

Tencent Smart Advisor

Operation Guide

Product Documentation



Copyright Notice

©2013-2024 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 Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. 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

Inspection Report

- Generating Report

- Subscribing to Report

- Managing Custom Report Templates

Assessment Items

- Enabling/Disabling Assessment Items

- Modifying Custom Rules

- Ignoring/Adding Resources

Risks

- Querying Risk Trends

- Querying Risk Details

Permission Management

- Role Permissions Related to Service Authorization

Operation Guide

Inspection Report

Generating Report

Last updated : 2022-11-07 11:20:44

Overview

This document describes how to generate Excel or PDF risk assessment reports in the Tencent Smart Advisor console.

Prerequisites

You need to complete the risk assessment.

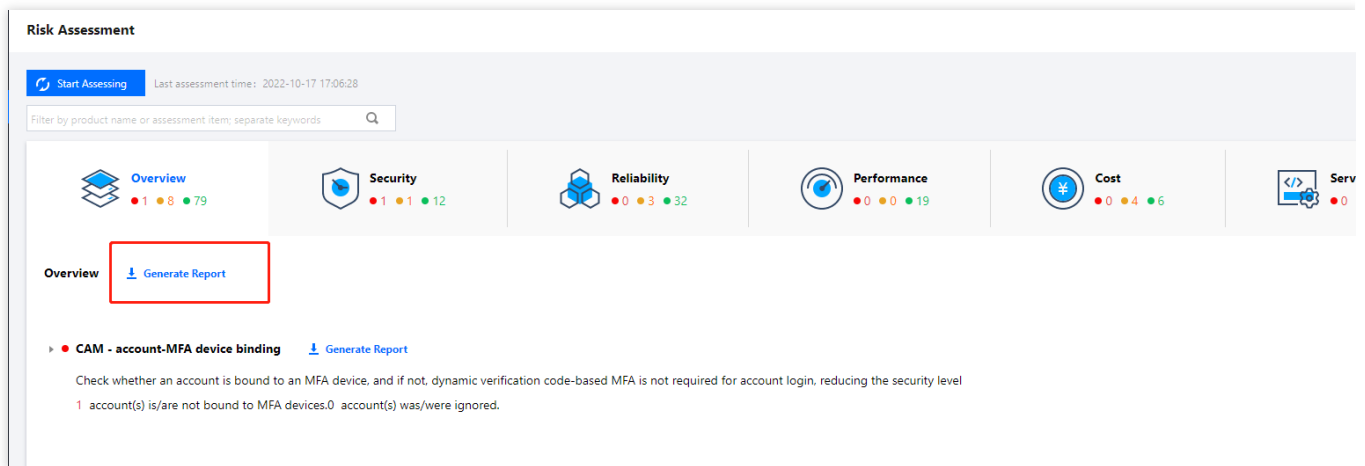
If the assessment is not performed, start one.

If the assessment is underway, wait for it to complete.

Directions

1. Log in to the Tencent Smart Advisor console and select **Risk Assessment** on the left sidebar.
2. On the **Risk Assessment** page, select a assessment type or module to generate the report (overview, security, reliability, performance, cost, and service restriction).
3. Generate the report:

Generating the report for the specific module: Click **Generate Report** on the first line of the module.



Risk Assessment

[Start Assessing](#) Last assessment time: 2022-10-17 17:06:28

Filter by product name or assessment item; separate keywords

Overview [Generate Report](#)

Security [Generate Report](#)

Reliability [Generate Report](#)

Performance [Generate Report](#)

Cost [Generate Report](#)

Serv [Generate Report](#)

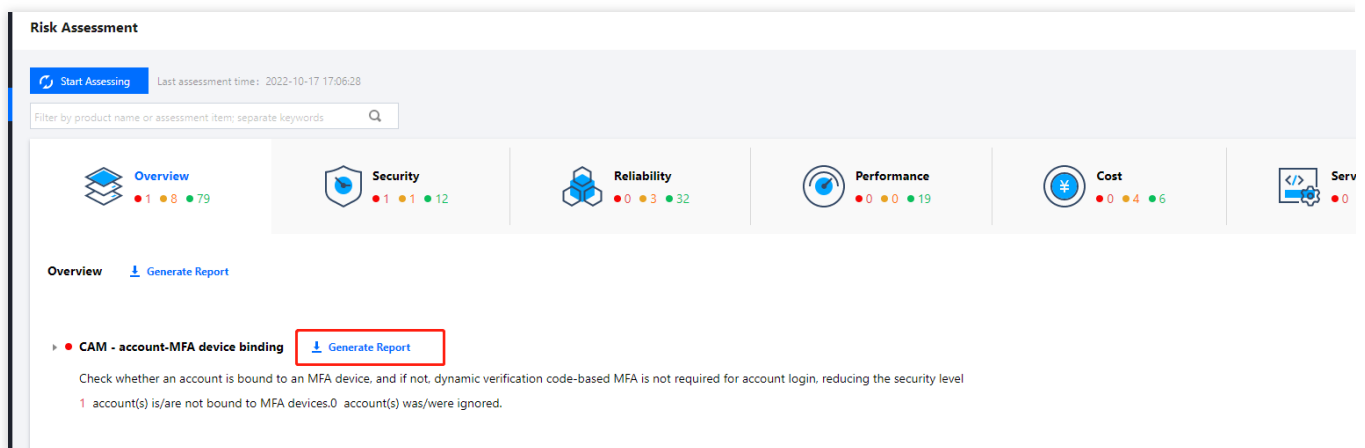
Overview [Generate Report](#)

