In	fo Go to Console						0
Name	Region	Resource status	Service	Resource Type	Enterprise Project	Operation	
vault-4a2c 2245/5ed-f249-4173	-a7b8-76a06e2 CN North-Beijing4	O In use	Cloud Backup and Reco	very (CBR) Vaults	default	View Details	
vault-644c	CN North-Beijing4	O In use	Cloud Backup and Reco	very (CBR) Vaults	default	View Details	

Step 4 In the search box in the middle of the page, set more refined filters to narrow down the search scope.

Resource List							G Feedback
 Resource List To view your re After you add, Data will not b If no data is av 	t may not list all of your resources. Supported Se resources and their billing details, go to Billing Cr. I, update, or delete resources, there is some delay be updated for resources that are not recorded by wailable, check whether the resource recorder is :	Invices and Regions Inter (2) y before the changes are displayed. Please the resource recorder, already enabled or whether your resources	check again later. are within the monitoring scope of the resou	rce recorder. You can also go to manage	ment console to view your resources.		
Only displa	ay cloud services and regions that contain resour	ces 💩 Supported Services and Regions					
Service API Filtern Name Resou Resourc Regio Select Resourc 1	At (1,912) Could Backgrand Recovery ((54) Resource Formation Service (19) Function/Graph (11) Chine Container Instance (CD) (2) (7) (1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Virbuil Private Cloud (VPC) (315) Domain Name Service (IDNS) (28) Config (16) Elastic Cloud Server (ECS) (7) Aufs Scaling (AS) (2) Direct Connect (1) Backup (2) Resource Type: Vaults	Identity and Access Managem (150) Data Encrystein Werkheite (Dr (28) Ellinite Volume Service (CTS) (5) NAT Gaterway (2) CodeArts (1) Policy (19) Region: All	Application OLM Management (124) Image Management Service ((.23) Colude Eye Benvice (15) EventCold (5) Key Par Service (0PS) (2) Model/Afts (1)	Log Tank Service (LTS) (78) VPC Endpoint (23) Simple Message Notification ((15) Enterprise Router (ER) (5) Content Delivery Network (CDN) (1)	Elastic Lead Balance (ELB) (42) Object Glorage Service (OBS) (22) Host Security Service (14) Cloud Container Engine (CCE) (4) Application Service Mesh (1)	
E 11 Q Search by na	ame by default.	Resource status	Service	Resource Type	Enterprise Project	Operation	00
vault-1841 0399d5	7-04963d	 In use 	Cloud Backup and Rect	overy (CBR) Vaults	default	View Details	

Filter	Description			
Name	Resource name. Fuzzy search is supported. The resource name is case-insensitive.			
Resource ID	Resource ID. Fuzzy search is supported. The resource ID is case-sensitive.			
Resource status	Resource status. Possible resource states include: • In use: A resource is being used.			
	• Deleted : A resource has been deleted.			
Tag	Resource tag. 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.			

----End

Related Information

The resource list allows you to perform the following operations on your resources:

- Querying details about a resource
- Exporting resources
- Checking resource compliance
- Learning about resource relationships
- Viewing resource changes

Config also provides the following advanced features for you to query resources in a more refined manner and aggregate resource data from other accounts.

- Advanced Queries
- Resource Aggregation

3 Evaluating Resource Compliance

Scenario

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

This section uses the built-in policy, **Last Login Check** as an example to describe how to detect inactive IAM users. This policy can help reduce idle users and password leakage risks for enhanced account security.

Preparations

- 1. If you already have a Huawei account, skip this step. If you do not have one, follow the following steps to create one:
 - a. Go to Huawei Cloud and click Sign Up.
 - b. Sign up for a Huawei account and enable Huawei Cloud services.

After your account is created, you will be directed to your personal information page.

- c. Complete real-name authentication by following the instructions in Individual Real-Name Authentication or Enterprise Real-Name Authentication.
- 2. Topping Up Your Account

Config is free of charge, but the SMN topic and the OBS bucket that you configured for the resource recorder will be charged. For details, see **SMN billing** and **OBS billing**.

Ensure your account has sufficient balance to avoid unavailability of the resource recorder and other functions of Config. For more details, see **Topping up an Account**.

3. Enabling the Resource Recorder

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. In addition, only resources within the monitoring scope of the resource recorder can be evaluated by Config rules, so you are advised to select all your resources when you configure the resource recorder.

Step 1: Add a Rule

The following procedure involves specific parameters for the example rule. Other rules may contain different parameters. For more details, see **Adding a Rule with a Predefined Policy**.

- **Step 1** Log in to the management console.
- **Step 2** Click in the upper left corner of the page. In the service list that is displayed, under **Management & Governance**, select **Config**.
- **Step 3** In the navigation pane on the left, choose **Resource Compliance**.
- **Step 4** On the **Rules** tab, click **Add Rule**.

Config	Resource Compliance								Feedback
Resource List Resource Compliance Conformance Packages	Only resources displayed on the After a rule is configured, Config Only supported resources are ended.	Resources List page can be evalu will send detailed information of ev valuated or aggregated.	ated. vents to Cloud Eye. To view events or	configure alarms, visit Event Monit	toring on Cloud Eye console.				×
Resource Recorder Advanced Queries Resource Aggregation V	Resource Compliance Overview 14 Total Rules	12 Non-Compliant Rules	67 Non-Compliant Resource	s					
	Rules Organization Rule Add Rule	s Non-Compliant Resou eyword. Status ⑦ 0	rces Policy Type ⊖	Trigger Type $ \Theta $	Region O	Evaluation Result 💿 🕏	Description \varTheta	Operation	0
	access-keys-rotated 652 5ee3	O Enabled	Bult-in policy	Periodic execution	-	Non-compliant (8)		Evaluate Disable Rule	More ~

Step 5 On the Basic Configurations page, select iam-user-last-login-check and click Next.

