

Config

Operation Guide

Product Documentation



Copyright Notice

©2013–2026 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by the Tencent corporate group, including its parent, subsidiaries and affiliated companies, as the case may be. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

Operation Guide

Resources

Viewing Resource List

Viewing Resource Details

Rule

Managed Rules

List of Managed Rule

MFA on Sensitive Operations Required for CAM Users

MFA on Login Required for CAM Users

No Idle User Groups on CAM

Association with User Group Required for CAM User

No Authorization Policies Directly Added to CAM Sub-account

No Administrator Access Permissions Granted to CAM Users, User Groups, or Roles

Granting of Specific High-Risk Permissions by CAM Not Allowed

No Idle Permission Policies on CAM

CAM Login Permission Check

Key of CAM User Rotated at Specified Interval

Login by CAM User within Specified Time Range

CVM Instance Associated with Specified Security Group

CVM Instance Not Moved to Recycle Bin

Association of CVM Instance with Specified Role

CVM Instance Enabled Automatic Renewal

Expiration Notification for CVM Instance Prepayment and Pay-As-You-Go Payment

No Idle Security Groups

CVM Instance in VPC

No CVM Instances Not Assigned to Project

Inactive Duration of CVM Instance After Shutdown Not Exceeding Specified Number of Days

Lease Duration of CVM Instance Meeting Requirement of Specified Number of Days

CVM Instance Bound to IPv4 Public Address

Specified Tag Existed for Resource

Access to Remote Risky Ports by Security Group Not Allowed

Access to All Ports by Security Group Not Allowed

CBS Disk Enabled Arrear Protection

CBS Disk Enabled Encryption

Detachable CBS Disk Not Moved to Recycle Bin

- Number of Available IP Addresses in VPC Subnet Greater than Specified Value
- Expiration Protection for CVM Instance in Pay-As-You-Go Mode
- No Idle CBS Disks

Using Rules

- Creating Managed Rules

Managing Rules

- Viewing Rule List
- Viewing Rule Details
- Editing Rule
- Enabling/Disabling Rule
- Deleting Rule
- Evaluating Rule
- Viewing Rule Evaluation Results

Conformance Pack

- Supported Conformance Pack Template

Managing Conformance Packs

- Viewing Conformance Pack List
- Viewing Conformance Pack Details
- Creating Conformance Pack
- Editing Conformance Pack
- Adding/Removing Rule
- Deleting Rule
- Deleting Conformance Pack
- Evaluating Conformance Pack
- Viewing Conformance Pack Evaluation Results

Settings

- Monitoring Management
- Delivery Service
- Resource Snapshot Update

Operation Guide

Resources

Viewing Resource List

Last updated: 2024-03-04 14:13:25

1. You can log in to the [Config console](#), and click **Resource** in the left sidebar to view the latest resource list updated by Config.

During beta, Config displays the resource data and resource timeline of the last year by default. If you need to view the data for a longer period of time, use the tracking set feature in Delivery service so that the log data will be stored in the specified bucket persistently.

Resource type	Resource ID/Name	Tag	Region	Creation time	Compliance status	Operation
QCS::CAM::Role CAM - Role			Global	2022-11-22 14:12:12	N/A	Manage resources Resource timeline
QCS::CAM::Policy CAM - Policy			Global	2022-06-01 19:12:06	N/A	Manage resources Resource timeline
QCS::CAM::Policy CAM - Policy			Global	2020-05-15 14:40:56	N/A	Manage resources Resource timeline
QCS::CAM::Policy CAM - Policy			Global	2020-11-09 10:13:32	N/A	Manage resources Resource timeline
QCS::CAM::Policy CAM - Policy			Global	2021-06-29 16:01:36	N/A	Manage resources Resource timeline
QCS::CAM::Policy CAM - Policy			Global	2022-01-26 15:13:29	N/A	Manage resources Resource timeline
QCS::CAM::Policy CAM - Policy			Global	2022-02-18 11:15:02	N/A	Manage resources Resource timeline
QCS::CAM::Policy CAM - Policy			Global	2022-02-18 16:25:49	N/A	Manage resources Resource timeline
QCS::CAM::Policy CAM - Policy			Global	2022-02-11 16:39:04	N/A	Manage resources Resource timeline
QCS::CAM::Policy CAM - Policy			Global	2022-03-11 16:45:39	N/A	Manage resources Resource timeline

2. All resources support cross-regional search. You can search for resources by fields such as resource ID, resource name, resource type, resource status, tag, and region.

Note:

To facilitate viewing, for CAM policies (QCS::CAM::Policy), only custom policies are displayed in the resource list while predefined policies are not.

3. You can click the **resource name** in the resource list to go to the **Resource Details** page for the detailed information about the resource. You can click **Manage Resources** to go to the corresponding page for further resource management. You can also click **Resource Timeline** to go to the resource timeline page for configuration change records of the resource.
4. You can click the **resource name** in the resource list to go to the **resource details** page for the detailed information about the resource. You can click **Manage resources** to go to the corresponding page for further resource management. You can also click **Resource timeline** to go to the resource timeline page for configuration change records of the resource.

Viewing Resource Details

Last updated: 2024-03-04 14:13:25

Resource Details

In the resource list, you can click the resource name to go to the **resource details** page comprised of three tabs.

Resource details

The **Resource details** tab displays the latest attributes, configuration information, and compliance evaluation result of the resource. For more information, see [Glossary](#).

The screenshot shows the 'Resource details' tab for a resource with ID 4611686028425397557. The page is divided into three main sections: Basic info, Configuration info, and Latest compliance evaluation result.

Basic info:

Resource ID	4611686028425397557	Resource name	COS_QCSRole
Resource type	QCS:CAM:Role(CAM - Role)	Region	Global
Tag		Creation time	2022-11-22 14:12:12
Update time	2022-11-22 14:12:27		

Configuration info: View details

Latest compliance evaluation result: Total evaluation results: 0, 0 are non-compliant

Rule name	Risk level	Rule trigger type	Last evaluation time	Evaluation result
		None		

Total items: 0

Related Resources

The **Related resources** tab displays specific resources associated with the current resource. For the detailed information on resource relationships supported by Config, see [Supported Resource Types](#).

The screenshot shows the 'Related resources' tab for the same resource. It features a search bar and a table with columns for Resource type, Resource ID, Resource name, and Operation.

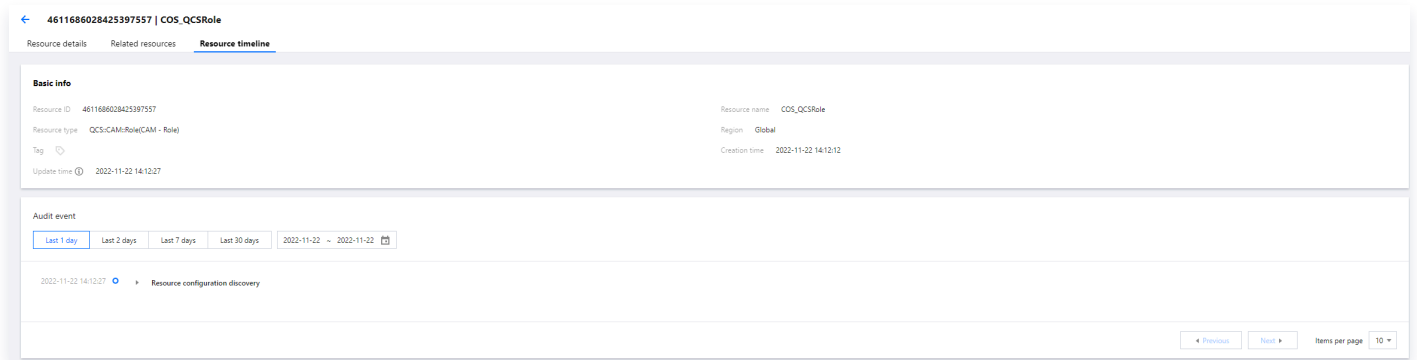
Search by resource:

Resource type	Resource ID	Resource name	Operation
		None	

Navigation: < Previous, Next >, Items per page: 10

Resource Timeline

The **Resource timeline** tab allows you to query all configuration change records of the resource made in the recent year.



1. Categories of Nodes in Timeline

Each configuration change of a resource will generate a node in the timeline. The specific configuration information of each node is defined and displayed through a configuration item **ConfigurationItem**.

○ Start of Timeline

If the resource was created before it was monitored by Config, the start of the resource timeline is the time when Config identified and recorded the configuration information of the resource for the first time. Otherwise, the start is the time when the resource was created for the first time.

○ End of Timeline

If the resource is deleted during monitoring by Config, the end is the time when the resource was deleted. Otherwise, the end is the time when the configuration was changed the last time.

2. Format of Nodes in Timeline

The configuration information on each node in the timeline is displayed through standard **ConfigurationItem**. It refers to the collection of various attributes and configuration information of a resource at a certain point in time and is composed of the basic information (Metadata), resource attributes (Attribute), related resources (Relationship), and detailed configuration (Configuration), as shown in the table below.

Part	Field Name	Field Description
Basic information Metadata	Version ID	Config version number, starting from 1.0.
	ConfigurationTime	Time when this configuration item was generated.
	Status	<ul style="list-style-type: none"> ResourceDiscovered (Initial discovery of resource configuration). ResourceRecorded (Record of resource configuration, not the initial discovery). ResourceChanged (Resource configuration has been altered, and the resource has not been deleted). ResourceDeleted (The resource has been deleted).