► **CAM - account-MFA device binding** [Generate Report](#)

Check whether an account is bound to an MFA device, and if not, dynamic verification code-based MFA is not required for account login, reducing the security level

1 account(s) is/are not bound to MFA devices.0 account(s) was/were ignored.

Generating the report for the specific inspection item: Click **Generate Report** next to the specific inspection item.



Risk Assessment

[Start Assessing](#) Last assessment time: 2022-10-17 17:06:28

Filter by product name or assessment item; separate keywords

Overview [Generate Report](#)

Security [Generate Report](#)

Reliability [Generate Report](#)

Performance [Generate Report](#)

Cost [Generate Report](#)

Serv [Generate Report](#)

Overview [Generate Report](#)

► **CAM - account-MFA device binding** [Generate Report](#)

Check whether an account is bound to an MFA device, and if not, dynamic verification code-based MFA is not required for account login, reducing the security level

1 account(s) is/are not bound to MFA devices.0 account(s) was/were ignored.

4. Click **Download Report**.

5. In the **Download Assessment Report** pop-up window, select **Assessment report in Excel** or **Assessment report in PDF** as needed and click **OK**.

Subscribing to Report

Last updated : 2022-11-07 11:20:44

Overview

Tencent Smart Advisor provides report subscription feature to email users their inspection reports. This document describes how to manage your subscriptions in the console, including creating, enabling/disabling, modifying, and deleting a subscription.

Directions

Creating a subscription

1. Log in to the Tencent Smart Advisor console and select **Email Notification** on the left sidebar.
2. On the **Subscriptions** tab, click **Create**.
3. In the **Create Subscription** pop-up window, enter the **Subscription Name**, toggle on **Enable**, and set the **Frequency**, **Time**, **Report Templates**, and **Email**.

Create Subscription ✕

Subscription Name

Enable ⓘ

Frequency Daily Weekly

Time 🕒

Email Email is not set. [Add Now](#)

Report Templates Default (all) ▾

Report Language English ▾

4. Click **Create**.

Enabling/Disabling a subscription

On the **Subscriptions** page, you can toggle on the **Enable/Disable** switch to enable/disable a subscription.

Email Notification

Subscriptions Report Templates

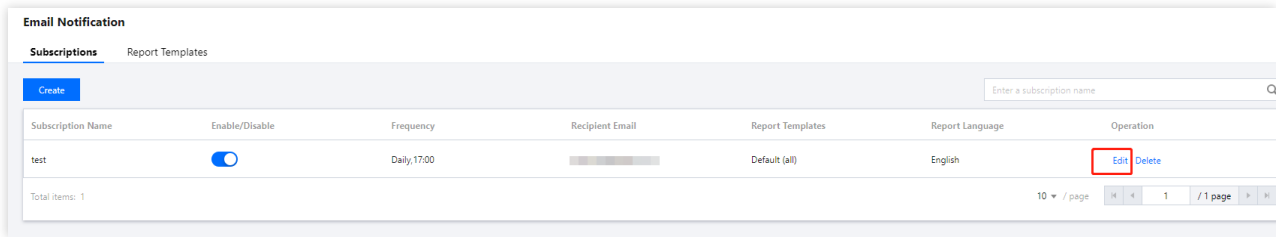
🔍

Subscription Name	Enable/Disable	Frequency	Recipient Email	Report Templates	Report Language	Operation
test	<input checked="" type="checkbox"/>	Daily, 17:00	<input type="text"/>	Default (all)	English	Edit Delete

