Optimization Advisor

User Guide

Issue 1.2

Date 2025-08-28

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

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

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

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: https://www.huawei.com

Email: support@huawei.com

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process*. For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

1 Risk Check

1.1 Overview

Scenarios

Risk Check helps you check cloud resources in terms of performance efficiency, reliability, security, cost optimization, and service quotas. It also provides a flexible mode for performing dedicated checks by cloud service type. This function can accurately identify potential risks and provide optimization suggestions. It helps you remove risks and enhance resource efficiency, maintaining reliable and stable cloud operations.

Functions

Risk Check provides the following functions:

- Proactive check
- Check report download
- Check with a single check item and download of its check report
- Automatic inspection: You can subscribe to check reports and enable scheduled checks.
- Custom check rules
- Optimization suggestions

Check Results

There are three types of check results:

- **Risky**: Services are affected to different degrees after a fault.
- **Safe**: There is no risk for the checked cloud service.
- **N/A**: The cloud service is not used or the service scenario is not involved.

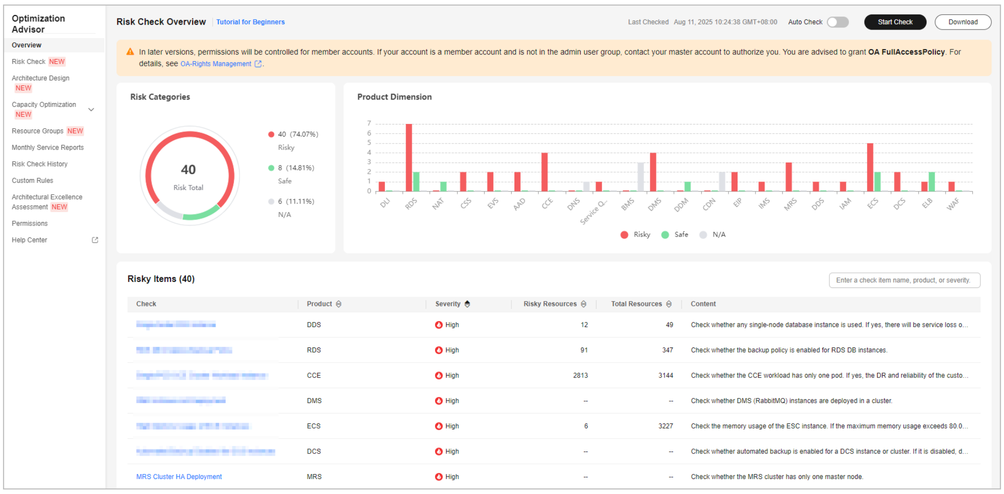
Risk Levels

There are three types of risk levels:

- **High-risk**: Services are interrupted after a fault.
- **Medium-risk**: Services are affected but the impact is controllable.
- **Low-risk**: Services are slightly affected after a fault.

1.2 Proactive Checks

You can learn about frequently used check functions on the **Overview** page.



In later versions, permissions will be controlled for member accounts. If your account is a member account and is not in the admin user group, contact your master account to authorize you. You are advised to grant **OA FullAccessPolicy**. For details, see OA-Rights Management.

Risky Items (40)

Check	Product	Severity	Risky Resources	Total Resources	Content
[redacted]	DDS	High	12	49	Check whether any single-node database instance is used. If yes, there will be service loss o...
[redacted]	RDS	High	91	347	Check whether the backup policy is enabled for RDS DB instances.
[redacted]	CCE	High	2813	3144	Check whether the CCE workload has only one pod. If yes, the DR and reliability of the custo...
[redacted]	DMS	High	--	--	Check whether DMS (RabbitMQ) instances are deployed in a cluster.
[redacted]	ECS	High	6	3227	Check the memory usage of the ESC instance. If the maximum memory usage exceeds 80.0...
[redacted]	DCS	High	--	--	Check whether automated backup is enabled for a DCS instance or cluster. If it is disabled, d...
MRS Cluster HA Deployment	MRS	High	--	--	Check whether the MRS cluster has only one master node.

Procedure

Step 1 Log in to the Huawei Cloud management console.

Step 2 In the upper left corner of the homepage, click ☰ to expand the service list and choose **Management & Governance** > **Optimization Advisor**.

Step 3 In the navigation pane, choose **Overview**.

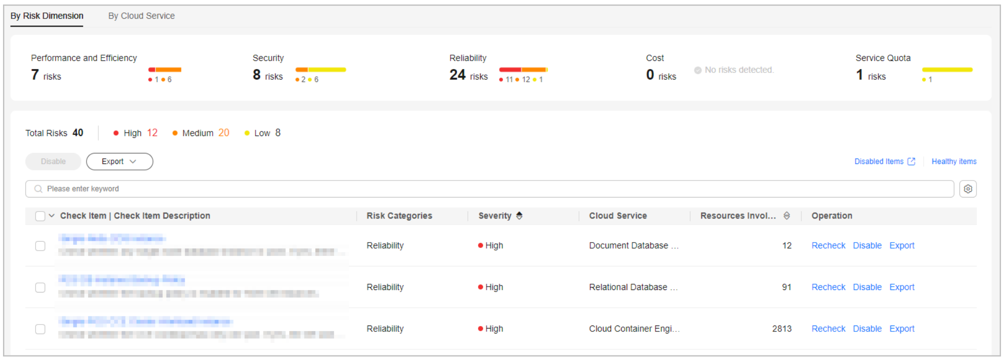
Step 4 Click **Start Check** in the upper right corner, set the check account and risk dimension, and start the check.

Step 5 After the check progress reaches 100%, check that the check results are automatically updated on the risk check overview page.

The check results consist of risk dimension statistics, risky product statistics, and the risky item list. You can click a check item to view its details.

Step 6 Alternatively, click **Risk Check** in the navigation pane to go to the **Risk Check Overview** page. You can view the check results by risk dimension or cloud service type.

- **By Risk Dimension**: The check results consist of risk dimension statistics, risk severities, and the risky item list. You can click a risky item to view its details.



By Risk Dimension | By Cloud Service

Performance and Efficiency
7 risks ● 1 ● 6

Security
8 risks ● 2 ● 6

Reliability
24 risks ● 11 ● 12 ● 1

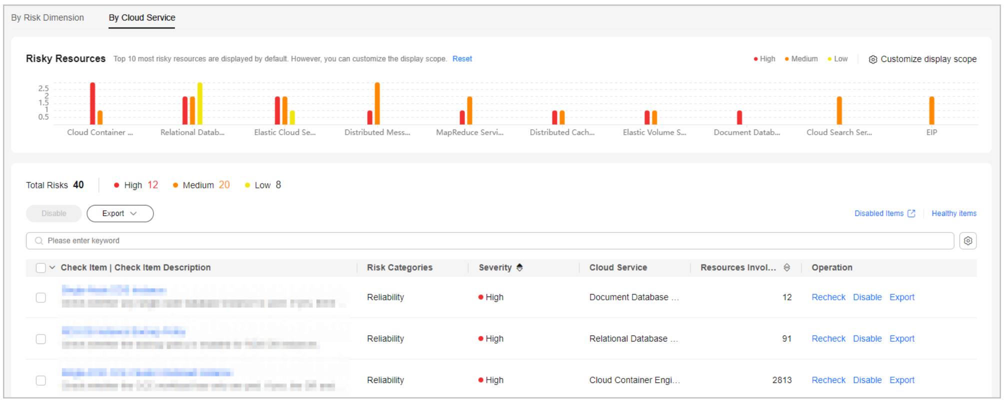
Cost
0 risks ○ No risks detected.

Service Quota
1 risks ● 1

Total Risks 40 | ● High 12 ● Medium 20 ● Low 8

□ Check Item | Check Item Description	Risk Categories	Severity	Cloud Service	Resources Invol...	Operation
□ [redacted]	Reliability	● High	Document Database ...	12	Recheck Disable Export
□ [redacted]	Reliability	● High	Relational Database ...	91	Recheck Disable Export
□ [redacted]	Reliability	● High	Cloud Container Engi...	2813	Recheck Disable Export

- **By Cloud Service**: The check results consist of a bar chart of risky resources and the risky item list. You can click a risky item to view its details.