	StateID	Configuration item ID, which is the unique key of the configuration item.
	EventType	<p>Event Type:</p> <ul style="list-style-type: none"> • Configuration (When a resource configuration is discovered or recorded, the configuration audit generates a resource configuration event) • ConfigurationChange (When a resource configuration is altered or a resource is deleted, the configuration audit generates a configuration change event) • Compliance (When an evaluation is triggered by a resource association rule, the configuration audit generates a compliance evaluation event)
Resource Attributes Attribute	AccountID	Root account ID.
	ResourceID	Resource ID.
	ResourceName	Resource name.
	ResourceType	Resource type, such as QCS::CVM::Instance.
	ResourceTypeNa me	Resource type description, such as CVM – Instance.
	Tags	Key–value pair of the resource tag.
	Product	Cloud service, such as CVM.
	QCS	Six–segment resource format.
	Region	Resource region name, such as ap–guangzhou. For global resources without the region attribute, the value is "global".
	CreatedTime	Resource creation time.
Associated Resource Relationship	ResourceID	ID of the associated resource. ID of the resource only of types currently supported by Config are displayed. If no ID is available, leave this field blank.
	ResourceName	Name of the associated resource.
	ResourceType	Type of associated resource.
	RelationshipType	Type of the relationship between the current resource and the associated resource.

	RelationshipType Name	Relationship type name.
Detailed configuration	–	Detailed configuration, which varies depending on the resource type.

3. Categories of Events in Timeline

Based on the displayed event information, a node can represent any of the following events:

- **Resource Configuration Event**

This refers to the first discovery or record of resource configuration, typically based on the resource snapshot taken by the system. This event is recorded when you enable Config for the first time or manually modify the monitored resource type.

- **Configuration Change Event**

This refers to the record of resource configuration changes. If the latest configuration of the resource differs from the previously recorded configuration, the node indicates a resource configuration change. This event is generally captured based on CloudAudit (CA) logs or automatically executed resource snapshots. If the configuration change is made on CA, the corresponding CA event will be recorded accordingly.

- **Compliance Evaluation Event**

This refers to the record of resource configuration evaluation results. For information on the rule-based evaluation triggering mechanism, see [Rule-Based Evaluation](#).

Rule

Managed Rules

Last updated: 2026-04-07 15:45:09

Config supports the following managed rules. For other managed rules, you can [submit a ticket](#).

Cloud Service	Resource Type	Managed Rule
Cloud Access Management (CAM)	QCS::CAM::User	MFA on sensitive operations required for CAM users.
	QCS::CAM::User	MFA on login required for CAM users.
	QCS::CAM::Group	No idle user groups on CAM.
	QCS::CAM::User QCS::CAM::Group	Association with user group required for CAM user.
	QCS::CAM::User	No authorization policies directly added to CAM sub-account
	QCS::CAM::User	No administrator access permissions granted to CAM users, user groups, or roles.
	<ul style="list-style-type: none"> QCS::CAM::User QCS::CAM::Group QCS::CAM::Role 	Granting of specific high-risk permissions by CAM not allowed.
	QCS::CAM::Policy	No idle permission policies on CAM.
	QCS::CAM::Policy	CAM login permission check.
	QCS::CAM::User	Key of CAM user rotated at specified interval.
	QCS::CAM::User	Login by CAM user within specified time range.
CVM	QCS::CVM::Instance	CVM instance associated with specified security group.
	QCS::CVM::Instance	CVM Instance has not entered the Recycle Bin.

	QCS::CVM::Instance	Association of CVM instance with specified role.
	QCS::CVM::Instance	CVM instance enabled automatic renewal.
	QCS::CVM::Instance	Expiration notification for CVM instance prepayment and pay-as-you-go payment.
	QCS::CVM::Instance	Expiration protection for CVM instance in pay-as-you-go mode.
	QCS::VPC::SecurityGroup	No Idle Security Groups.
	QCS::CVM::Instance	CVM instance in VPC.
	QCS::CVM::Instance	No CVM instances not assigned to project.
	QCS::CVM::Instance	Inactive duration of CVM instance after shutdown not exceeding specified number of days.
	QCS::CVM::Instance	Lease duration of CVM instance meeting requirement of specified number of days.
	QCS::CVM::Instance	CVM instance bound to public IPv4 address.
CBS	QCS::CBS::Disk	No idle CBS disks.
	QCS::CBS::Disk	CBS disk enabled arrear protection.
	QCS::CBS::Disk	CBS disk enabled encryption.
	QCS::CBS::Disk	Detachable CBS disk not moved to Recycling Bin.
TAG	QCS::CVM::Instance	Specified tag existed for resource.
SecurityGroup	QCS::VPC::SecurityGroup	Access to remote risky ports by security group not allowed.
	QCS::VPC::SecurityGroup	Access to all ports by security groups not allowed.
Subnet	QCS::VPC::Subnet	Number of available IP addresses in VPC subnet greater than specified value.

List of Managed Rule

MFA on Sensitive Operations Required for CAM Users

Last updated: 2024-03-01 15:54:47

Rule purpose: Check whether MFA on sensitive operations is enabled on CAM.

Compliance evaluation logic: If MFA on sensitive operations has been enabled on CAM, the evaluation result is "compliant".

Rule Identifier: `cam-account-action-mfa-enabled`

Risk Level: High

Applicable Resource Type: `QCS::CAM::User`

Rule trigger type: Periodic execution, every 24 hours.

Keyword: User, MFA.

Rule parameter: None.

MFA on Login Required for CAM Users

Last updated: 2024-03-04 14:58:54

Rule purpose: Check whether MFA on login is enabled on CAM.

Compliance evaluation logic: If MFA on login has been enabled on CAM, the evaluation result is "compliant".

Rule Identifier: `cam-account-login-mfa-enabled`

Risk Level: High.

Applicable Resource Type: `QCS::CAM::User`

Rule trigger type: Periodic execution, every 24 hours.

Keyword: User, MFA.

Rule parameter: None.

No Idle User Groups on CAM

Last updated: 2024-03-04 15:23:57

Rule purpose: Check whether any idle user group exists on CAM.

Compliance evaluation logic: If each CAM user group has at least one user, the evaluation result is "compliant".

Rule Identifier: `cam-group-user-bound`

Risk Level: Low

Applicable Resource Type: `QCS::CAM::Group`

Rule trigger type: Periodic execution, every 24 hours.

Keyword: User, user group.

Rule parameter: None

Association with User Group Required for CAM User

Last updated: 2024-03-04 15:25:00

Rule purpose: Check whether the CAM user is associated with a user group.

Compliance evaluation logic: If the CAM user has been associated with at least one user group, the evaluation result is "compliant".

Rule Identifier: `cam-user-group-bound`

Risk Level: Low

Applicable Resource Type: `QCS::CAM::User`

Rule trigger type: Periodic execution, every 24 hours.

Keyword: User, user group.

Rule parameter: None.

No Authorization Policies Directly Added to CAM Sub-account

Last updated: 2022-12-05 17:45:03

Rule purpose: Check whether any authorization policy has been directly added to the CAM sub-account.

Compliance evaluation logic: If no authorization policies have been directly added to the CAM sub-account, the evaluation result is "compliant".

Rule Identifier: `cam-user-policy-directly-bound`

Risk Level: Low.

Applicable Resource Type: `QCS::CAM::User`

Rule trigger type: Periodic execution, every 24 hours.

Keyword: User, policy.

Rule parameter: None.

No Administrator Access Permissions Granted to CAM Users, User Groups, or Roles

Last updated: 2024-03-04 15:57:49

Rule purpose: Check whether the administrator access permissions are granted to CAM users, user groups, and roles.

Compliance evaluation logic: If no administrator access permissions are granted to CAM users, user groups, or roles, the evaluation result is "compliant".

Rule Identifier: `cam-policy-admin-access-bound`

Risk Level: High.

Applicable resource type: `QCS::CAM::User` , `QCS::CAM::Group` , `QCS::CAM::Role` .

Rule trigger type: Periodic execution, every 24 hours.

Keyword: User, user group, role, policy.

Rule parameter: None.

Granting of Specific High-Risk Permissions by CAM Not Allowed

Last updated: 2024-03-04 15:58:29

Rule purpose: Check whether CAM has granted specific high-risk permissions.

Compliance evaluation logic: When no CAM users, user groups, or roles are granted specific high-risk permissions, the evaluation result is "compliant".

Rule Identifier: `cam-user-risky-policy-bound` .

Risk Level: Low

Applicable resource type: `QCS::CAM::User` , `QCS::CAM::Group` , `QCS::CAM::Role` .

Rule trigger type: Periodic execution, every 24 hours.

Keyword: User, user group, role, policy.

Rule parameter:

Parameter name	Default value	Relationship
policies	AdministratorAcces	Contains

No Idle Permission Policies on CAM

Last updated: 2024-03-04 15:59:07

Rule purpose: Check whether any idle permission policy exists on CAM.

Compliance evaluation logic: When each permission policy is associated with at least one user, user group, or role, the evaluation result is "compliant".

Rule Identifier: `cam-policy-in-use` .

Risk Level: Low.

Applicable Resource Type: `QCS::CAM::Policy` .

Rule trigger type: Periodic execution, every 24 hours.

Keyword: User, user group, role, policy.

Rule parameter: None.

CAM Login Permission Check

Last updated: 2024-03-04 15:59:58

Rule purpose: Check the CAM login permission.

Compliance evaluation logic: If the console login permission and only one API key are enabled for any CAM user, the evaluation result is "compliant".

Rule Identifier: `cam-user-login-check` .

Risk Level: Low.

Applicable Resource Type: `QCS::CAM::User` .

Rule trigger type: Periodic execution, every 24 hours.

Keyword: User, login, key.

Rule parameter: None.

Key of CAM User Rotated at Specified Interval

Last updated: 2024-03-04 16:00:19

Rule purpose: Check whether the key of the CAM user is rotated at a specified interval.

Compliance evaluation logic: If the key of the CAM user is rotated at a specified interval, the evaluation result is "compliant".

Rule Identifier: `cam-user-ak-rotated` .

Risk Level: High.

Applicable Resource Type: `QCS::CAM::User` .

Rule trigger type: Periodic execution, every 24 hours.