Total items: 1 10 / page ⏪ ⏩ 1 / 1 page ⏪ ⏩

Modifying a subscription

1. On the **Subscriptions** page, click **Edit** on the right of the target subscription.

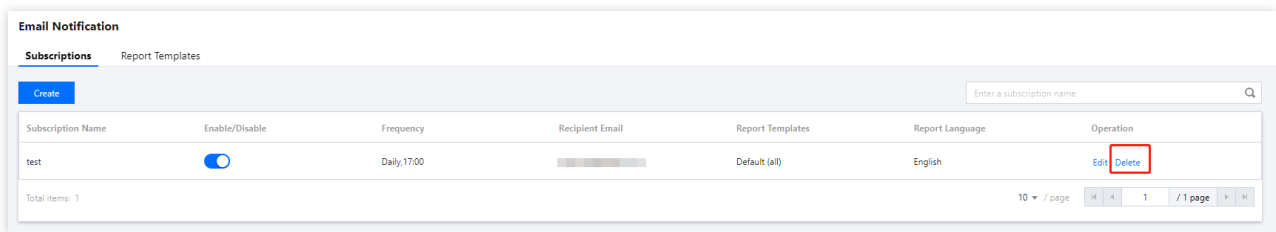


2. In the **Edit Subscription** pop-up window, edit the parameters.

3. Click **OK**.

Deleting a subscription

1. On the **Subscriptions** page, click **Delete** on the right of the target subscription.



2. In the pop-up window, click **Delete**.

Managing Custom Report Templates

Last updated : 2022-11-07 11:20:45

Overview

When creating a subscription report, you can use the default or custom template. This document describes how to custom a report template in the dimension of product, risk type, or tag and modify or delete the report in the Tencent Smart Advisor console.

Directions

Creating a template

1. Log in to the Tencent Smart Advisor console and select **Email Notification** on the left sidebar.
2. On the **Report Templates** tab, click **Create**.
3. In the **Create Template** pop-up window, enter the **Template Name** and select the **Product**, **Risk Type**, and **Tag**.

Create Template X

Template Name

Product All ▾

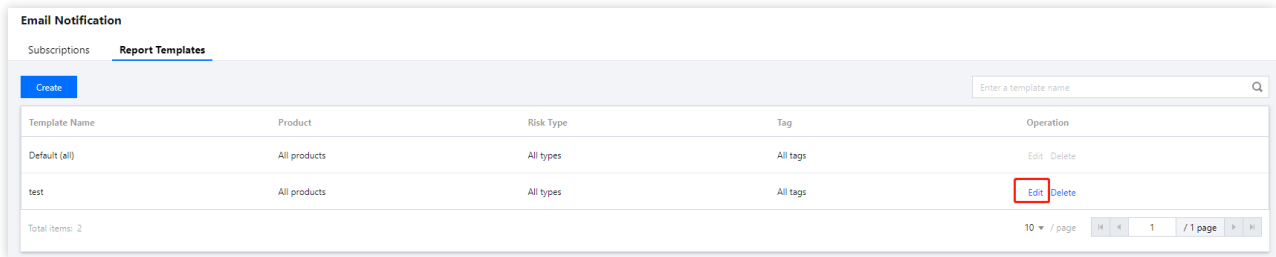
Risk Type All
 Security Reliability Service limits Cost Performance

Tag No tag selected (all resources selected) [Add Tag](#)

4. Click **Create**.

Modifying a template

1. On the **Email Notification** page, click **Edit** on the right of the target template.



Email Notification

Subscriptions **Report Templates**

Create

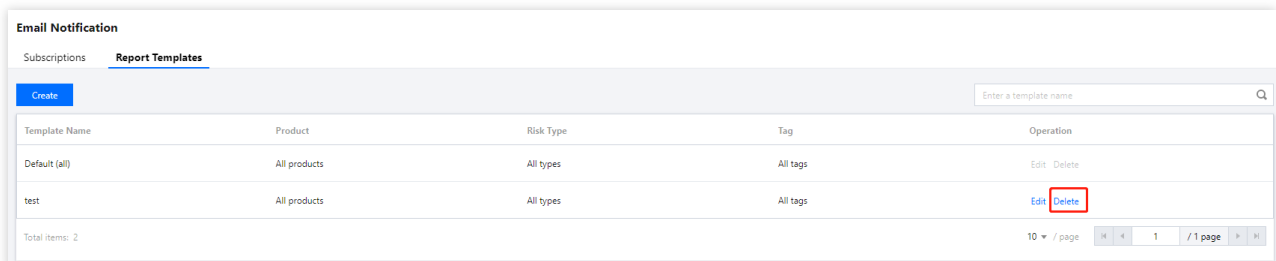
Template Name	Product	Risk Type	Tag	Operation
Default (all)	All products	All types	All tags	Edit Delete
test	All products	All types	All tags	Edit Delete

Total items: 2 10 / page 1 / 1 page

2. In the **Edit Template** pop-up window, edit the information and click **OK**.

Deleting a template

1. On the **Email Notification** page, click **Delete** on the right of the target template.



Email Notification

Subscriptions **Report Templates**

Create

Template Name	Product	Risk Type	Tag	Operation
Default (all)	All products	All types	All tags	Edit Delete
test	All products	All types	All tags	Edit Delete

Total items: 2 10 / page 1 / 1 page

2. In the pop-up window, click **Delete**.

Assessment Items

Enabling/Disabling Assessment Items

Last updated : 2022-11-07 11:20:45

Overview

This document describes how to enable and disable assessment items in the Tencent Smart Advisor console. A disabled item will be excluded from the next inspection.