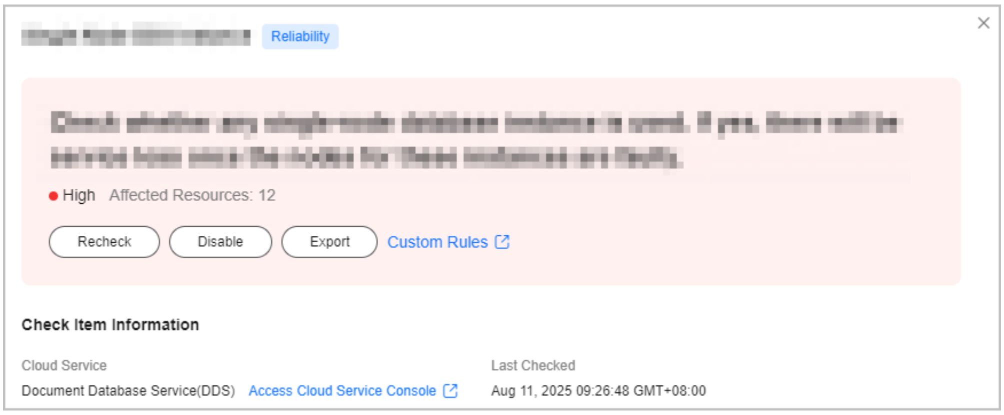
By Risk Dimension | By Cloud Service

Risky Resources Top 10 most risky resources are displayed by default. However, you can customize the display scope. Reset

Total Risks 40 | ● High 12 ● Medium 20 ● Low 8

□ Check Item | Check Item Description	Risk Categories	Severity	Cloud Service	Resources Invol...	Operation
□ [redacted]	Reliability	● High	Document Database ...	12	Recheck Disable Export
□ [redacted]	Reliability	● High	Relational Database ...	91	Recheck Disable Export
□ [redacted]	Reliability	● High	Cloud Container Engi...	2813	Recheck Disable Export

Step 7 After rectifying risky resources, you can re-check your resources using a single check item to verify the rectification. Click **Recheck** to refresh the check result.



[redacted] Reliability

[redacted]

● High Affected Resources: 12

Check Item Information

Cloud Service
Document Database Service(DDS) Access Cloud Service Console

Last Checked
Aug 11, 2025 09:26:48 GMT+08:00

----End

1.3 Custom Check Rules

Scenarios

Risk checks automatically include all items by default. The risk thresholds of check items such as resource usage follow standard guidelines but might not suit everyone. You can customize check rules as needed.

Procedure

Step 1 Log in to the Huawei Cloud management console.

Step 2 In the upper left corner of the homepage, click ☰ to expand the service list and choose **Management & Governance** > **Optimization Advisor**.

Step 3 In the navigation pane, choose **Custom Rules**.

Step 4 **Customize a single check rule.**

In the custom rule list, locate a specific check item and click **Enable** or **Disable** in the **Operation** column to enable or disable it. Click **Configure Threshold** to modify the risk threshold of the check item.

Step 5 **Customize check rules in batches.**

Select one or more check items, and click **Enable** or **Disable** above the list to enable or disable them. Click **Restore Initial Settings** to restore the thresholds of the selected check items to the initial settings.

NOTE

- Blue indicates available actions and gray shows unavailable ones. Once you enable a rule, only the **Disable** option is available. When you disable a rule, only the **Enable** option becomes available.
- Currently, you can only customize thresholds for some check items in terms of performance and costs (the cost dimension is available only if you have purchased Business-level or Enterprise-level support plans).
- If you disable or enable a check item, the operation will take effect from the next check, without affecting the result of the last check.

----End

1.4 Risk Reports

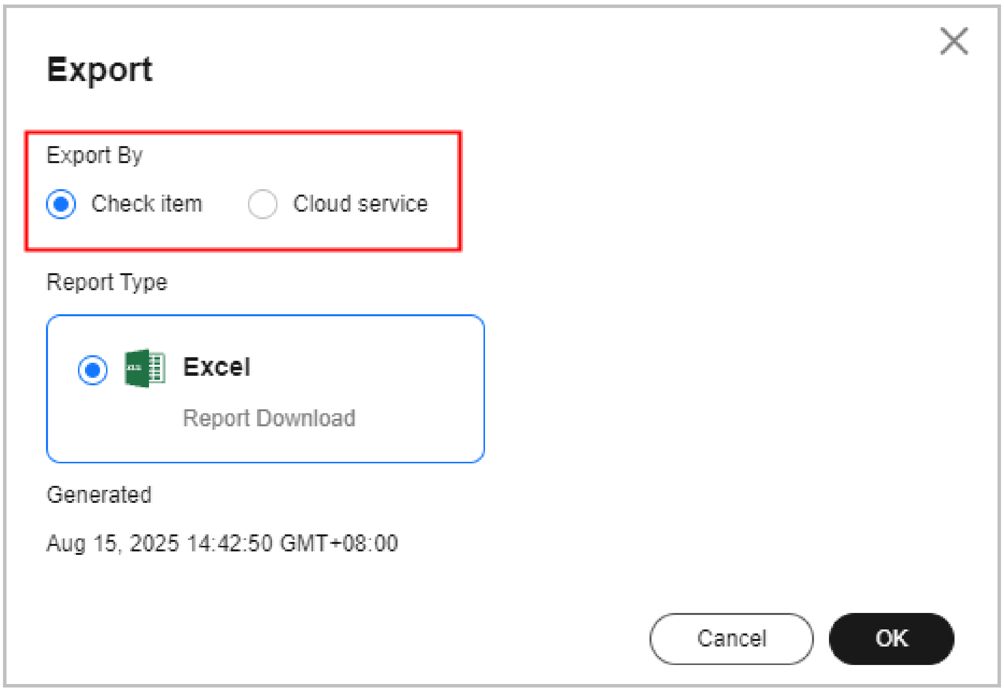
Procedure

Step 1 Log in to the Huawei Cloud management console.

Step 2 In the upper left corner of the homepage, click ☰ to expand the service list and choose **Management & Governance** > **Optimization Advisor**.

Step 3 In the navigation pane, choose **Overview**.

Step 4 Click **Download** in the upper right corner, set **Export By** to **Check item** or **Cloud service**, and select a report type to download the risk check report. The check report is displayed in **Risk Check Overview** and each risk item is displayed on a sheet.



Export

Export By

● Check item ○ Cloud service

Report Type

● Excel

Report Download

Generated

Aug 15, 2025 14:42:50 GMT+08:00

Cancel OK

Step 5 Export risk reports in either of the following ways:

1. Choose **Risk Check** > **By Risk Dimension** (or **By Cloud Service**), select a check item in the list, and click **Export** in the **Operation** column to download the check report of the check item.
2. Select **Risk Check History**. The check records and check results within the last month are displayed. Click a task No. to go to its details page. Click **Download** in the upper right corner to download the check report.

----End

1.5 Auto Checks

Scenarios

Auto Check lets you schedule regular risk checks by setting the interval and time. You can also receive risk check reports. This eases cloud resource management and ensures service stability.

Procedure

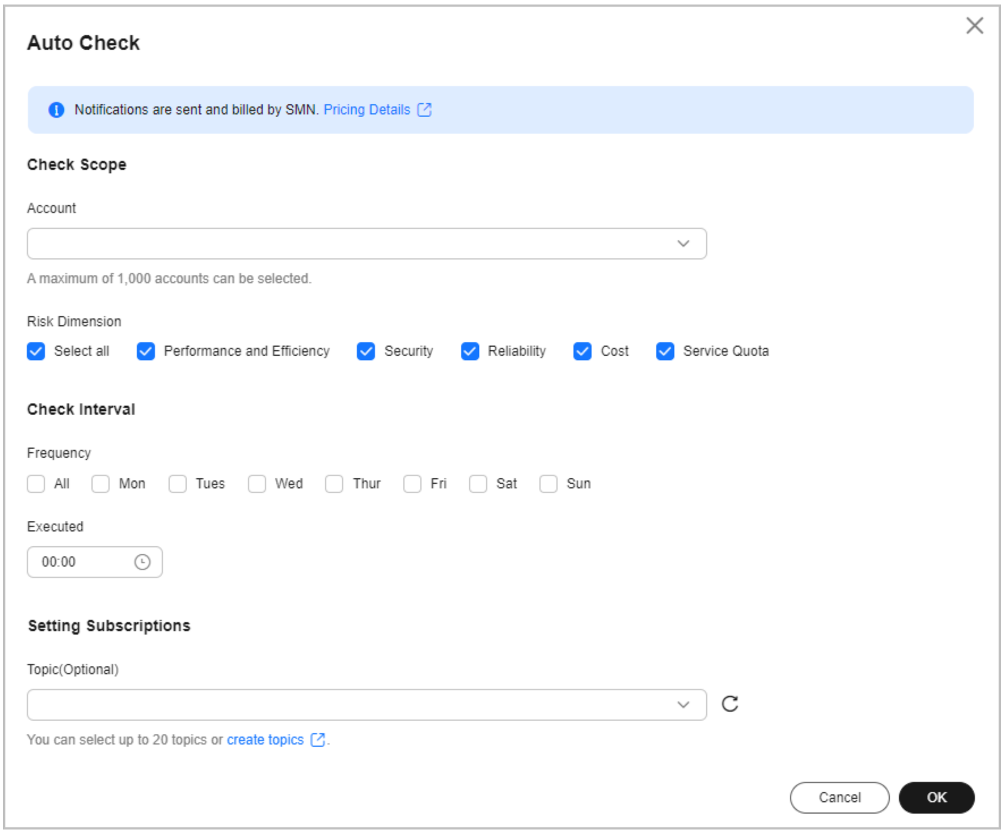
Step 1 Log in to the Huawei Cloud management console.