Keyword: User, key.

Rule parameter:

Parameter name	Default value	Relationship
days	90	Less than or equal to

Login by CAM User within Specified Time Range

Last updated: 2024-03-04 16:01:21

Rule purpose: Check whether the CAM user has logged in within the specified time range.

Compliance evaluation logic: If the CAM user has logged in within the specified time range, the evaluation result is "compliant".

Rule Identifier: `cam-user-logged-in` .

Risk Level: Medium.

Applicable Resource Type: `QCS::CAM::User` .

Rule trigger type: Periodic execution, every 24 hours.

Keyword: User, login.

Rule parameter:

Parameter name	Default value	Relationship
days	90	Less than or equal to

CVM Instance Associated with Specified Security Group

Last updated: 2024-02-29 11:02:53

Rule purpose: Check whether the CVM instance is associated with a specified security group.

Compliance evaluation logic: If the CVM instance has been associated with a specified security group, the evaluation result is "compliant".

Rule Identifier: `cbs-disk-noidle`

Risk Level: High.

Applicable Resource Type: `QCS::CBS::Disk`

Rule trigger type: Periodic execution, every 24 hours.

Keyword: Security group, CVM.

Rule parameter: None.

CVM Instance Not Moved to Recycle Bin

Last updated: 2024-02-29 11:02:53

Rule purpose: Check whether the CVM instance has been moved to Recycle Bin.

Compliance evaluation logic: If the CVM instance is not moved to Recycle Bin due to reasons such as arrears or destruction, the evaluation result is "compliant".

Rule Identifier: `cvm-instance-no-recycle-bin`

Risk Level: High.

Applicable Resource Type: `QCS::CVM::Instance`

Rule trigger type: Configuration change.

Keyword: CVM.

Rule parameter: None.

Association of CVM Instance with Specified Role

Last updated: 2024-02-29 11:02:53

Rule purpose: Check whether the CVM instance has been associated with a specified role.

Compliance evaluation logic: If the CVM instance has been associated with a specified role, the evaluation result is "compliant".

Rule Identifier: `cvm-instance-specified-role`

Risk Level: Low

Applicable Resource Type: `QCS::CVM::Instance`

Rule trigger type: Configuration change

Keyword: CVM

Rule parameter: None

CVM Instance Enabled Automatic Renewal

Last updated: 2024-03-04 16:20:27

Rule purpose: Check whether the CVM instance has enabled automatic renewal.

Compliance evaluation logic: If the CVM instance has enabled automatic renewal, the evaluation result is "compliant".

Rule Identifier: `cvm-instance-automatic-renewal`

Risk Level: High.

Applicable Resource Type: `QCS::CVM::Instance`

Rule trigger type: Configuration change, periodic execution, every 24 hours.

Keyword: CVM.

Rule parameter: None.

Expiration Notification for CVM Instance Prepayment and Pay-As-You-Go Payment

Last updated: 2026-04-07 16:01:10

Rule purpose: Check whether notification about expiration is enabled for the CVM instance in yearly/monthly subscription or pay-as-you-go mode.

Compliance evaluation logic: If the duration between the expiration date of the CVM instance in yearly/monthly subscription or pay-as-you-go mode and the evaluation date is greater than the set number of days, the evaluation result is "compliant". Default duration: 30 days.

Rule Identifier: `cvm-instance-prepaid`

Risk Level: High.

Applicable Resource Type: `QCS::CVM::Instance`

Rule trigger type: Periodic execution, every 24 hours.

Keyword: CVM.

Rule parameter:

Parameter name	Default value	Relationship
days	30	Greater than or equal to

No Idle Security Groups

Last updated: 2024-02-29 11:02:53

Rule purpose: Check whether any idle security group exists.

Compliance evaluation logic: If all security groups have been bound, the evaluation result is "compliant".

Rule Identifier: `cvm-no-sg`

Risk Level: Medium

Applicable Resource Type: `QCS::VPC::SecurityGroup`

Rule trigger type: Configuration change

Keyword: Security Group

Rule parameter: None

CVM Instance in VPC

Last updated: 2024-02-29 11:02:53

Rule purpose: Check whether the CVM instance is in a VPC.

Compliance evaluation logic: If the CVM instance is in a specified VPC, the evaluation result is "compliant".

Rule Identifier: `cvm-instance-vpc`

Risk Level: Medium

Applicable Resource Type: `QCS::CVM::Instance`

Rule trigger type: Configuration change.

Keyword: CVM, VPC.

Rule parameter:

Parameter name	Default value	Relationship
vpcids	None	Contains

No CVM Instances Not Assigned to Project

Last updated: 2024-02-29 11:02:53

Rule purpose: Check whether all CVM instances have been assigned to a project.

Compliance evaluation logic: If all CVM instances have been assigned to a project, the evaluation result is "compliant".

Rule Identifier: `cvm-no-assigned-items`

Risk Level: Medium

Applicable Resource Type: `QCS::CVM::Instance`

Rule trigger type: Configuration change

Keyword: CVM

Rule parameter: None

Inactive Duration of CVM Instance After Shutdown Not Exceeding Specified Number of Days

Last updated: 2024-03-04 16:07:17

Rule purpose: Check whether the CVM instance has been shut down for more than specified number of days.

Compliance evaluation logic: If the CVM instance has not been shut down for more than specified number of days, the evaluation result is "compliant".

Rule Identifier: `cvm-instance-shutdown`

Risk Level: Medium

Applicable Resource Type: `QCS::CVM::Instance`

Rule trigger type: Periodic execution, every 24 hours.

Keyword: CVM

Rule parameter:

Parameter name	Default value	Relationship
days	None	Less than or equal to

Lease Duration of CVM Instance Meeting Requirement of Specified Number of Days

Last updated: 2024-02-29 11:02:53

Rule purpose: Check whether the lease duration of the CVM instance meets the requirement of specified number of days.

Compliance evaluation logic: If the lease duration of the CVM instance meets the requirement of specified number of days, the evaluation result is "compliant".

Rule Identifier: `cvm-instance-lease-duration`

Risk Level: Low

Applicable Resource Type: `QCS::CVM::Instance`

Rule trigger type: Periodic execution, every 24 hours.

Keyword: CVM.

Rule parameter:

Parameter name	Default value	Relationship
days	None	Greater than

CVM Instance Bound to IPv4 Public Address

Last updated: 2024-02-29 11:02:53

Rule purpose: Check whether the CVM instance is bound to an IPv4 public address.

Compliance evaluation logic: If the CVM instance has bound to an IPv4 public address, the evaluation result is "compliant". (This rule is applicable only to IPv4 addresses.)

Rule Identifier: `cvm-instance-publicipv4-bound`

Risk Level: Medium.

Applicable Resource Type: `QCS::CVM::Instance`

Rule trigger type: Configuration change.

Keyword: CVM, public IP address.

Rule parameter: None.

Specified Tag Existed for Resource

Last updated: 2024-02-29 11:02:53

Rule purpose: Check whether the specified tag for the resource exists.

Compliance evaluation logic: If the instance is associated with the specified tag, the evaluation result is "compliant".

Rule Identifier: `cvm-resource-exists-specified-tag`

Risk Level: High.

Applicable Resource Type: `QCS::CVM::Instance`

Rule trigger type: Configuration change.

Keyword: CVM, tag, storage bucket.

Rule parameter: None.

Access to Remote Risky Ports by Security Group Not Allowed

Last updated: 2024-02-29 11:02:54

Rule purpose: Check whether the security group can access remote risky ports when rules covering all network segments are set.

Compliance evaluation logic: When the security group has set rules covering all network segments (0.0.0.0/0 or ::/0), the port range cannot contain specified risky ports. If no such rules are set, the port range can contain specified risky ports. The evaluation result is "compliant" when the above conditions are met.

Rule Identifier: `cvm-sg-no-remote-access`

Risk Level: High

Applicable Resource Type: `QCS::VPC::SecurityGroup`

Rule trigger type: Configuration change

Keyword: Security Group

Rule parameter: None

Access to All Ports by Security Group Not Allowed

Last updated: 2024-02-29 11:02:54

Rule purpose: Check whether the port range value is set to All when rules involving all network segments are configured.

Compliance evaluation logic: When the security group has set rules covering all network segments (0.0.0.0/0 or ::/0), the port range value cannot be set to ALL. If no such rules are set, the port range value can be ALL. The evaluation result is "compliant" if the above conditions are met.

Rule Identifier: `cvm-sg-no-remote-access`

Risk Level: High

Applicable Resource Type: `QCS::VPC::SecurityGroup`

Rule trigger type: Configuration change

Keyword: Security Group

Rule parameter: None

CBS Disk Enabled Arrear Protection

Last updated: 2024-02-29 11:02:54

Rule purpose: Check whether arrear protection has been enabled for the CBS disk.

Compliance evaluation logic: If arrear protection has been enabled for the CBS disk, the evaluation result is "compliant".

Rule Identifier: `cbs-disk-open-arrears-protection`

Risk Level: Medium

Applicable Resource Type: `QCS::CBS::Disk`

Rule trigger type: Configuration change

Keyword: CBS disk

Rule parameter: None

CBS Disk Enabled Encryption

Last updated: 2024-03-04 16:24:46

Rule purpose: Check whether encryption has been enabled for the CBS disk.

Compliance evaluation logic: If encryption has been enabled for the CBS disk, the evaluation result is "compliant".

Rule Identifier: `cbs-disk-encrypted`

Risk Level: Medium

Applicable Resource Type: `QCS::CBS::Disk`

Rule trigger type: Configuration change

Keyword: CBS disk

Rule parameter: None

Detachable CBS Disk Not Moved to Recycle Bin

Last updated: 2026-04-07 15:44:04

Rule purpose: Check whether the detachable CBS disk has been moved to Recycle Bin.