Directions

1. Log in to the Tencent Smart Advisor console and select **Assessment Items** on the left sidebar.
2. On the **Assessment Settings** page, toggle on or off the **Switch** to enable or disable an assessment item.

Type	Product	Assessment Item	Description	Switch	Operation
Reliability	CBS	CBS - storage capacity	Check the storage capacity usage of CBS cloud disks. If the capacity utilization is excessive, cloud disk read/write will be affected	<input checked="" type="checkbox"/>	Modify rules
Reliability	CBS	CBS - no snapshots created	Check whether CBS cloud disks have snapshots or are configured with a scheduled snapshot policy, and if not, it will be difficult to ...	<input checked="" type="checkbox"/>	Modify rules
Reliability	Ckafka	Ckafka - multi-AZ deployment	If the instances are not deployed across AZs, when a severe fault occurs in the single-AZ Ckafka cluster, the cluster may become un...	<input checked="" type="checkbox"/>	Modify rules
Reliability	CLB	CLB - health check configuration	Check whether health check is configured for CLB instances, and if not, CLB will forward traffic to all real servers (including exceptio...	<input checked="" type="checkbox"/>	Modify rules
Reliability	CLB	CLB - forwarding rule configuration	Check the listener configuration of CLB instances. If no forwarding rules are configured, CLB features cannot be used normally, and ...	<input checked="" type="checkbox"/>	Modify rules
Reliability	COS	COS - bucket versioning	Check the versioning configuration of COS buckets. If it is not enabled, data may be lost	<input checked="" type="checkbox"/>	Modify rules
Reliability	COS	COS - log management configuration of buckets	Check the log management feature of COS buckets. If the owners of the destination and source buckets are different, bucket log sh...	<input checked="" type="checkbox"/>	Modify rules
Reliability	CVM	CVM - system disk snapshot	Check CVM system disk snapshots. If no snapshots are created, it will be difficult to recover the data when a server or cloud disk is ...	<input checked="" type="checkbox"/>	Modify rules
Reliability	CVM	CVM - excessive instance disk space utilization	Check the disk utilization of CVM instances. If the utilization is excessive, disk read/write will be affected	<input checked="" type="checkbox"/>	Modify rules
Reliability	CVM	CVM - instance local disk type	Check the local disk usage of CVM instances. If an instance is not an I/O or Big Data model but uses a local disk, its disk data canno...	<input checked="" type="checkbox"/>	Modify rules

Total items: 89

10 / page 1 / 9 pages

Modifying Custom Rules

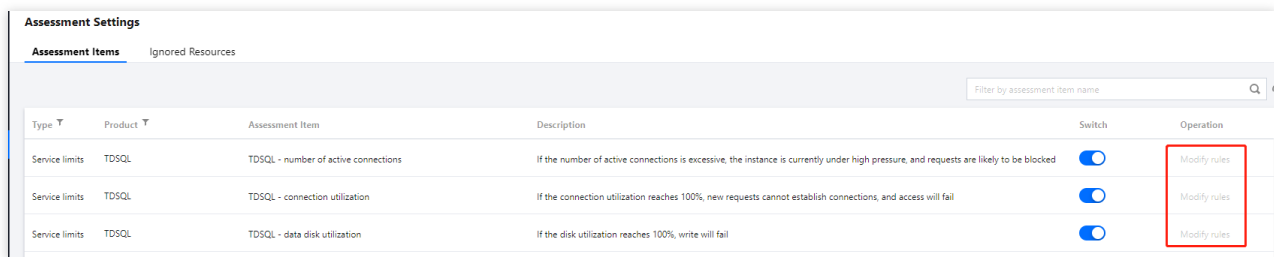
Last updated : 2022-11-07 11:20:45

Overview

You can customize rules for some assessment items for CVM, CBS, TencentDB, etc. as needed. This document describes how to modify risk assessment rules in the Tencent Smart Advisor console.

Directions

1. Log in to the Tencent Smart Advisor console and select **Assessment Items** on the left sidebar.
2. On the **Assessment Items** page, click **Modify rules** on the right of the target item.



The screenshot shows the 'Assessment Settings' page in the Tencent Smart Advisor console. The 'Assessment Items' tab is selected, and a search bar is visible. The table below lists three assessment items, each with a 'Modify rules' button highlighted in a red box.