Step 2 In the upper left corner of the homepage, click ☰ to expand the service list and choose **Management & Governance** > **Optimization Advisor**.

Step 3 In the navigation pane, choose **Overview**.

Step 4 Enable **Auto Check** in the upper right corner.

Step 5 In the displayed dialog box, set the risk dimension, execution frequency, and execution time.



Auto Check

Notifications are sent and billed by SMN. Pricing Details

Check Scope

Account

A maximum of 1,000 accounts can be selected.

Risk Dimension

☑ Select all ☑ Performance and Efficiency ☑ Security ☑ Reliability ☑ Cost ☑ Service Quota

Check Interval

Frequency

□ All □ Mon □ Tues □ Wed □ Thur □ Fri □ Sat □ Sun

Executed

00:00

Setting Subscriptions

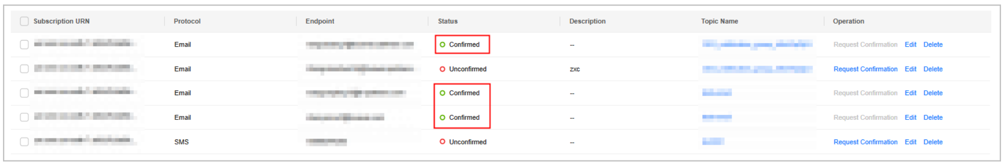
Topic(Optional)

You can select up to 20 topics or create topics.

Step 6 (Optional) Select a notification topic to send the risk report to your mailbox through Simple Message Notification (SMN).

NOTE

- Currently, only topic subscriptions are supported, and the subscription protocol can only be email.
- If no topic is available, you can click **create topics** to go to the SMN console. In the upper right corner of the page, click **Create Topic**. After the topic is created, locate it and click **Add Subscription** in the **Operation** column. Set **Protocol** to **Email** and enter an email address in the **Endpoint** text box. In the navigation pane, choose **Subscriptions**. Locate the newly created subscription URN, click **Request Confirmation** in the **Operation** column, and confirm the subscription in the email.
- Topics can be subscribed to only if their subscription status is **Confirmed**.



□ Subscription URN	Protocol	Endpoint	Status	Description	Topic Name	Operation
□ [redacted]	Email	[redacted]	○ Confirmed	--	[redacted]	Request Confirmation Edit Delete
□ [redacted]	Email	[redacted]	○ Unconfirmed	zxc	[redacted]	Request Confirmation Edit Delete
□ [redacted]	Email	[redacted]	○ Confirmed	--	[redacted]	Request Confirmation Edit Delete
□ [redacted]	Email	[redacted]	○ Confirmed	--	[redacted]	Request Confirmation Edit Delete
□ [redacted]	SMS	[redacted]	○ Unconfirmed	--	[redacted]	Request Confirmation Edit Delete

----End

2 Architecture Design

2.1 Deployment Architecture

2.1.1 Creating a Deployment Architecture

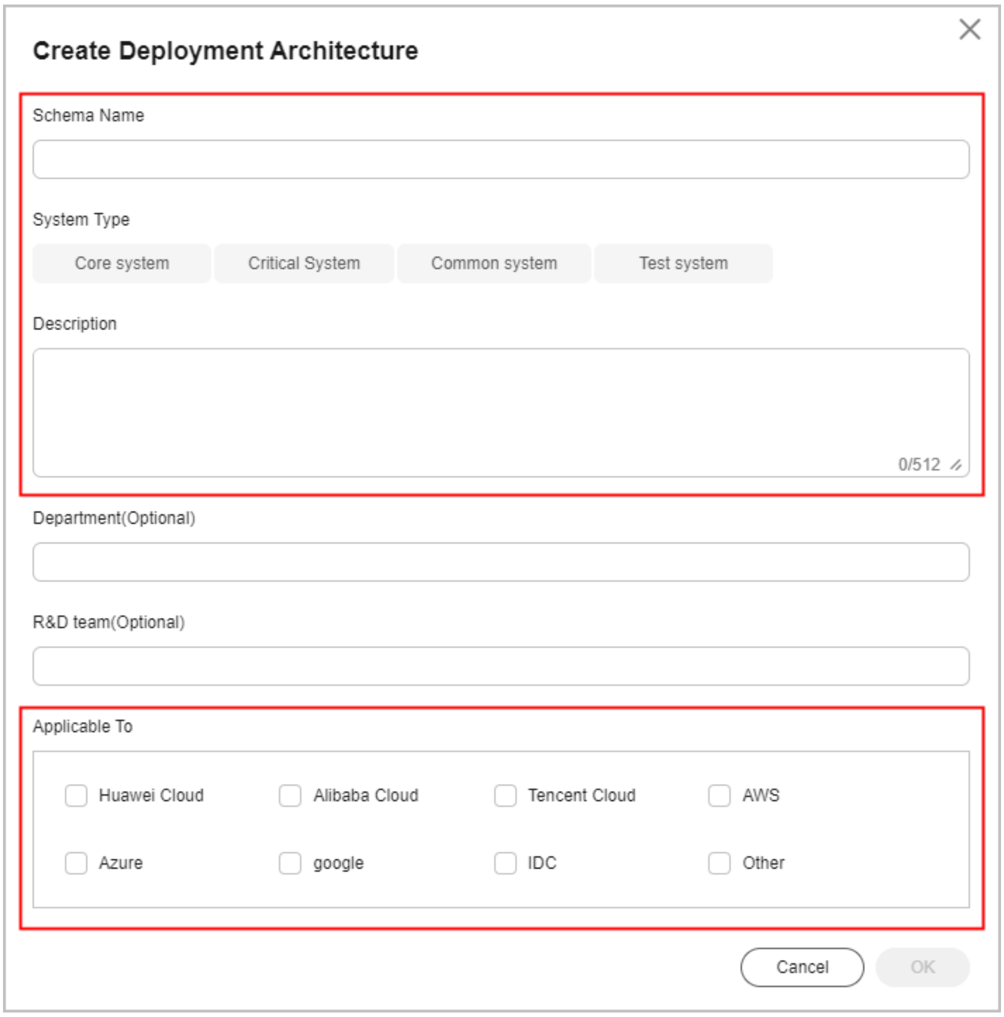
Procedure

Step 1 Log in to the Huawei Cloud management console.

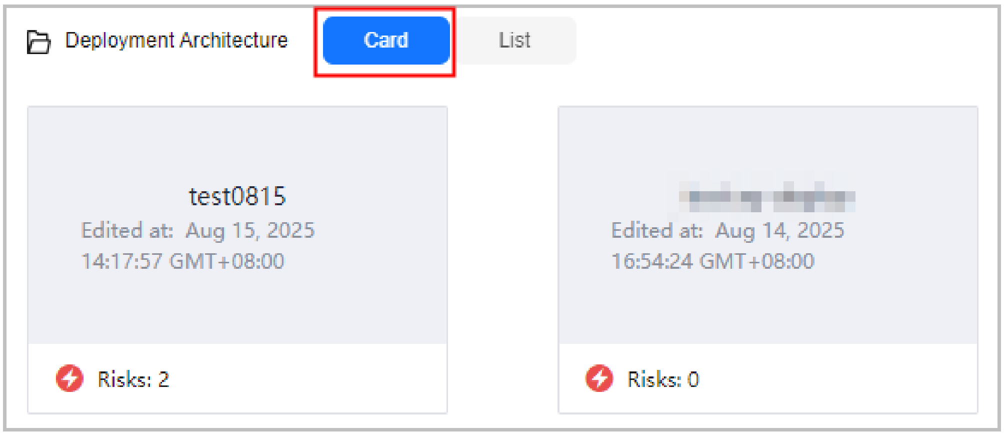
Step 2 In the upper left corner of the homepage, click ☰ to expand the service list and choose **Management & Governance** > **Optimization Advisor**.