Compliance evaluation logic: If the detachable CBS disk in yearly/monthly subscription mode has not been moved to Recycle Bin due to reasons such as arrears or returns, the evaluation result is "compliant".

Rule Identifier: `cbs-disk-no-trash`

Risk Level: Medium

Applicable Resource Type: `QCS::CBS::Disk`

Rule trigger type: Configuration change

Keyword: CBS disk

Rule parameter: None

Number of Available IP Addresses in VPC Subnet Greater than Specified Value

Last updated: 2024-02-29 11:02:54

Rule purpose: Check whether the number of available IP addresses in the VPC subnet exceeds a specified value.

Compliance evaluation logic: If the number of available IP addresses in the VPC subnet exceeds the configured specified value, the evaluation result is "compliant".

Rule Identifier: `vpc-subnet-availip`

Risk Level: Low.

Applicable Resource Type: `QCS::VPC::Subnet`

Rule trigger type: Periodic execution, every 24 hours.

Keyword: VPC, subnet.

Rule parameter:

Parameter name	Default value	Relationship
numbers	None	Greater than or equal to

Expiration Protection for CVM Instance in Pay-As-You-Go Mode

Last updated: 2024-02-29 11:02:54

Rule purpose: Check whether expiration protection has been enabled for the CVM instance in pay-as-you-go mode.

Compliance evaluation logic: During the billing period for the CVM instance in pay-as-you-go mode, if the instance is not shutdown and is still within the lease validity period, the evaluation result is "compliant".

Rule Identifier: `cvm-instance-fee-expiration-protection`

Risk Level: High.

Applicable Resource Type: `QCS::CVM::Instance`

Rule trigger type: Periodic execution, every 24 hours.

Keyword: CVM.

Rule parameter: None.

No Idle CBS Disks

Last updated: 2024-02-29 11:02:54

Rule purpose: Check whether any idle CBS disk exists.

Compliance evaluation logic: If no idle CBS disks exist and snapshots have been taken for all CDS disks, the evaluation result is "compliant".

Rule Identifier: `cbs-disk-noidle`

Risk Level: Low.

Applicable Resource Type: `QCS::CBS::Disk`

Rule trigger type: Configuration change.

Keyword: CBS disk, snapshot.

Rule parameter: None.

Using Rules

Creating Managed Rules

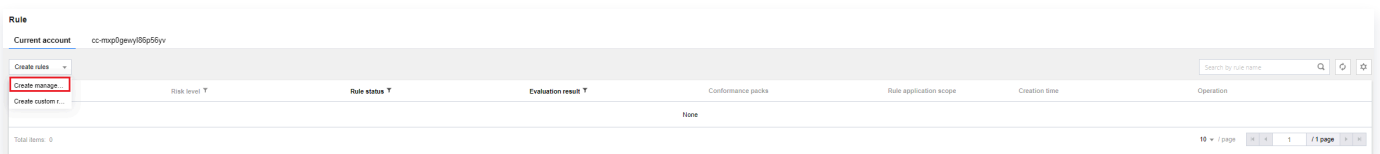
Last updated: 2024-03-04 14:26:59

Overview

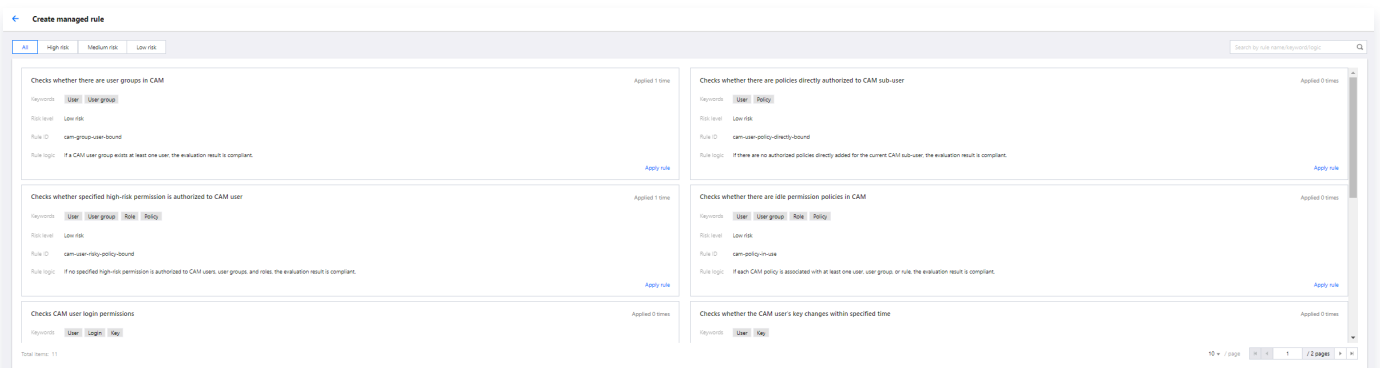
This document describes how to create a managed rule in the Config console for auditing and evaluating resources.

Directions

1. Log in to the Config console and click [Rule](#) in the left side bar.
2. On the **Rule** page, click **Create managed rule**. (You can select an individual account or a global account group for rule creation, depending on the actual account.)



3. On the **Create managed rule** page, select the managed rule that needs to be applied. For detailed information about supported managed rules, see [Supported Managed Rules](#).



4. On the **Basics** page, enter the rule name, risk level, and rule description, and then click **Next**.

The screenshot shows the 'Create managed rule' interface at the 'Basics' step. The breadcrumb navigation includes: 1 Basics, 2 Associated resources, 3 Trigger type, 4 Parameter, and 5 Preview and save. The 'Rule type' section has 'Managed rules' selected with a checkbox, and a sub-note: 'Use an existing rule function to quickly create a rule'. Below it is a 'Custom rule' option. The 'Rule name' field contains 'Expiration notification for CVM instance prepayment anc'. The 'Risk level' section has 'High risk' selected. The 'Description' field contains: 'For CVM instance prepayment and pay-as-you-go payment, if the number of days from the expiration time to the check time is greater than the specified number of days, the requirements are met. Default value: 30 days.' A 'Next' button is at the bottom left.

5. On the **Associated resources** page, select the resources you need to audit. You can also specify the rule application scope by tag or region as needed, or exclude resources by resource ID. Then, click **Next**.

The screenshot shows the 'Create managed rule' interface at the 'Associated resources' step. The breadcrumb navigation includes: 1 Basics, 2 Associated resources, 3 Trigger type, 4 Parameter, and 5 Preview and save. The 'Rule application scope' section includes: 'By resource type' with a dropdown menu showing 'QCS::CVM::Instance CVM - Instance;'; 'By tag' with 'Tag Key' and 'Tag Value' dropdowns, an 'x' icon, and '+ Add' and 'Paste' buttons; 'By region' with a dropdown menu showing 'Select a resource region'. The 'Rule exclusion scope' section includes: 'By resource ID' with a text input field containing 'Enter resource IDs and separate them by comma'. 'Previous' and 'Next' buttons are at the bottom left.

6. On the **Trigger type** page, set the rule trigger mechanism, then click **Next**.

The screenshot shows the 'Create managed rule' wizard at step 3, 'Trigger type'. The breadcrumb trail is: Basics > Associated resources > 3 Trigger type > 4 Parameter > 5 Preview and save. The 'Trigger' section has a checked checkbox for 'Periodically' with the subtext 'Execute evaluation at the specified frequency'. Below it, the 'Rule trigger condition' section has a 'Frequency' dropdown menu set to '24 hours'. At the bottom, there are 'Previous' and 'Next' buttons.

7. On the **Parameter** page, set the expected values for the rule parameter, and then click **Next**.

The screenshot shows the 'Create managed rule' wizard at step 4, 'Parameter'. The breadcrumb trail is: Basics > Associated resources > Trigger type > 4 Parameter > 5 Preview and save. A blue information banner at the top reads: 'Set input parameter thresholds for some managed rules. When a resource attribute complies with the specified input parameters, the evaluation result is compliant.' Below this is a table for 'Rule parameters':

Rule input parameter name	Relationship	Expected value
days		30

At the bottom, there are 'Previous' and 'Next' buttons.

8. On the **Preview and save** page, check the rule information you have entered. You can click Previous to go to the corresponding step to edit the information if needed. After you confirm that the information is correct, click **Save** to create the rule.

←
Create managed rule

✓ Basics
✓ Associated resources
✓ Trigger type
✓ Parameter
5 Preview and save

Basics

Rule type: Managed rule

Rule name: Expiration notification for CVM instance prepayment and pay-as-you-go payment

Risk level: High risk

Description: For CVM instance prepayment and pay-as-you-go payment, if the number of days from the expiration time to the check time is greater than the specified number of days, the requirements are met. Default value: 30 days.

Associated resources

Resource type: QCS::CVM::Instance(CVM - Instance);

Tag: -

Region: -

Rule exclusion scope

Resource ID: -

Trigger type

Trigger: Periodically

Frequency: 24 hours

Parameter

Rule input parameter name	Relationship	Expected value
days		30

Previous
Save

Note:

When you create or edit a conformance pack, if the select rule is already added to another conformance pack or is a supported managed rule or a rule in the conformance pack template, the system will add the rule to the current conformance pack after you save the changes.

Managing Rules

Viewing Rule List

Last updated: 2024-03-04 14:26:59

Click on the **Rule** menu to navigate to the **Rule** page, where you can view all the rules under this account. You can filter rules by Rule name, Risk level, Rule status, and Evaluation result.

Click **Rule** in the left sidebar to go to the **Rule** page. On this page, you can view all rules under the login account and filter rules by fields such as rule name, risk level, rule status, and evaluation result.