Type	Product	Assessment Item	Description	Switch	Operation
Service limits	TDSQL	TDSQL - number of active connections	If the number of active connections is excessive, the instance is currently under high pressure, and requests are likely to be blocked	<input checked="" type="checkbox"/>	Modify rules
Service limits	TDSQL	TDSQL - connection utilization	If the connection utilization reaches 100%, new requests cannot establish connections, and access will fail	<input checked="" type="checkbox"/>	Modify rules
Service limits	TDSQL	TDSQL - data disk utilization	If the disk utilization reaches 100%, write will fail	<input checked="" type="checkbox"/>	Modify rules

3. In the **Modify rules** pop-up window, modify the risk trigger condition as needed.
4. Click **Confirm**.

Ignoring/Adding Resources

Last updated : 2022-11-07 11:20:45

Overview

Tencent Smart Advisor allows you to ignore and exclude the following resources from inspections:

Resources with a specified tag key and value

Instances

Resources set to **Ignored** can be added to inspections again as needed.

Note:

To add or ignore resources through tag keys and values, you need to add tags to resources. For detailed directions, see [Creating Tags and Binding Resources](#).

Directions

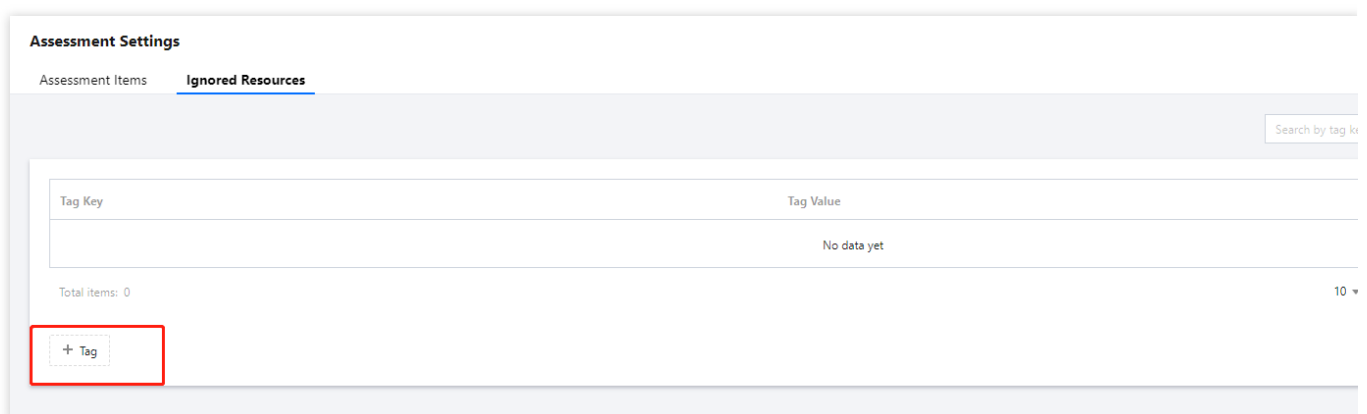
Ignoring resources

You can specify resources to be excluded from inspections in the following ways:

Ignoring resources by tag

Ignoring resources by instance

1. Log in to the Tencent Smart Advisor console and select **Assessment Items** on the left sidebar.
2. On the **Assessment Settings** page, select the **Ignored Resources** tab and click **+ Tag**.



3. Expand the **Tag Key** and **Tag Value** drop-down lists and select the tag key and value to be ignored.

4. Click **Save**, and resources with the selected tag key and value will be excluded from inspections.

1. Log in to the Tencent Smart Advisor console and select **Risk Assessment** on the left sidebar.
2. Click the assessment items to expand them, click the **Assessed Resource** tab, and select the target instance.

Overview [Generate Report](#)

CAM - account-MFA device binding [Generate Report](#)

Check whether an account is bound to an MFA device, and if not, dynamic verification code-based MFA is not required for account login, reducing the security level

Alarm Condition

- No MFA devices are bound for both login and sensitive operations
- No MFA devices are bound for login or sensitive operations

Optimization Advice

We recommend you bind your account to a [virtual MFA device](#) in the console to add another layer of security verification for relevant account operations and thus protect the account security

Resource List

1 account(s) is/are not bound to MFA devices.0 account(s) was/were ignored.

Assessed Resource Ignored Resources

[Ignore](#) [Restore](#)

Separate keywords with ";" press Enter

<input checked="" type="checkbox"/>	UIN	Sub Account Count	Tag	Operation ⓘ
<input checked="" type="checkbox"/>	● 	4	None	Ignore Restore

Total items: 1 10 / page

3. Click **Ignore**, and the instance will be excluded from inspections.

Adding resources

You can add ignored resources to inspections in the following ways:

Adding resources by tag

Adding resources by instance

- Log in to the Tencent Smart Advisor console and select **Assessment Items** on the left sidebar.
- On the **Assessment Settings** page, select the **Ignored Resources** tab.
- Modify or delete a configured tag key and value as needed to add corresponding resources to inspections:

Edit: Click **Edit** on the right of the target tag and modify the information as needed.