Step 3 In the navigation pane, choose **Architecture Design** and click the **Architecture Design** tab.

Step 4 Click **Create Deployment Architecture** in the upper left corner. On the displayed page, enter the architecture name, select the architecture type (no impact on drawing), enter a description about the architecture, and select the deployment status (no impact on drawing).



Step 5 View that the created deployment architecture is displayed in the **Card** view by default.



test0815
Edited at: Aug 15, 2025 14:17:57 GMT+08:00
Risks: 2

[redacted]
Edited at: Aug 14, 2025 16:54:24 GMT+08:00
Risks: 0

----End

2.1.2 Managing a Deployment Architecture

You can view, edit, copy, delete, export, or rename a deployment architecture.

Procedure

Step 1 Log in to the Huawei Cloud management console.

Step 2 In the upper left corner of the homepage, click ☰ to expand the service list and choose **Management & Governance** > **Optimization Advisor**.

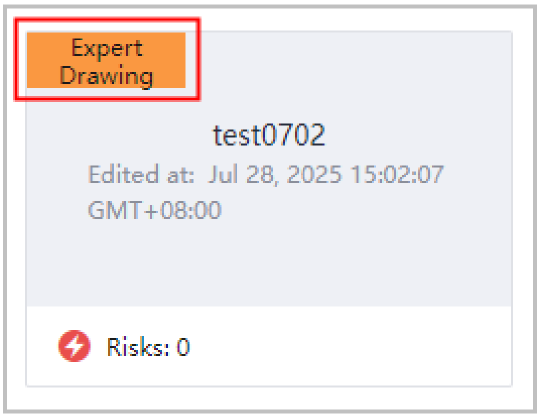
Step 3 In the navigation pane, choose **Architecture Design** and click the **Architecture Design** tab.

Step 4 In the **Card** view of **Deployment Architecture**, select the target architecture and hover the mouse over its center to view, rename, export, copy, or delete the architecture.

Step 5 Click **View Architecture** to go to its details page. Click **Architecture Drawings** on the top of the canvas to start drawing.

NOTE

Architectures labeled **Expert Drawing** in the upper left corner of the card are created by technical experts via the management tool and synced with the OA architecture design. You can only view these architectures. To edit and modify them, contact technical experts.



Expert Drawing

test0702

Edited at: Jul 28, 2025 15:02:07 GMT+08:00

Risks: 0

----End

2.1.3 Enabling Capacity Risk Monitoring

This section describes how to enable capacity risk monitoring.

Procedure

Step 1 Log in to the Huawei Cloud management console.

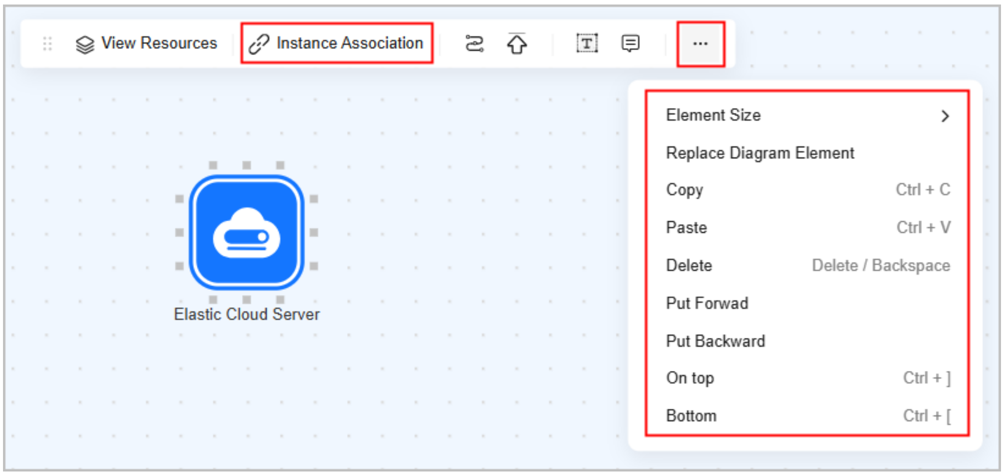
Step 2 In the upper left corner of the homepage, click ☰ to expand the service list and choose **Management & Governance** > **Optimization Advisor**.

Step 3 In the navigation pane, choose **Architecture Design** and click the **Architecture Design** tab.

Step 4 In the **Card** view of **Deployment Architecture**, select the target architecture and hover the mouse over its center and click **View Architecture** to go to its details page. Click **Architecture Drawings** on the top of the canvas to start drawing.

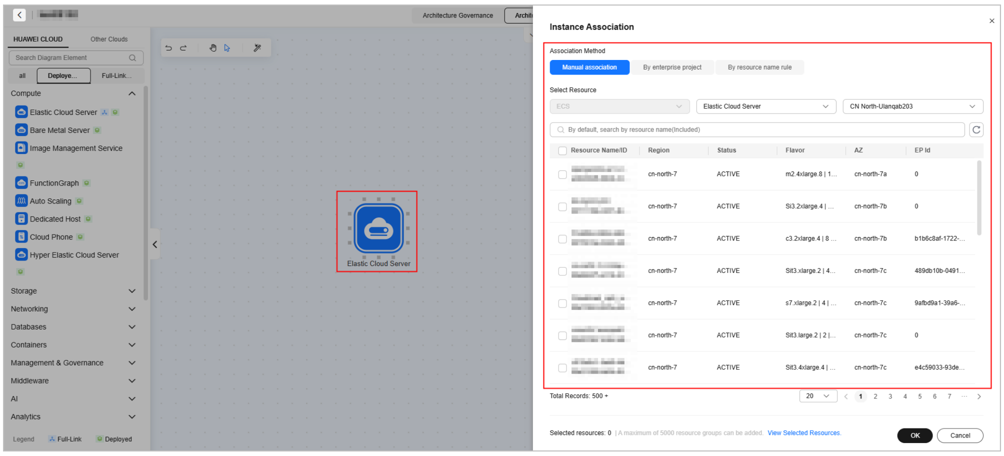
Step 5 On the left pane, choose **HUAWEI CLOUD** > **Deployed as Instances** in the drawing toolbar, and drag a cloud service diagram element (for example, **Elastic Cloud Server**) to the canvas.

Step 6 Click the cloud service diagram element. In the properties panel, you can modify its size, name, and remarks.



Step 7 Click **Instance Association** in the properties panel. In the displayed dialog box on the right, select an association method and resources.

Select the resources to be monitored and click **OK**. The capacity risk monitoring is enabled for these resources.



Instance Association

Association Method

Manual association | By enterprise project | By resource name rule

Select Resource

ECS | Elastic Cloud Server | CN North-Ulanqab203

By default, search by resource name(Included)

☐ Resource Name/ID	Region	Status	Flavor	AZ	EP Id
☐ [redacted]	cn-north-7	ACTIVE	m2.4xlarge.8 | 1...	cn-north-7a	0
☐ [redacted]	cn-north-7	ACTIVE	Si3.2xlarge.4 | ...	cn-north-7b	0
☐ [redacted]	cn-north-7	ACTIVE	c3.2xlarge.4 | 8 ...	cn-north-7b	b1b6c8af-1722-...
☐ [redacted]	cn-north-7	ACTIVE	Sit3.xlarge.2 | 4...	cn-north-7c	489db10b-0491...
☐ [redacted]	cn-north-7	ACTIVE	s7.xlarge.2 | 4 | ...	cn-north-7c	9afbd9a1-39a6-...
☐ [redacted]	cn-north-7	ACTIVE	Sit3.large.2 | 2 |...	cn-north-7c	0
☐ [redacted]	cn-north-7	ACTIVE	Sit3.4xlarge.4 | ...	cn-north-7c	e4c59033-93de...