< Add Rule				
Basic Configurations	Configure Rule Parameters	— (3) Confirm		
Policy Type	Built-in policy Quickly add a rule based on a buil	t-in policy.	ustom policy di rule based on a custom policy.	
Built-in Policy	Q Policy Name: iam-user-last-login-chec	\mathbf{k} × Add filter		×
	Policy Name	Тад	Resource Type	Description
	iam-user-last-login-check	lam	Identity and Access Management-Users	An IAM user is noncompliant if it has never signed in within the allowed number of days.
Rule Name	iam-user-last-login-check			
Description	An IAM user is noncompliant if it has never number of days.	signed in within the allowed		
		4		

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

< Add Rule				
O Basic Configurations 2 Configurations	re Rule Parameters (3) Con	ពីកា		
* Trigger Type	Configuration change	dic execution		
* Execute Every * Resource Scope	24 hours > All >			
Configure Rule Parameters	Parameter allowedinactivePeriod	Description Maximum number of days without login.	Value 90	
Tag	TMS's predefined tags are recommende + Add Tag You can add 20 more tags.	d for adding the same tag to different cloud resources. Create p	redefined tags 🕜 📿	
				Previous

Parameter	Example	Description
Execute Every	24 hours	How often a rule will be triggered.
		The rule will be periodically triggered at the configured frequency.
		Available options: 1 hour , 3 hours , 6 hours , 12 hours , 24 hours .
Resource	All	The region where your resources are deployed.
Scope		Only resources in the specified region will be evaluated.
Configure Rule Parameters	90	Number of days during which an IAM user has not logged in the system. The default value is 90 .
		If an IAM user does not log in to the system within the specified period of time, this user is noncompliant.

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

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

----End

Step 2: View evaluation results.

Step 1 On the **Rules** tab of the **Resource Compliance** page, click the name of the rule that was added in **Step 1**.

Resource Compliance											
Only resources displayed on the Resources List page can be evaluated. After a rule is configured. Config will send detailed information of events to Cloud Eye. To view events or configure alarms, visit Event Monitoring on Cloud Eye console. Only supported resources are evaluated or appreciated.											
Resource Compliance Overview 14 Total Rules	Den 12 Non-Compliant Rules	67 Non-Compliant Resources									
Rules Organization Rule	es Non-Compliant Resourc	ces									
Rule Name: iam-user-last-l	ogin-check × Add filter Status ⑦ ⊕	Policy Type \varTheta	Trigger Type	Region 🖯	Evaluation Result 💿 🔶	Description 🖯	Operation	×Q®			
iam-user-last-login-check 670c7 560e24	O Enabled	Built-in policy	Periodic execution	All	Non-compliant (49)	-	Evaluate Disable Ri	ule More v			

Step 2 View evaluation results and rule details on the **Basic Information** tab.

< iam-user-l	last-login-che	ck	¥		(Evaluate) (Modity) (Disable Rule) Delots					
Basic Information	Remeulan	n management	Tay							
Evaluation Re	esults						Enabled	Non-Compliant Resources 49		
Q Evaluation Result. Non-compilant × Add Illior × Q 🛞										
Resource Nam	rce Name/ID Evaluation Result Region		Region	Service Resource Type		Last Evaluated	Rule Name	lam-user-last-login-check		
z O	ec7ab3	Non-compliant	-	Identity and Access Managem	Users	Oct 14, 2024 09:36:10 GMT+	Policy Type	Built-in policy		
h 0	372c5e	Non-compliant		Identity and Access Managem	Users	Oct 14, 2024 09:38:10 GMT+	Created	Oct 14, 2024 09:36:09 GMT+08:00		
р 1	d42a86	Non-compliant	-	Identity and Access Managem	Users	Oct 14, 2024 09:36:10 GMT+	Trigger			
v 1	e1d912	Non-compliant	-	Identity and Access Managem	Users	Oct 14, 2024 09:36:10 GMT+	Trigger Type	Periodic execution		
h 1	7b5ae9	Non-compliant	-	Identity and Access Managem	Users	Oct 14, 2024 09:36:10 GMT+	Execute Every Execute Every	y 24 hours		
с 2	ca9e5fc	Non-compliant		Identity and Access Managem	Users	Oct 14, 2024 09:36:10 GMT+	Configure Rul	le Parameters		
X	7fce752	Non-compliant	-	Identity and Access Managem	Users	Oct 14, 2024 09:36:10 GMT+	Configure R	anowedinactive/enod: 90		

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.

IAM users that do not log in to the management console within 90 days are listed as noncompliant users. You can make adjustments on these users as needed.

----End

Related Information

Config also provides the following features to meet your requirements of resource compliance audit:

- **Custom rules**: You can create custom rules with FunctionGraph if built-in policies cannot meet your resource audit requirements.
- **Organization rules**: 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.
- **Conformance packages**: 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.