Rule

Current account

Create rules Search by rule name 🔍 ⌂ ⚙️

Rule name ⚡	Risk level ⌵	Rule status ⌵	Evaluation result ⌵	Conformance packs	Rule application scope	Creation time	Operation
test_Checks whether login protection MFA is enabl...	High risk	Enable	Compliant	-		2023-05-10 15:36:16	Edit Disable Delete
Checks CAM user login permissions	Low risk	Enable	Compliant	-		2023-05-10 14:00:51	Edit Disable Delete
Checks whether there are policies directly authoriz...	Low risk	Enable	Compliant	22		2022-11-23 10:13:07	Edit Disable Delete
Checks whether there are user groups in CAM	Low risk	Enable	Compliant	22		2022-11-23 10:13:07	Edit Disable Delete
Checks CAM user login permissions	Low risk	Enable	Compliant	-		2022-11-23 10:12:46	Edit Disable Delete
Checks whether there are user groups in CAM	Low risk	Enable	Compliant	test		2022-11-22 18:22:46	Edit Disable Delete
Checks whether there are policies directly authoriz...	Low risk	Enable	Compliant	-		2022-11-22 18:22:46	Edit Disable Delete
Checks whether specified high-risk permission is a...	Low risk	Enable	Compliant	test		2022-11-22 18:22:46	Edit Disable Delete
Checks whether there are idle permission policies i...	Low risk	Enable	Compliant	test		2022-11-22 18:22:46	Edit Disable Delete
Checks CAM user login permissions	Low risk	Enable	Compliant	test		2022-11-22 18:22:46	Edit Disable Delete

Total items: 16 10 / page ⏪ 1 / 2 pages ⏩

Viewing Rule Details

Last updated: 2024-03-04 14:26:59

You can click the name of a rule to view the detailed information. The rule details page will display the basic attributes of the rule, associated resources, trigger type, parameters, and evaluation result. You can edit, enable, disable, or delete the rule and perform evaluation, on the details page.

Rule

Current account

Create rules

Rule name	Risk level	Rule status	Evaluation result	Conformance packs	Rule application scope	Creation time	Operation
test_Checks whether login protection MFA is enabled for CAM user	High risk	Enable	Compliant	-		2023-05-10 15:36:16	Edit Disable Delete
Checks CAM user login permissions	Low risk	Enable	Compliant	-		2023-05-10 14:00:51	Edit Disable Delete
Checks whether there are policies directly authorizing the user	Low risk	Enable	Compliant	22		2022-11-23 10:13:07	Edit Disable Delete
Checks whether there are user groups in CAM	Low risk	Enable	Compliant	22		2022-11-23 10:13:07	Edit Disable Delete
Checks CAM user login permissions	Low risk	Enable	Compliant	-		2022-11-23 10:12:46	Edit Disable Delete
Checks whether there are user groups in CAM	Low risk	Enable	Compliant	test		2022-11-22 18:22:46	Edit Disable Delete
Checks whether there are policies directly authorizing the user	Low risk	Enable	Compliant	-		2022-11-22 18:22:46	Edit Disable Delete
Checks whether specified high-risk permission is authorized	Low risk	Enable	Compliant	test		2022-11-22 18:22:46	Edit Disable Delete
Checks whether there are idle permission policies in use	Low risk	Enable	Compliant	test		2022-11-22 18:22:46	Edit Disable Delete
Checks CAM user login permissions	Low risk	Enable	Compliant	test		2022-11-22 18:22:46	Edit Disable Delete

Total items: 16 10 / page 1 / 2 pages

[←](#) **test_Checks whether login protection MFA is enabled for CAM user** [Edit](#) [Evaluate](#) [Disable](#) [Delete](#)

Basics

Rule type: Managed rule	Rule name: test_Checks whether login protection MFA is enabled for CAM user
Rule ID: cam-account-login-mfa-enabled	Risk level: High risk
Creation time: 2023-05-10 15:36:16	Description: If login protection MFA is enabled in CAM, the evaluation result is compliant.
Owner account: [blurred]	

Associated resources

Rule application scope

Resource type: QCS:CAM:User(CAM - User):

Tag: -

Region: -

Rule exclusion scope

Resource ID: -

Trigger type

Trigger: Periodically

Frequency: 24 hours

Parameter

Rule input parameter name	Relationship	Expected value
	None	

Editing Rule

Last updated: 2024-03-04 14:26:59

Find the rule to be edited in the rule list, and click **Edit** in the Operation column to modify the rule settings.

Rule

Current account

Create rules ▾ Search by rule name 🔍 ↻ ⚙️

Rule name ↕	Risk level ▾	Rule status ▾	Evaluation result ▾	Conformance packs	Rule application scope	Creation time	Operation
test_Checks whether login protection MFA is enabl...	High risk	Enable	Compliant	-		2023-05-10 15:36:16	Edit Disable Delete

Enabling/Disabling Rule

Last updated: 2024-03-04 14:26:59

Rules that are temporarily not in use can be disabled by clicking **Disable** in the **rule list** or on the **rule details** page. Once a rule is **disabled**, evaluation cannot be performed unless it is **enabled** again, regardless of automatic execution based on execution cycle settings or manual execution by clicking **Evaluate**.

Rule							
Current account							
Rule name	Risk level	Rule status	Evaluation result	Conformance packs	Rule application scope	Creation time	Operation
test_Checks whether login protection MFA is enabl...	High risk	Enable	Compliant	-	1302000590@qq.co555(100000624047)	2023-05-10 15:36:16	Edit Disable Delete

Deleting Rule

Last updated: 2024-03-04 14:26:59

Rules that are no longer needed can be deleted. To delete a rule, click **Delete** in the **rule list**, or click the rule name to go to the **rule details** page and then click **Delete**. The rule must be **disabled** first before it is **deleted** to prevent accidental deletion. Rules that have been added to conformance packs can be deleted in batch by **deleting** the conformance packs.

Rule

Current account

Create rules Search by rule name

Rule name	Risk level	Rule status	Evaluation result	Conformance packs	Rule application scope	Creation time	Operation
test_Checks whether login protection MFA is enabl...	High risk	Enable	Compliant	-		2023-05-10 15:36:16	Edit Disable Delete

[←](#) **Checks whether there are policies directly authorized to CAM sub-user** [Edit](#) [Evaluate](#) [Disable](#) [Delete](#)

Basics

Rule type: Managed rule	Rule name: Checks whether there are policies directly authorized to CAM sub-user
Rule ID: cam-user-policy-directly-bound	Risk level: Low risk
Creation time: 2022-11-22 18:22:46	Description: If there are no authorized policies directly added for the current CAM sub-user, the evaluation result is compliant.
Owner account: [redacted]	

Associated resources

Rule application scope

Resource type: QCS::CAM::User(CAM - User)

Tag: -

Region: -

Rule exclusion scope

Resource ID: -

Trigger type

Trigger: Periodically

Frequency: 24 hours

Parameter

Rule input parameter name	Relationship	Expected value
	None	

Evaluating Rule

Last updated: 2024-03-04 14:26:59

Evaluation can be automatically triggered by the system or manually triggered by users for enabled rules. For disabled rules, evaluation can only be triggered after they are **enabled**.

Manual triggering

- Single rule

Users **create** a rule or **edit** an existing rule and then save the changes.

Users **enable** a disabled rule.

Users click on **Evaluate** on the rule details page.

The screenshot shows the details page for a rule. At the top right, there are buttons for 'Edit', 'Evaluate' (highlighted with a red box), 'Disable', and 'Delete'. The rule name is 'Checks whether there are policies directly authorized to CAM sub-user'. The 'Basics' section includes: Rule type: Managed rule; Rule ID: cam-user-policy-directly-bound; Creation time: 2022-11-22 18:22:46; Owner account: 100000624047; Rule name: Checks whether there are policies directly authorized to CAM sub-user; Risk level: Low risk; Description: If there are no authorized policies directly added for the current CAM sub-user, the evaluation result is compliant. The 'Associated resources' section includes: Rule application scope: Resource type: QCS::CAM::User(CAM - User); Tag: -; Region: -; Rule exclusion scope: Resource ID: -. The 'Trigger type' section includes: Trigger: Periodically; Frequency: 24 hours. The 'Parameter' section is empty.

- Multiple rules

Evaluation based on multiple rules in a conformance pack can be triggered in the following scenarios:

Users create a conformance pack or edit an existing conformance pack and then save the changes.

Users click on **Evaluate** on the conformance pack details page.

← Checks whether there are policies directly authorized to CAM sub-user

Edit
Evaluate
Disable
Delete

Basics

Rule type: Managed rule	Rule name: Checks whether there are policies directly authorized to CAM sub-user
Rule ID: cam-user-policy-directly-bound	Risk level: Low risk
Creation time: 2022-11-22 18:22:46	Description: If there are no authorized policies directly added for the current CAM sub-user, the evaluation result is compliant.
Owner account: 100000624047	

Associated resources

Rule application scope

Resource type: QCS::CAM::User(CAM - User)

Tag: -

Region: -

Rule exclusion scope

Resource ID: -

Trigger type

Trigger: Periodically

Frequency: 24 hours

Parameter

Rule input parameter name	Relationship	Expected value
	None	

Automatic triggering

If users have configured an execution cycle for a rule or conformance pack, the evaluation will be automatically performed based on the settings each day. The first evaluation on each day starts at 00:30.

Creation time 2022-11-23 10:12:46

Description If either the console login and access permission or API key is enabled by any CAM user, the evaluation result is compliant.