Total Records: 500 +   20   < 1 2 3 4 5 6 7 ··· >

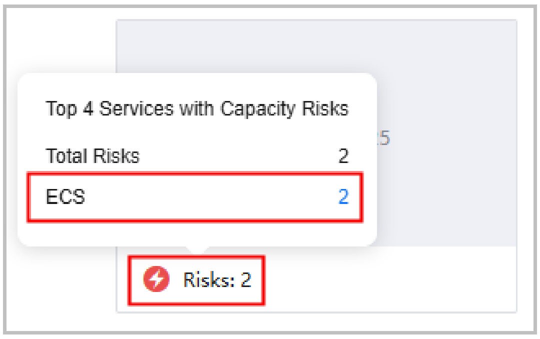
Selected resources: 0 | A maximum of 5000 resource groups can be added. View Selected Resources.

OK   Cancel

Step 8 Click **Start check** in **Resource Overview** on the left. In the **Configuring Capacity Monitoring Rules** dialog box on the right, select an analysis scenario, for example, **Routine risk analysis**. Click **Custom Risk Analysis**.

Configure monitoring rules. Set the monitoring interval, aggregation period, and triggering conditions. If a resource metric reaches the preset threshold, the resource is regarded as a risky resource.

Step 9 Click **Start analysis**. The system monitors the check result. If there are risks, the number of risks will be displayed below the deployment architecture card. Move the cursor to the number. The four cloud services with the most risks are displayed.

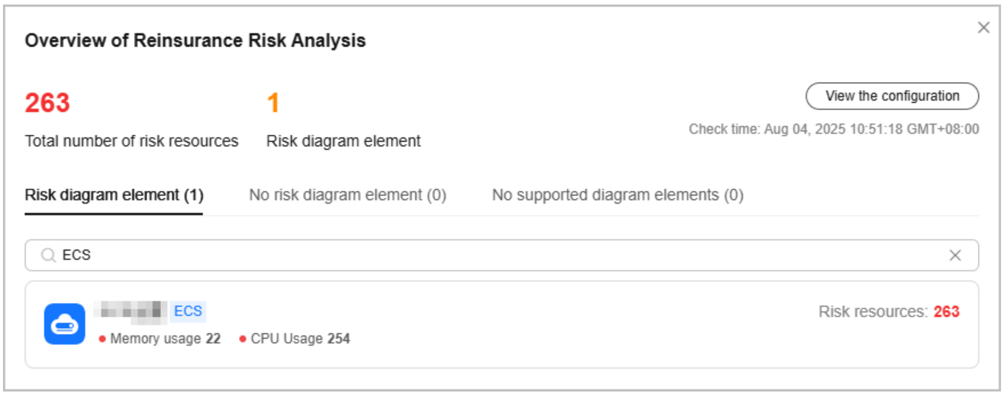


Top 4 Services with Capacity Risks

Total Risks	2
ECS	2

Risks: 2

Step 10 Click the number next to a cloud service to go to the risk identification result page.



Overview of Reinsurance Risk Analysis

263 Total number of risk resources

1 Risk diagram element

View the configuration

Check time: Aug 04, 2025 10:51:18 GMT+08:00

Risk diagram element (1) No risk diagram element (0) No supported diagram elements (0)

ECS

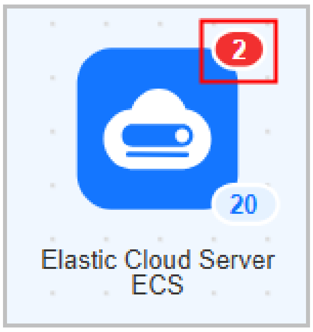
[redacted] ECS

● Memory usage 22 ● CPU Usage 254

Risk resources: 263

NOTE

- The architecture highlights cloud services with capacity risks using a red number in the top-right corner of their diagram elements.



----End

2.1.4 Drawing a Deployment Architecture

Procedure

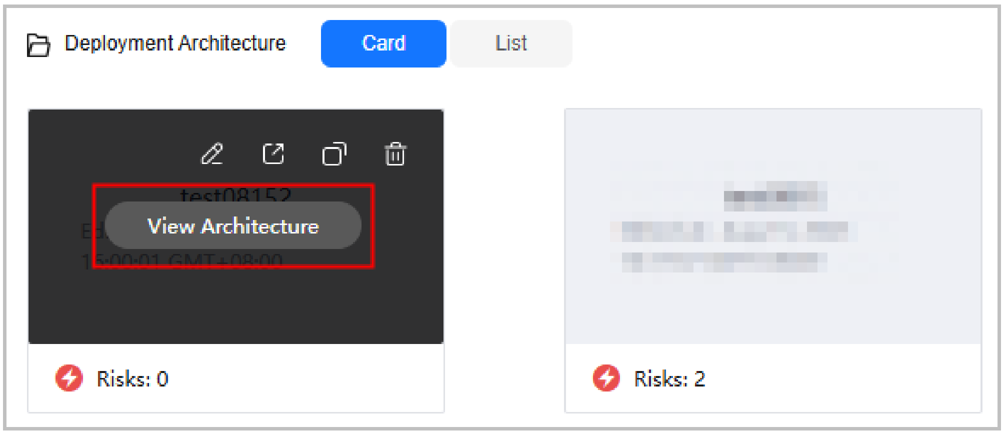
Step 1 Log in to the Huawei Cloud management console.

Step 2 In the upper left corner of the homepage, click ☰ to expand the service list and choose **Management & Governance** > **Optimization Advisor**.

Step 3 In the navigation pane, choose **Architecture Design** and click the **Architecture Design** tab.

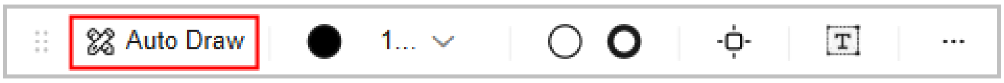
Step 4 Click **Create Deployment Architecture** in the upper left corner. On the displayed page, enter the architecture name, select the architecture type (no impact on drawing), enter a description about the architecture, and select the deployment status (no impact on drawing).

Step 5 In the **Card** view of **Deployment Architecture**, select the created architecture and hover the mouse over its center and click **View Architecture** to go to its details page. Click **Architecture Drawings** on the top of the canvas to start drawing.



Step 6 On the left pane, view the basic diagram elements and cloud service diagram elements required for drawing.

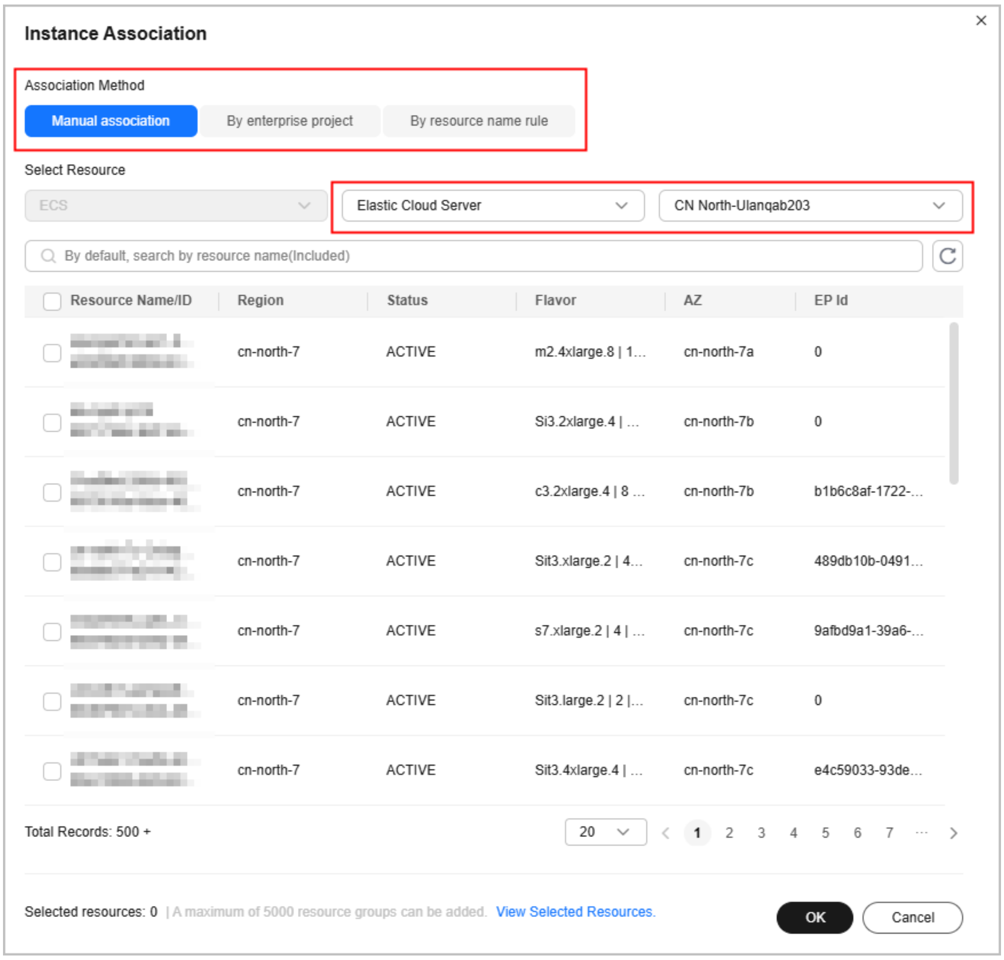
Step 7 On the toolbar, click **Auto Draw**. Drag the **Subnet** diagram element to the canvas, click it, and then click **Auto Draw** in the properties panel.