Assessment Settings

Assessment Items **Ignored Resources**

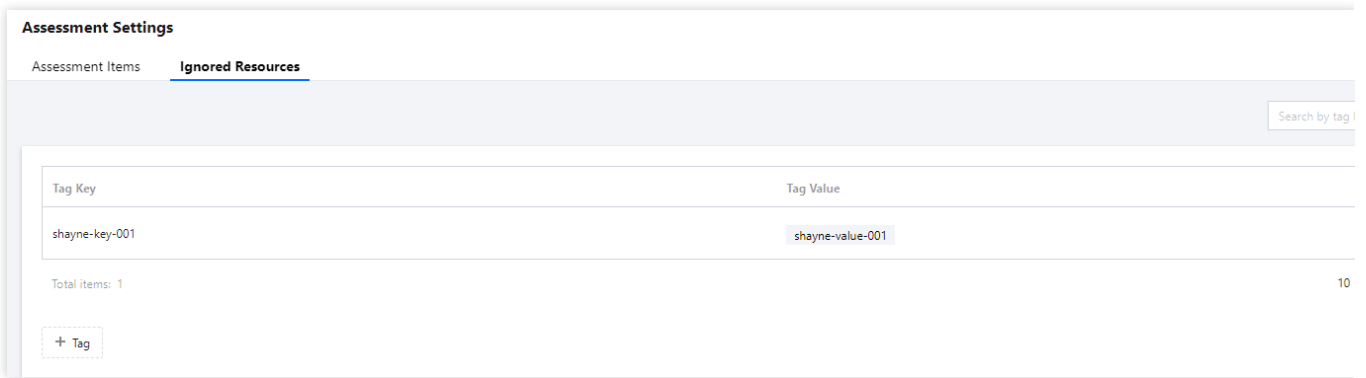
Search by tag

Tag Key	Tag Value
shayne-key-001	shayne-value-001

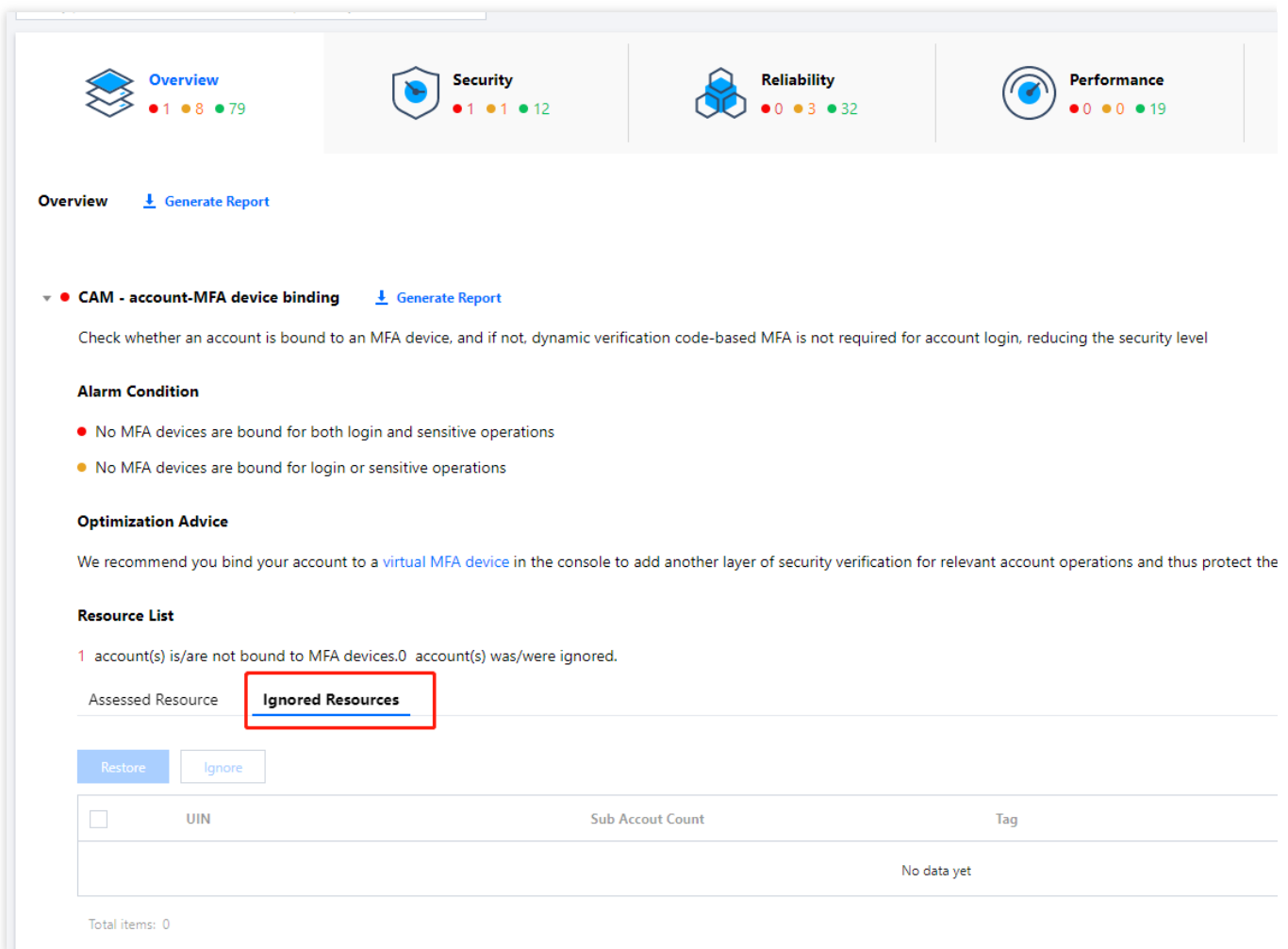
Total items: 1 10

[+ Tag](#)

Delete: Click **Delete** on the right of the target tag to delete it.



1. Log in to the Tencent Smart Advisor console and select **Risk Assessment** on the left sidebar.
2. Click the assessment items to expand them, click the **Ignored Resources** tab, and select the target instance.