Owner account 100000624047

Associated resources

Rule application scope

Resource type QCS::CAM::User(CAM - User);

Tag -

Region -

Rule exclusion scope

Resource ID -

Trigger type

Trigger Periodically;

Frequency 24 hours

Parameter

Rule input parameter name	Relationship	Expected value
	None	

Evaluation result

Total evaluation results: 0, 0 are non-compliant

Resource type	Resource ID/Name	Evaluation result	Operation
		None	

Total items: 0

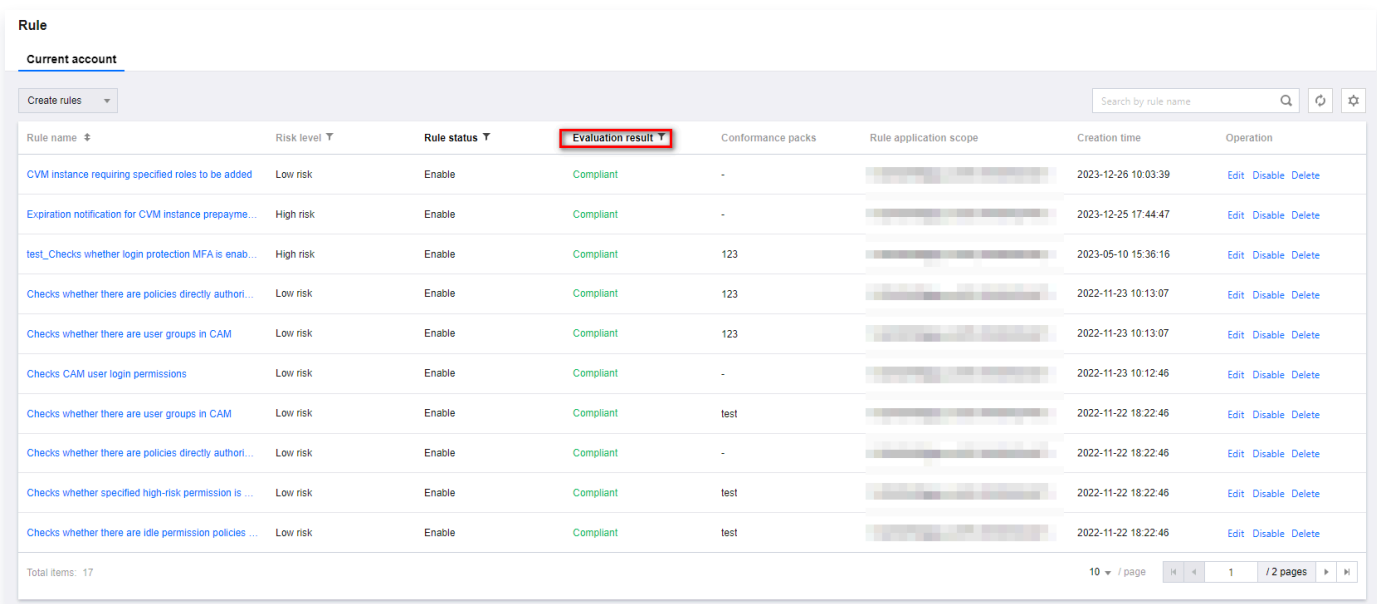
10 / page 1 / 1 page

Viewing Rule Evaluation Results

Last updated: 2024-03-04 14:26:59

After rule-based evaluation is completed, you can view the evaluation result in the following ways:

1. Click **Rule** in the left sidebar to go to the **Rule** page. Then, click the rule name to go to the **rule details** page. You can view the most recent results of evaluation on all associated resources.



Rule name	Risk level	Rule status	Evaluation result	Conformance packs	Rule application scope	Creation time	Operation
CVM instance requiring specified roles to be added	Low risk	Enable	Compliant	-		2023-12-26 10:03:39	Edit Disable Delete
Expiration notification for CVM instance prepayme...	High risk	Enable	Compliant	-		2023-12-25 17:44:47	Edit Disable Delete
test_Checks whether login protection MFA is enab...	High risk	Enable	Compliant	123		2023-05-10 15:36:16	Edit Disable Delete
Checks whether there are policies directly authori...	Low risk	Enable	Compliant	123		2022-11-23 10:13:07	Edit Disable Delete
Checks whether there are user groups in CAM	Low risk	Enable	Compliant	123		2022-11-23 10:13:07	Edit Disable Delete
Checks CAM user login permissions	Low risk	Enable	Compliant	-		2022-11-23 10:12:46	Edit Disable Delete
Checks whether there are user groups in CAM	Low risk	Enable	Compliant	test		2022-11-22 18:22:46	Edit Disable Delete
Checks whether there are policies directly authori...	Low risk	Enable	Compliant	-		2022-11-22 18:22:46	Edit Disable Delete
Checks whether specified high-risk permission is ...	Low risk	Enable	Compliant	test		2022-11-22 18:22:46	Edit Disable Delete
Checks whether there are idle permission policies ...	Low risk	Enable	Compliant	test		2022-11-22 18:22:46	Edit Disable Delete

2. Click **Resource** in the left sidebar to go to the **<Resource** page. Then, click the resource name to go to the **resource details** page. In the Latest compliance evaluation result section, you can view the latest evaluation results of this resource corresponding to all associated rules.

Creation time 2022-11-22 18:22:46 Description If a CAM user group exists at least one user, the evaluation result is compliant.
Owner account [redacted]

Associated resources

Rule application scope
Resource type QCS::CAM::Group(CAM - User group);
Tag -
Region -

Rule exclusion scope
Resource ID -

Trigger type
Trigger Periodically;
Frequency 24 hours

Parameter

Rule input parameter name	Relationship	Expected value
	None	

Evaluation result
Total evaluation results: 0, 0 are non-compliant

Resource type	Resource ID/Name	Evaluation result	Operation
		None	

Total items: 0 10 / page 1 / 1 page

Conformance Pack

Supported Conformance Pack Template

Last updated: 2024-03-04 14:13:26

Currently, Config provides a predefined conformance pack template based on best practices of account security. For other templates, you can [submit a ticket](#).

Conformance Pack Template	Managed Rule
Best practices of account security	MFA on sensitive operations for CAM users.
	MFA on login for CAM users.
	No idle user groups on CAM.
	Association with user group required for CAM user.
	No authorization policies directly added to CAM sub-accounts.
	No administrator access permission granted to CAM users, user groups, or roles.
	Granting of specific high-risk permissions by CAM not allowed.
	No idle permission policies on CAM.
	CAM login permission check.
	Key of CAM user rotated at specified interval.
	Login of CAM user within specified time range.

Managing Conformance Packs

Viewing Conformance Pack List

Last updated: 2024-03-04 14:13:26

Click **Conformance Pack** in the left sidebar to go to the **Conformance packs** page. On this page, you can view all the conformance packs under the current account. You can also filter the packs by pack name, risk level, pack status, and evaluation result.

Conformance packs					
Current account					
Create conformance pack					
Search by conformance pack name					
Conformance pack name	Risk level	Conformance pack status	Evaluation result	Creation time	Operation
test	High risk	Enable	Compliant	2022-11-22 18:22:46	Edit Disable Delete
22	High risk	Enable	Compliant	2022-11-23 10:13:07	Edit Disable Delete

Total items: 2

10 / page 1 / 1 page

Viewing Conformance Pack Details

Last updated: 2024-03-04 14:13:26

In the **conformance pack list**, you can click the name of a conformance pack to go to the **details** page. This page displays the basic attributes of the conformance pack, the rules it contains, and the evaluation results. You can also **edit** or **delete** the conformance pack, perform evaluation based on the conformance pack, and **add**, **remove**, or **delete** rules on the details page.

Conformance packs

Current account

Create conformance pack

Search by conformance pack name

Conformance pack name	Risk level	Conformance pack status	Evaluation result	Creation time	Operation
test	High risk	Enable	Compliant	2022-11-22 18:22:46	Edit Disable Delete
22	High risk	Enable	Compliant	2022-11-23 10:13:07	Edit Disable Delete

Total items: 2

10 / page

test

Edit Evaluate Disable Delete

Basic info

Conformance pack name: test Risk level: High risk

Creation time: 2022-11-22 18:22:46 Description:

Rule

Add rule

Search by rule name or keywords

Rule name	Risk level	Keywords	Rule status	Evaluation result	Operation
Checks whether there are user groups in CAM	Low risk	User/User group	Enable	Compliant	Remove Delete
Checks whether specified high-risk permission is authorized to CA...	Low risk	User/User group/Role/Policy	Enable	Compliant	Remove Delete
Checks whether there are idle permission policies in CAM	Low risk	User/User group/Role/Policy	Enable	Compliant	Remove Delete
Checks CAM user login permissions	Low risk	User/Login/Key	Enable	Compliant	Remove Delete
Checks whether the CAM user's key changes within specified time	High risk	User/Key	Enable	Compliant	Remove Delete
Checks whether there are login activities for CAM users during spe...	Medium risk	User/ Login	Enable	Compliant	Remove Delete
Checks whether there are super admin permissions under CAM su...	Low risk	User/User group/Role/Policy	Enable	Compliant	Remove Delete
Checks whether login protection MFA is enabled for CAM user	High risk	User/MFA	Enable	Compliant	Remove Delete
Checks whether sensitive operation MFA is enabled for CAM user	High risk	User/MFA	Enable	Compliant	Remove Delete

Creating Conformance Pack

Last updated: 2024-03-04 14:13:26

To create a conformance pack, click **Conformance Pack** in the left sidebar to go to the **Conformance packs** page, click **Create conformance pack**, and set the basic attributes, add rules, and configure rule parameters.

Conformance packs

Current account

[Create conformance pack](#)

Conformance pack name	Risk level ▾	Conformance pack status ▾	Evaluation result ⓘ ▾	Creation time ⚙	Operation
test	High risk	Enable	Compliant	2022-11-22 18:22:46	Edit Disable Delete
22	High risk	Enable	Compliant	2022-11-23 10:13:07	Edit Disable Delete

Total items: 2 10 / page 1 / 1 page

[←](#) **Create conformance pack**

1 Basic info > 2 Add rule > 3 Configure rule > 4 Preview and save

Conformance pack name *

Risk level * High risk Medium risk Low risk

Description

Editing Conformance Pack

Last updated: 2024-03-04 14:13:25

Find the target pack in the **conformance pack list** and then click **Edit** in the Operation column to edit the pack.