Step 8 In the **Auto Draw** dialog box, set the region, VPC, and subnet information, and click **Start analysis**. The system will identify resources within the subnet and organize them according to the logical structure. If VPC flow logs are enabled, the relationships between resources can be drawn.

Step 9 In the drawing toolbar on the left, click **Full-Link Cloud Services**. The cloud services provided here support one-click full-link drawing.

- Drag a cloud service diagram element (for example, Elastic Cloud Server) to the canvas.
- **Associating resources**: Click the ECS diagram element. In the properties panel, click **Instance Association**. In the displayed dialog box, set the association method, select a region and resource type to search for ECS resources in the region, select the desired resources, and click **OK**.



Instance Association

Association Method

Manual association | By enterprise project | By resource name rule

Select Resource

ECS | Elastic Cloud Server | CN North-Ulanqab203

By default, search by resource name(Included)

□ Resource Name/ID	Region	Status	Flavor	AZ	EP Id
□ [redacted]	cn-north-7	ACTIVE	m2.4xlarge.8 | 1...	cn-north-7a	0
□ [redacted]	cn-north-7	ACTIVE	Si3.2xlarge.4 | ...	cn-north-7b	0
□ [redacted]	cn-north-7	ACTIVE	c3.2xlarge.4 | 8 ...	cn-north-7b	b1b6c8af-1722-...
□ [redacted]	cn-north-7	ACTIVE	Sit3.xlarge.2 | 4...	cn-north-7c	489db10b-0491...
□ [redacted]	cn-north-7	ACTIVE	s7.xlarge.2 | 4 | ...	cn-north-7c	9afbd9a1-39a6-...
□ [redacted]	cn-north-7	ACTIVE	Sit3.large.2 | 2 |...	cn-north-7c	0
□ [redacted]	cn-north-7	ACTIVE	Sit3.4xlarge.4 | ...	cn-north-7c	e4c59033-93de...

Total Records: 500 +

20 | < 1 2 3 4 5 6 7 ··· >

Selected resources: 0 | A maximum of 5000 resource groups can be added. View Selected Resources.

OK | Cancel

- **Full-link drawing**: Click the ECS diagram element and click in the properties panel to draw a full-link diagram.

Step 10 In the toolbar on the left, click the **Deployed as Instances** tab. The cloud services displayed on this page support instance association.

- Drag a cloud service diagram element (for example, Elastic Cloud Server) to the canvas.
- **Associating resources**: Click the ECS diagram element. In the properties panel, click **Instance Association**. In the displayed dialog box, set the association method, select a region and resource type to search for ECS resources in the region, select the desired resources, and click **OK**.

----End

2.1.5 Exporting the Resource List

Procedure

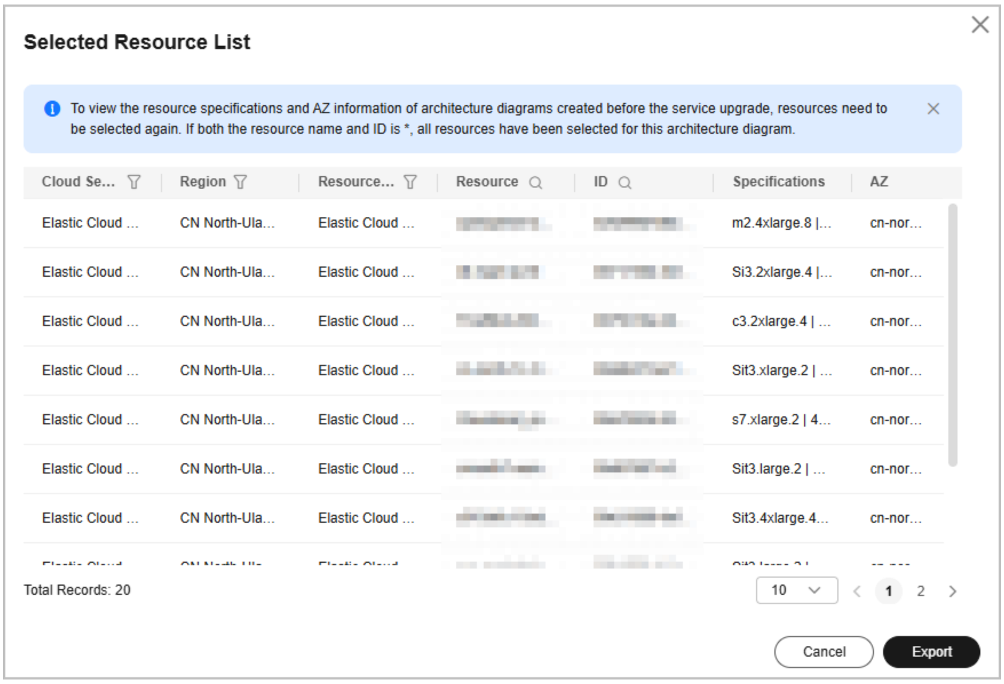
Step 1 Log in to the Huawei Cloud management console.

Step 2 In the upper left corner of the homepage, click ☰ to expand the service list and choose **Management & Governance** > **Optimization Advisor**.

Step 3 In the navigation pane, choose **Architecture Design** and click the **Architecture Design** tab.

Step 4 In the **Card** view of **Deployment Architecture**, select the target architecture and hover the mouse over its center and click **View Architecture** to go to its details page.

Step 5 In the upper right corner of the drawing page, click ··· to view all resources associated with the architecture and their details. Click **Export** to download the architecture list.



Selected Resource List

To view the resource specifications and AZ information of architecture diagrams created before the service upgrade, resources need to be selected again. If both the resource name and ID is *, all resources have been selected for this architecture diagram.

Cloud Se...	Region	Resource...	Resource	ID	Specifications	AZ
Elastic Cloud ...	CN North-Ula...	Elastic Cloud ...	[redacted]	[redacted]	m2.4xlarge.8 |...	cn-nor...
Elastic Cloud ...	CN North-Ula...	Elastic Cloud ...	[redacted]	[redacted]	Si3.2xlarge.4 |...	cn-nor...
Elastic Cloud ...	CN North-Ula...	Elastic Cloud ...	[redacted]	[redacted]	c3.2xlarge.4 | ...	cn-nor...
Elastic Cloud ...	CN North-Ula...	Elastic Cloud ...	[redacted]	[redacted]	Sit3.xlarge.2 | ...	cn-nor...
Elastic Cloud ...	CN North-Ula...	Elastic Cloud ...	[redacted]	[redacted]	s7.xlarge.2 | 4...	cn-nor...
Elastic Cloud ...	CN North-Ula...	Elastic Cloud ...	[redacted]	[redacted]	Sit3.large.2 | ...	cn-nor...
Elastic Cloud ...	CN North-Ula...	Elastic Cloud ...	[redacted]	[redacted]	Sit3.4xlarge.4...	cn-nor...
Elastic Cloud	CN North-Ula	Elastic Cloud	[redacted]	[redacted]	Sit3.large.2 |	cn-nor