3. Click **Add**, and the instance will be added to inspections.

Risks

Querying Risk Trends

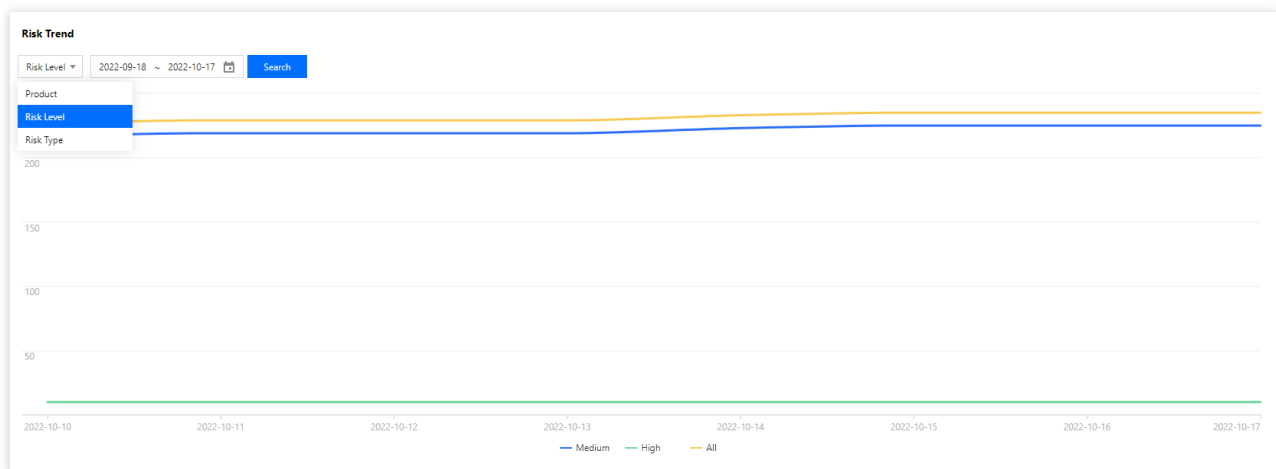
Last updated : 2022-11-07 11:20:45

Overview

This document describes how to query risk trends in the past 30 days in the Tencent Smart Advisor console.

Directions

1. Log in to the Tencent Smart Advisor console and select **Risks** on the left sidebar.
2. On the **Risks** page, select the dimension (product, risk level, or risk type) for trend analysis and the time range and then click **Search**.