Conformance pack name	Risk level ▾	Conformance pack status ▾	Evaluation result ⓘ ▾	Creation time ↕	Operation
	High risk	Enable	Compliant	2022-11-22 18:22:46	Edit Disable Delete

Total items: 1 10 / page 1 / 1 page

You can also click **Edit** at the top of the **conformance pack details** page to edit the pack.

← test

Edit
Evaluate
Disable
Delete

Basic info

Conformance pack name: test	Risk level: High risk
Creation time: 2022-11-22 18:22:46	Description:

Rule

Add rule

Search by rule name or keywords Q

Rule name	Risk level	Keywords	Rule status	Evaluation result	Operation
Checks whether there are user groups in CAM	Low risk	User/User group	Enable	Compliant	Remove Delete
Checks whether specified high-risk permission is authorized to CA...	Low risk	User/User group/Role/Policy	Enable	Compliant	Remove Delete
Checks whether there are idle permission policies in CAM	Low risk	User/User group/Role/Policy	Enable	Compliant	Remove Delete
Checks CAM user login permissions	Low risk	User/Login/Key	Enable	Compliant	Remove Delete
Checks whether the CAM user's key changes within specified time	High risk	User/Key	Enable	Compliant	Remove Delete
Checks whether there are login activities for CAM users during spe...	Medium risk	User/ Login	Enable	Compliant	Remove Delete
Checks whether there are super admin permissions under CAM su...	Low risk	User/User group/Role/Policy	Enable	Compliant	Remove Delete
Checks whether login protection MFA is enabled for CAM user	High risk	User/MFA	Enable	Compliant	Remove Delete
Checks whether sensitive operation MFA is enabled for CAM user	High risk	User/MFA	Enable	Compliant	Remove Delete

Adding/Removing Rule

Last updated: 2024-03-04 14:13:26

To add rules existed in the **rule list** to the conformance pack, click **Edit** in the conformance pack list and add the rule in the step **Add rule**. You can also go to the **conformance pack details** page and add rules in the step **Add rule**. In addition, you can remove rules from the conformance pack.

If the select rule is a managed rule or has been added to the conformance pack template or a custom conformance pack, the system will automatically duplicate and add the rule to the current conformance pack.

- Click **Edit** in the **conformance pack list**.

Conformance pack name	Risk level ▾	Conformance pack status ▾	Evaluation result ⓘ ▾	Creation time ⌵	Operation
	High risk	Enable	Compliant		Edit Disable Delete

Total items: 1 10 / page << >> 1 / 1 page >>

- Select the rules to add in the step **Add rule**.

← Edit conformance pack

Basic info > **2 Add rule** > 3 Configure rule > 4 Preview and save

Rule list

Search by rule name

<input checked="" type="checkbox"/>	Rule name	Risk I...	Description
<input checked="" type="checkbox"/>	Expiration notification for CVM instanc...	High risk	For CVM instance prepayment and pay-as-you-go payment, if t...

Total items: 1 10 / page << >> 1 / 1 page >>

Hold down on the Shift key to select multiple items

Selected (1)

Rule name	Rule source ⓘ	
Expiration notification for C...	Managed rules	<input checked="" type="checkbox"/>

[Previous](#) [Next](#)

- Go to the **conformance pack details** page, and select the target rule in the step **Add rule**.

←██████████EditEvaluateDisableDelete

Basic info

Conformance pack name ██████████	Risk level High risk
Creation time ██████████	Description

Rule

Add rule

Search by rule name or keywords Q

Rule name	Risk level	Keywords	Rule status	Evaluation result	Operation
Expiration notification for CVM instance prepayment and pay-as-...	High risk	CVM	Enable	Compliant	Remove Delete

Deleting Rule

Last updated: 2024-03-04 14:13:25

In the **conformance pack details** page, you can click **Delete** in the rules area to delete rules in the current conformance pack.

← 323 Edit Evaluate Disable Delete

Basic info

Conformance pack name 323 Risk level **High risk**

Creation time 2024-01-04 19:49:33 Description

Rule

Add rule Q

Rule name	Risk level	Keywords	Rule status	Evaluation result	Operation
	Low risk	CVM	Enable	Compliant	Remove Delete

Deleting Conformance Pack

Last updated: 2024-03-04 14:13:25

For conformance page that are no longer required, you may directly click on **Delete** in the **Conformance packs List** or **Conformance packs Details** page. When a conformance pack is deleted, the rules within the package will be concurrently removed.

For conformance packs that are no longer needed, you can click **Delete** in the **conformance pack list** or on the **conformance pack details** page. When a conformance pack is deleted, the rules in the pack will be deleted as well.

Conformance packs

Current account

Create conformance pack

Search by conformance pack name

Conformance pack name	Risk level	Conformance pack status	Evaluation result	Creation time	Operation
test	High risk	Enable	Compliant	2022-11-22 18:22:46	Edit Disable Delete
22	High risk	Enable	Compliant	2022-11-23 10:13:07	Edit Disable Delete

Total items: 2

10 / page

test

Edit Evaluate Disable **Delete**

Basic info

Conformance pack name test Risk level High risk

Creation time 2022-11-22 18:22:46 Description

Rule

Add rule

Search by rule name or keywords

Rule name	Risk level	Keywords	Rule status	Evaluation result	Operation
Checks whether there are login activities for CAM users during s...	Medium risk	User/ Login	Enable	Compliant	Remove Delete
Checks whether there are idle permission policies in CAM	Low risk	User/User group/Role/Policy	Enable	Compliant	Remove Delete
Checks whether there are super admin permissions under CAM s...	Low risk	User/User group/Role/Policy	Enable	Compliant	Remove Delete
Checks CAM user login permissions	Low risk	User/Login/Key	Enable	Compliant	Remove Delete
Checks whether sensitive operation MFA is enabled for CAM user	High risk	User/MFA	Enable	Compliant	Remove Delete
Checks whether login protection MFA is enabled for CAM user	High risk	User/MFA	Enable	Compliant	Remove Delete
Checks whether the CAM user's key changes within specified tme	High risk	User/Key	Enable	Compliant	Remove Delete
Checks whether there are user groups in CAM	Low risk	User/User group	Enable	Compliant	Remove Delete
Checks whether specified high-risk permission is authorized to C...	Low risk	User/User group/Role/Policy	Enable	Compliant	Remove Delete

Evaluating Conformance Pack

Last updated: 2024-03-04 14:13:26

Evaluation can be triggered automatically by the system or manually by the user for enabled conformance packs.

Manual triggering

User operations include **Create conformance pack** and saving after **editing**.

Users can click on **Evaluate** compliance package on the **Compliance Package Details** page.

← test Edit **Evaluate** Disable Delete

Basic info

Conformance pack name: test Risk level: High risk
 Creation time: 2022-11-22 18:22:46 Description:

Rule

Add rule

Rule name	Risk level	Keywords	Rule status	Evaluation result	Operation
Checks whether there are user groups in CAM	Low risk	User/User group	Enable	Compliant	Remove Delete
Checks whether specified high-risk permission is authorized to CA...	Low risk	User/User group/Role/Policy	Enable	Compliant	Remove Delete
Checks whether there are idle permission policies in CAM	Low risk	User/User group/Role/Policy	Enable	Compliant	Remove Delete
Checks CAM user login permissions	Low risk	User/Login/Key	Enable	Compliant	Remove Delete
Checks whether the CAM user's key changes within specified time	High risk	User/Key	Enable	Compliant	Remove Delete
Checks whether there are login activities for CAM users during spe...	Medium risk	User/ Login	Enable	Compliant	Remove Delete
Checks whether there are super admin permissions under CAM su...	Low risk	User/User group/Role/Policy	Enable	Compliant	Remove Delete
Checks whether login protection MFA is enabled for CAM user	High risk	User/MFA	Enable	Compliant	Remove Delete
Checks whether sensitive operation MFA is enabled for CAM user	High risk	User/MFA	Enable	Compliant	Remove Delete

Automatic triggering

Users can configure an execution cycle for rules in the conformance pack. Evaluation will be automatically performed at the specified time.

Viewing Conformance Pack Evaluation Results

Last updated: 2024-03-04 14:13:26

You can view the evaluation result of each conformance pack in the **conformance pack list**. If the results of evaluation based on all rules in the conformance pack are Compliant, the overall result of the conformance pack is Compliant. Otherwise, the overall result is Non-compliant.

Conformance packs

Current account

Create conformance pack

Search by conformance pack name

Conformance pack name	Risk level	Conformance pack status	Evaluation result	Creation time	Operation
test	High risk	Enable	Compliant	2022-11-22 18:22:46	Edit Disable Delete
22	High risk	Enable	Compliant	2022-11-23 10:13:07	Edit Disable Delete
123	High risk	Enable	Compliant	2023-12-26 16:17:34	Edit Disable Delete

Total items: 3

10 / page 1 / 1 page

If you want to view the results of each rule in the conformance pack, you can click the conformance pack name to go to the **details** page and view the results.