Total Records: 20

----End

2.2 Service Architectures

2.2.1 Creating a Service Architecture

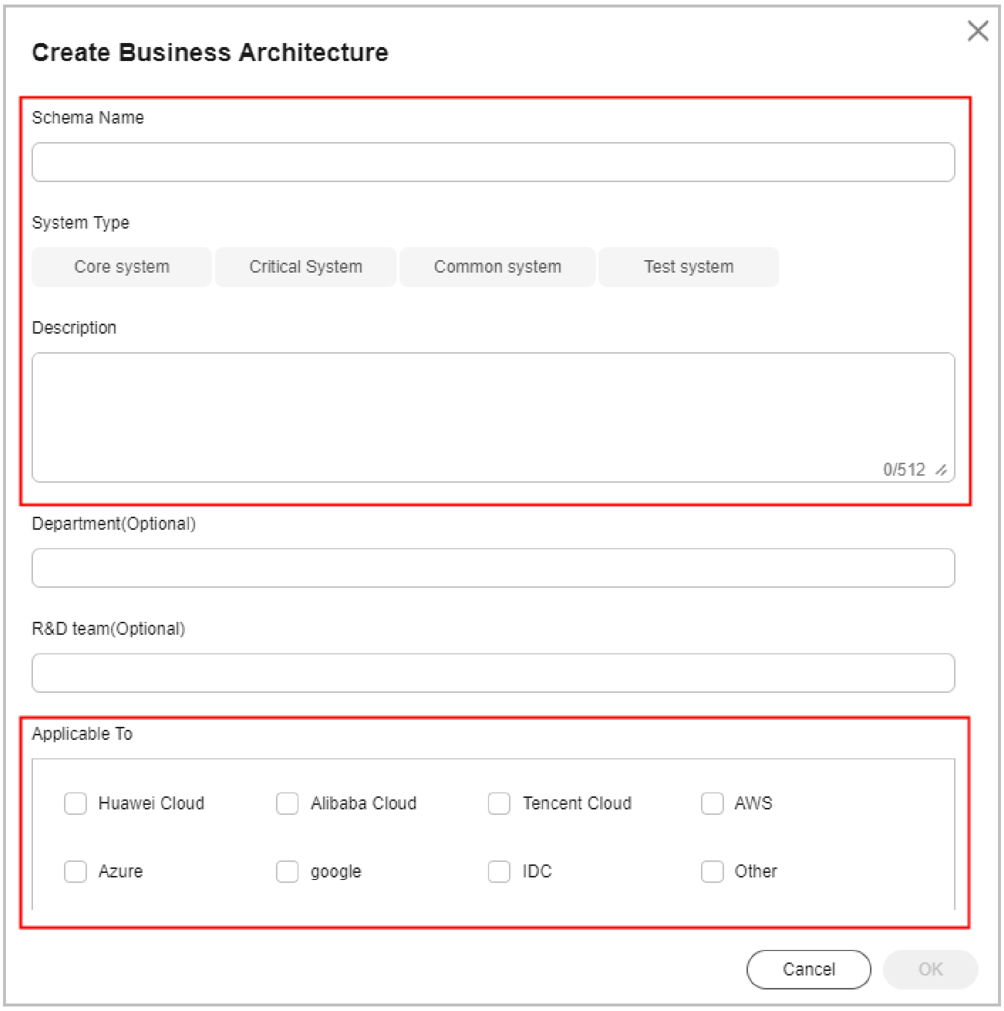
Procedure

Step 1 Log in to the Huawei Cloud management console.

Step 2 In the upper left corner of the homepage, click ☰ to expand the service list and choose **Management & Governance** > **Optimization Advisor**.

Step 3 In the navigation pane, choose **Architecture Design** and click the **Architecture Design** tab.

Step 4 Click **Create Business Architecture** in the upper left corner. On the displayed page, enter the architecture name, select the architecture type (no impact on drawing), enter a description about the architecture, and select the deployment status (no impact on drawing).



Create Business Architecture

Schema Name

System Type

Core system | Critical System | Common system | Test system

Description

0/512

Department(Optional)

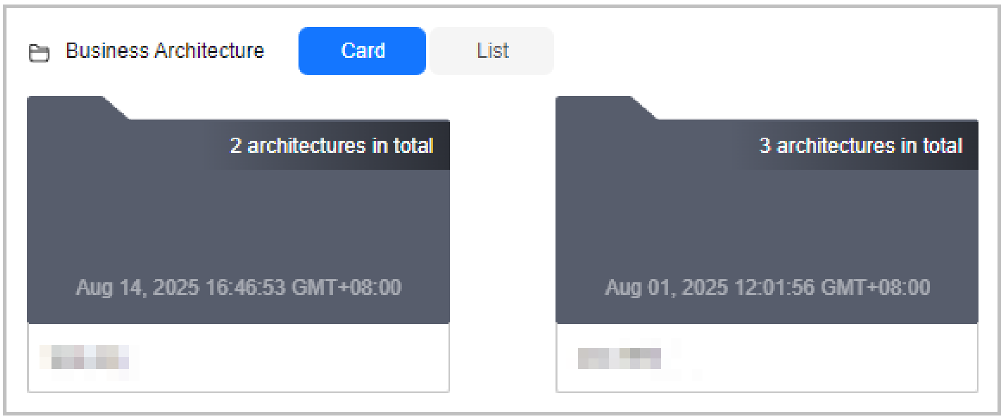
R&D team(Optional)

Applicable To

☐ Huawei Cloud ☐ Alibaba Cloud ☐ Tencent Cloud ☐ AWS

☐ Azure ☐ google ☐ IDC ☐ Other

Step 5 View that the created business architecture is displayed in the **Card** view by default.



2 architectures in total

Aug 14, 2025 16:46:53 GMT+08:00

[redacted]

3 architectures in total

Aug 01, 2025 12:01:56 GMT+08:00

[redacted]

----End

2.2.2 Drawing a Business Architecture

You can view, edit, copy, delete, export, or rename a business architecture.

Procedure

Step 1 Log in to the Huawei Cloud management console.

Step 2 In the upper left corner of the homepage, click ☰ to expand the service list and choose **Management & Governance** > **Optimization Advisor**.

Step 3 In the navigation pane, choose **Architecture Design** and click the **Architecture Design** tab.

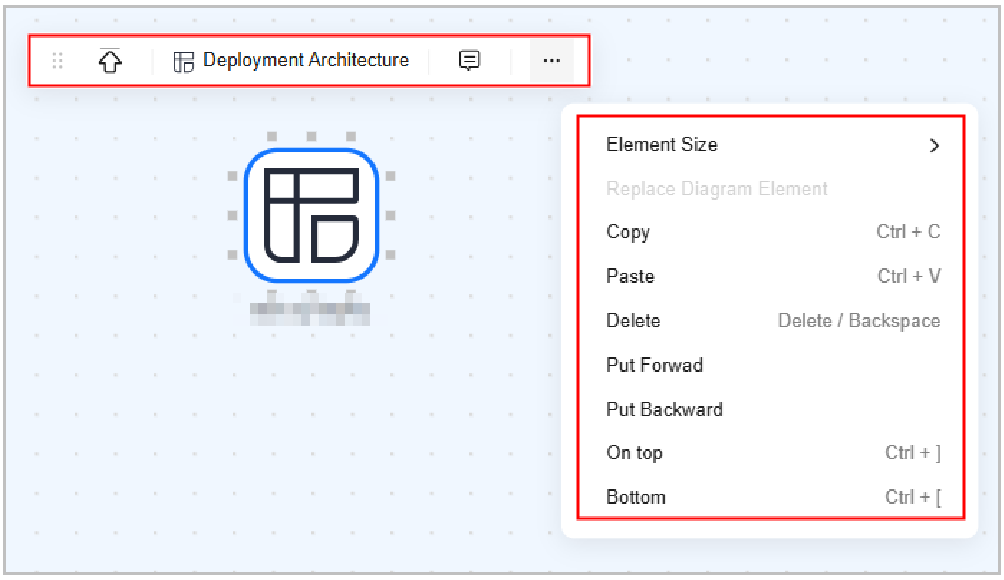
Step 4 Click **Create Business Architecture** in the upper left corner. On the displayed page, enter the architecture name, select the architecture type (no impact on drawing), enter a description about the architecture, and select the deployment status (no impact on drawing).

Step 5 The created business architecture is displayed in the **Card** view by default. Locate the target architecture and hover the mouse over its center to view, rename, export, copy, or delete the architecture.