Querying Risk Details

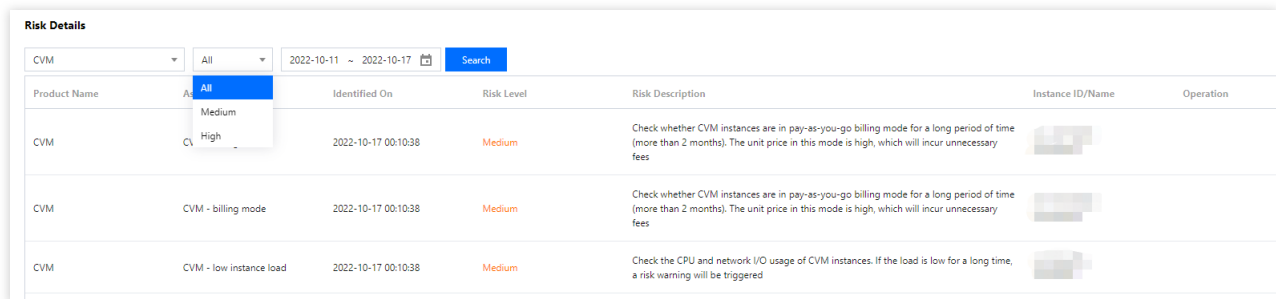
Last updated : 2022-11-07 11:20:45

Overview

This document describes how to query risk details in the past 30 days in the Tencent Smart Advisor console.

Directions

1. Log in to the Tencent Smart Advisor console and select **Risks** on the left sidebar.
2. On the **Risk Details** tab, select the product, risk level, and time range and then click **Search**.



The screenshot shows the 'Risk Details' interface in the Tencent Smart Advisor console. At the top, there are filters for 'CVM', 'All', and a date range from '2022-10-11' to '2022-10-17'. A 'Search' button is also present. Below the filters is a table with the following columns: Product Name, Risk Level, Risk Description, and Instance ID/Name. The table contains three rows of risk information, all with a 'Medium' risk level.

Product Name	Risk Level	Risk Description	Instance ID/Name
CVM	Medium	Check whether CVM instances are in pay-as-you-go billing mode for a long period of time (more than 2 months). The unit price in this mode is high, which will incur unnecessary fees	[Redacted]
CVM - billing mode	Medium	Check whether CVM instances are in pay-as-you-go billing mode for a long period of time (more than 2 months). The unit price in this mode is high, which will incur unnecessary fees	[Redacted]
CVM - low instance load	Medium	Check the CPU and network I/O usage of CVM instances. If the load is low for a long time, a risk warning will be triggered	[Redacted]

Permission Management

Role Permissions Related to Service Authorization

Last updated : 2022-11-07 11:20:45

When you use Tencent Smart Advisor, in order to use Tencent Cloud resources, you will encounter a variety of scenarios that require service authorization. Each scenario usually involves preset policies for different roles. Here, the

`Advisor_QCSLinkedRoleInBusinessContinuity` role and

`QcloudAccessForAdvisorLinkedRoleInBusinessContinuity` preset policy are mainly involved. This document details authorization policies, scenarios, and directions.

Role Authorization

Role name

`Advisor_QCSLinkedRoleInBusinessContinuity`

Permission description

After Tencent Smart Advisor is activated on the [Service Authorization](#) page, Tencent Cloud will grant your account the `Advisor_QCSLinkedRoleInBusinessContinuity` role. By default, the role is associated with the `QcloudAccessForAdvisorLinkedRoleInBusinessContinuity` preset policy, which grants Tencent Smart Advisor access to CVM, VPC, TencentDB, and other Tencent Cloud resources under your account.

Preset Policy

Policy name

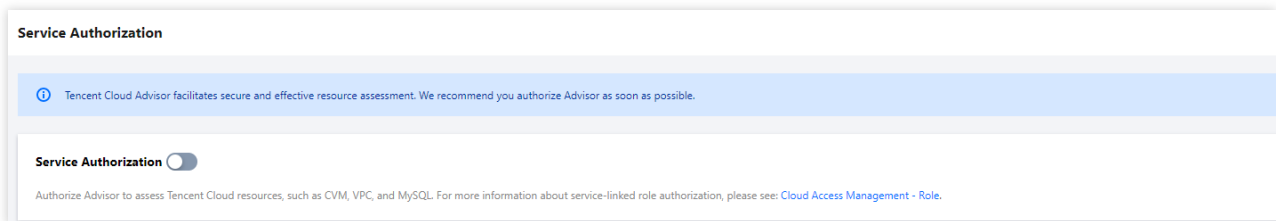
`QcloudAccessForAdvisorLinkedRoleInBusinessContinuity`

Authorization scenario

When you log in to the [Tencent Smart Advisor console](#) for the first time after registering and logging in to a Tencent Cloud account, you need to go to the **Cloud Access Management** page to grant Tencent Smart Advisor permissions to manipulate CVM, VPC, TencentDB, and other Tencent Cloud resources.

Authorization steps

1. Log in to the Tencent Smart Advisor console and select **Authorization** on the left sidebar.
2. On the **Service Authorization** page, enable **Service Authorization**.



3. In the **Authorize** pop-up window, click **Cloud Access Management** to enter the CAM console.
4. On the **Role Management** page, click **Grant** to complete authentication.