← 123

Edit Evaluate Disable Delete

Basic info

Conformance pack name 123 Risk level High risk

Creation time 2023-12-26 16:17:34 Description

Rule

Add rule

Search by rule name or keywords

Rule name	Risk level	Keywords	Rule status	Evaluation result	Operation
Checks whether there are user groups in CAM	Low risk	User/User group	Enable	Compliant	Remove Delete
Checks whether there are policies directly authorized to CAM sub-...	Low risk	User/Policy	Enable	Compliant	Remove Delete
test_Checks whether login protection MFA is enabled for CAM user	High risk	User/MFA	Enable	Compliant	Remove Delete

Settings

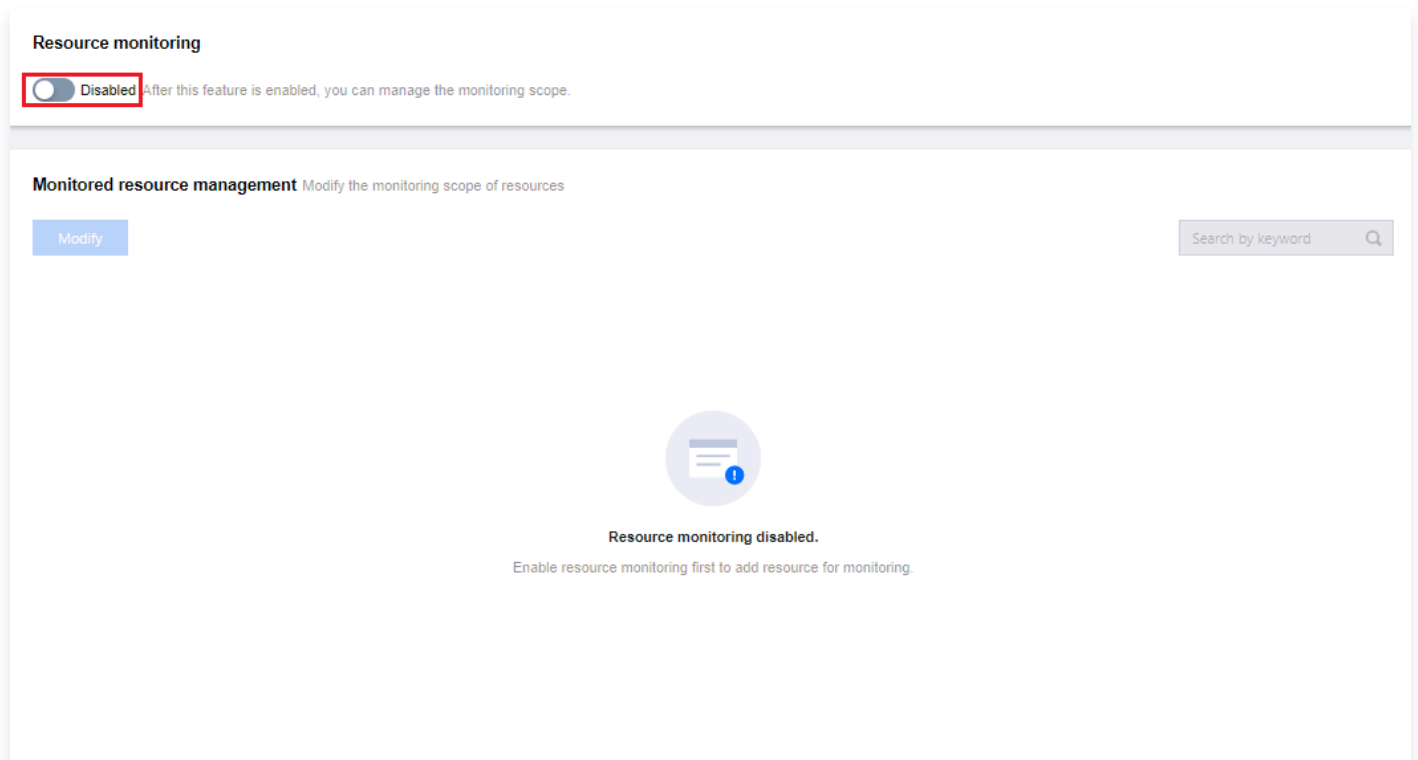
Monitoring Management

Last updated: 2024-03-04 14:13:24

You can choose **Settings > Service Settings** to enable resource monitoring and set the scope of resources to be monitored.

Enabling Resource Monitoring

You can enable resource monitoring on the **Monitoring Management** page. If resource monitoring is enabled for the first time, you need to authorize the corresponding role (Config_QCSLinkedRoleInConfigRecorder) and select the types of resources to be monitored. For resource types supported by Config, see [Supported Resource Types](#).



Disabling Resource Monitoring

If resource monitoring is not needed, you can disable it on the **Monitoring Management** page. Once disabled, Config no longer monitors and updates resource configuration changes. The stored resource configuration data, created rules, and compliance evaluation results will be cleared and cannot be recovered. However, historical data that have been delivered to the COS bucket will not be affected.

Resource monitoring

Enabled After this feature is enabled, you can manage the monitoring scope.

Monitored resource management Modify the monitoring scope of resources

[Modify](#)

Product/Resource type	Update time
QCS:CVM:Instance CVM - Instance	2022-11-22 17:53:34
QCS:CBS:Disk Instance - CBS	2023-06-28 10:36:44
QCS:VPC:Vpc VPC - VPC	2023-06-28 10:18:32
QCS:VPC:SecurityGroup VPC - Security group	2023-06-28 11:19:45
QCS:VPC:Subnet VPC - Subnet	2023-06-28 11:34:37

Total items: 5 10 / page / 1 page

Resource management Modify the monitoring scope of resources

Product/Resource type Update time

2022-11-22 17:53:34

Are you sure you want to disable resource monitoring? ✕

If you disable resource monitoring, the stored resource configuration data, created rules, and obtained compliance results will be cleared and cannot be restored. Are you sure you want to disable resource monitoring?

By now, resource monitoring has:

- ✔ Recorded 359 resource changes.
- ✔ Audited 0 non-compliant records (in 0 rules applied by 0 resources).

10

Monitoring scope change

If you have already enabled resource monitoring, you can click **Modify** to change the types of resources being monitored. Monitoring scope changes will result in the addition of new resources to the resource list, corresponding updates, and re-evaluation based on existing rules and conformance packs under your account. This process is expected to take about 10–15 minutes. Please wait patiently.

Resource monitoring

Enabled After this feature is enabled, you can manage the monitoring scope.

Monitored resource management Modify the monitoring scope of resources

Modify Search by keyword

Product/Resource type	Update time
QCS::CVM::Instance CVM - Instance	2022-11-22 17:53:34
QCS::CBS::Disk Instance - CBS	2023-06-28 10:36:44
QCS::VPC::Vpc VPC - VPC	2023-06-28 10:18:32
QCS::VPC::SecurityGroup VPC - Security group	2023-06-28 11:19:45
QCS::VPC::Subnet VPC - Subnet	2023-06-28 11:34:37

Total items: 5 10 / page 1 / 1 page

Monitored resource management Modify the monitoring scope of resources

Modify monitoring scope ✕

Select resource types to monitor (10)

Search by resource type

- Resource type
- QCS::CVM::Instance
CVM - Instance
- QCS::CBS::Disk
Instance - CBS
- QCS::VPC::Vpc
VPC - VPC
- QCS::VPC::SecurityGroup
VPC - Security group
- QCS::VPC::Subnet
VPC - Subnet

Hold down on the Shift key to select multiple items

Selected (5)

Resource type	
QCS::CVM::Instance CVM - Instance	✕
QCS::CBS::Disk Instance - CBS	✕
QCS::VPC::Vpc VPC - VPC	✕
QCS::VPC::SecurityGroup VPC - Security group	✕
QCS::VPC::Subnet VPC - Subnet	✕

Delivery Service

Last updated: 2024-03-04 14:13:25

Delivering Resource Configuration Change Records

You can choose **Settings > Delivery Service** in the left sidebar to go to the **Delivery service** page. On this page, you can **enable** and configure the delivery service to deliver the resource configuration change records on the resource timeline page to the specified COS bucket regularly. This allows for a more detailed analysis and longer-term storage of the resource configuration data.

Delivery service
①After the delivery service is enabled, Config will deliver the resource configuration change records to the specified log file at 00:00 AM every day. Due to a large data volume, it takes about 15 minutes to deliver resource configuration snapshots, after which the data will be updated in the log file.

Current account

Disabled

Delivery service
①After the delivery service is enabled, Config will deliver the resource configuration change records to the specified log file at 00:00 AM every day. Due to a large data volume, it takes about 15 minutes to deliver resource configuration snapshots, after which the data will be updated in the log file.

Current account

Enabled

Delivery type *

Delivery service name *
Supports up to 20 characters consisting of English characters

COS bucket * Existing bucket Create bucket

Log file prefix *
Supports up to 30 characters consisting of only letters and numbers.

Encryption mode * Not encrypted SSE-COS

Upon activating the delivery service, the configuration audit will deliver the resource configuration change history to your designated COS bucket daily at 00:00 when the timeline is updated. When you **Disable** the delivery service, updates to the timeline will not be stored in the corresponding bucket.

Once the delivery service is enabled, Config delivers the resource configuration changes to the specified COS bucket at 00:00 every day if the change records are updated on the timeline page. If the service is **disabled**, resource configuration record updates on the timeline page will not be delivered to the corresponding bucket.

Delivery service

①After the delivery service is enabled, Config will deliver the resource configuration change records to the specified log file at 00:00 AM every day. Due to a large data volume, it takes about 15 minutes to deliver resource configuration snapshots, after which the data will be updated in the log file.

Current account Enabled

Delivery service name

[Edit](#)

COS bucket

Region

Log file prefix

configtk

Encryption mode

Not encrypted

Are you sure you want to deactivate the delivery service?

If you disable the feature, delivery will be stopped, and data already delivered to the bucket will be retained. Are you sure you want to disable the feature?

[OK](#)[Cancel](#)

Config will take about 10 minutes to pull resource configuration snapshots and deliver them to the COS bucket. Therefore, a certain delay exists for data updates in the COS bucket. Please wait patiently.

Resource Snapshot Update

Last updated: 2024-03-04 14:13:26

Click on **Update**, the system will promptly retrieve the latest resource snapshot data, and update the resource list and corresponding resource timeline based on the captured most recent resource snapshot data.

After you click **Update**, the system will promptly pull the latest resource snapshot data and update the resource list and corresponding resource configuration records on the timeline page based on the captured resource snapshot data.

Update resource snapshot

Resource snapshot update (manual)

Update

After manual update, the system immediately pulls the latest resource snapshot data. If the resource or configuration changes, the system updates the resource list and the corresponding resource timeline. It takes 15 minutes to pull, generate, and update the snapshot data.