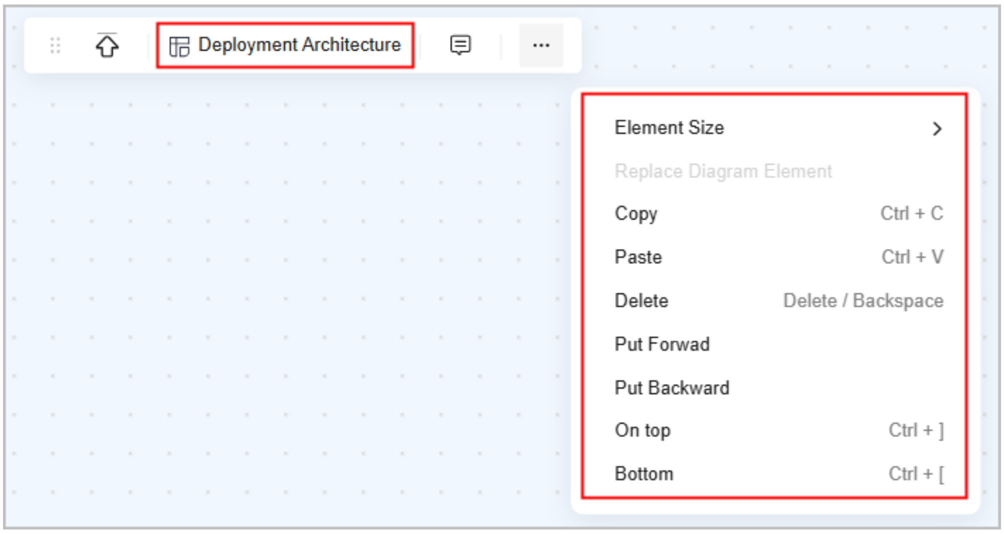
Step 6 Click **View Architecture**. On the displayed page, click **Browse** above the canvas to start editing.

Step 7 On the left, basic diagram elements and cloud service diagram elements required for drawing are provided. Drag a basic diagram element from the left element drawer to draw an architecture.

Click **Basic Diagram Elements**. In the properties panel, you can modify its size, name, and remarks.



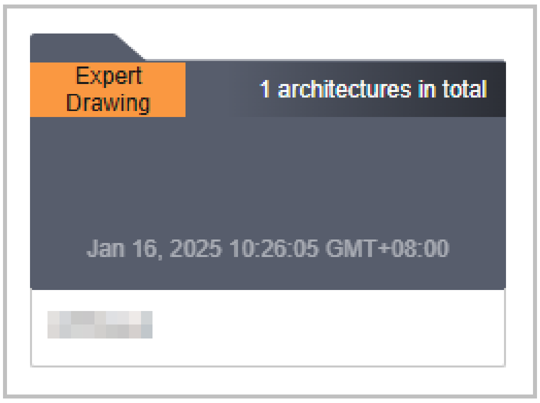
Step 8 In the left navigation pane, choose **Deployment Architecture** to display all created deployment architectures. You can directly drag one to the canvas for drawing. Click the **Deployment Architecture** diagram element in the canvas. In the properties panel, you can modify its size and remarks.



Step 9 Click **Deployment Architecture**. In the drawer displayed on the right, the deployment architecture name, cloud service, resource type, region, and quantity are displayed.

NOTE

Architectures labeled **Expert Drawing** in the upper left corner of the card are created by technical experts via the management tool and synced with the OA architecture design. You can only view these architectures. To edit and modify them, contact technical experts.



----End

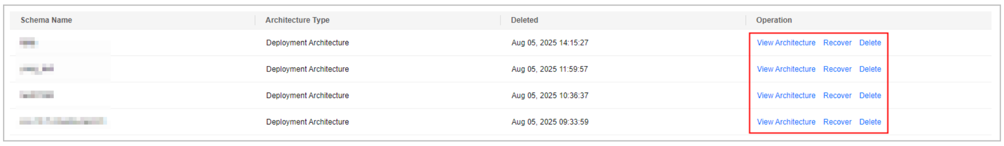
2.3 Recycle bin

Step 1 Log in to the Huawei Cloud management console.

Step 2 In the upper left corner of the homepage, click ☰ to expand the service list and choose **Management & Governance** > **Optimization Advisor**.

Step 3 In the navigation pane, choose **Architecture Design** > **Recycle Bin**.

Step 4 You can view, restore, and delete deleted architecture diagrams in the list.



Schema Name	Architecture Type	Deleted	Operation
[redacted]	Deployment Architecture	Aug 05, 2025 14:15:27	View Architecture Recover Delete
[redacted]	Deployment Architecture	Aug 05, 2025 11:59:57	View Architecture Recover Delete
[redacted]	Deployment Architecture	Aug 05, 2025 10:36:37	View Architecture Recover Delete
[redacted]	Deployment Architecture	Aug 05, 2025 09:33:59	View Architecture Recover Delete

NOTE

After being deleted, service and deployment architectures can be retained in the recycle bin for a maximum of 6 months. After the retention period expires, the architectures will be permanently deleted.

----End

3 Capacity Optimization

During O&M, you need to identify heavily loaded risky instances in advance and take measures to ensure service continuity. Capacity optimization allows you to quickly identify risky instances based on the security thresholds you set and provides optimization suggestions.

Scenarios

You can use this function to predict resource load and identify heavily loaded resources.

Constraints

- To use capacity optimization, you need to enable **Enterprise Support Plan**.
- Capacity optimization consists of daily risk prediction (custom risk analysis and intelligent risk analysis) and KEA period risk prediction. Intelligent risk analysis and KEA period risk prediction are only available to whitelisted users. You can **submit a service ticket** to apply for whitelist inclusion.

3.1 Daily Risk Prediction

Procedure

Step 1 Log in to the Huawei Cloud management console.

Step 2 In the upper left corner of the homepage, click ☰ to expand the service list and choose **Management & Governance** > **Optimization Advisor**.

Step 3 In the navigation pane, choose **Capacity Optimization** > **Daily Risk Prediction**.

Step 4 Configure custom risk analysis or intelligent risk analysis as needed. By default, the **Custom Risk Analysis** page is displayed.

NOTE

Currently, intelligent risk prediction is only available to whitelisted users.

- **Custom risk analysis**: a peak prediction method that identifies risky instances based on the input predicted peak value.

- Predicted peak value = Historical peak value in the reference period x (1 + Pressure coefficient)
- Risky instances: If either the historical peak capacity value or predicted peak value of an instance reaches the security threshold, the instance is considered risky and included in the risk report.

Table 1 lists the parameters for custom risk analysis.

Table 3-1 Parameters for custom risk analysis

Parameter	Description
Monitoring Date	Reference load data. The system identifies the peak capacity value within the monitoring period to predict peak capacity.
Pressure Coefficient	How many times service traffic increases. Predicted peak value = Peak capacity value within the effective period x (1 + Pressure coefficient)
In Aggregation Period	The maximum, minimum, and average values from raw data are calculated and collected over a period, which is referred to as an aggregation period. The system supports three aggregation periods: 1 hour, 4 hours, and 24 hours.
Trigger Condition	Number of consecutive times a specified condition must be met before the resource is considered as a risky instance.
Monitoring Scope	Risky resource scope. You can select **Resource Groups** or **Resource**.
Metric Name	Name of the metric to be analyzed.
Monitoring Policy	1. **Metric value type** can be: a. **Average** is the value calculated by averaging raw data over an aggregation period. b. **Maximum value** is the maximum value of raw data over an aggregation period. c. **Minimum value** is the minimum value of raw data over an aggregation period. 2. **Safety Threshold** indicates the threshold set for an analysis metric. 3. **Operator** compares the metric value with the threshold. Supported operators: >, >=, <, and <=

- **Intelligent risk analysis**: A trend prediction method that predicts the future capacity trend based on input value and algorithms.
  - **Predicted trend**: The capacity trend of the next seven days is predicted based on the capacity trend in the reference period (within the last one month) using the prediction algorithms.

– **Risky instance**: If the capacity hits the safety limit during either the reference or prediction period, the instance is considered risky and included in the risk report.

Table 2 lists the parameters for intelligent risk analysis.

Table 3-2 Parameters for intelligent risk analysis

Parameter	Description
Reference Time Period	The prediction is based on the capacity trend in the reference time segment. By default, the end date matches the current time and cannot be changed.
Forecast Period	The intelligent prediction period in the next seven days cannot be changed.
In Aggregation Period	The maximum, minimum, and average values from raw data are calculated and collected over a period, which is referred to as an aggregation period. The system supports three aggregation periods: 1 hour, 4 hours, and 24 hours.
Trigger Condition	Number of consecutive times a specified condition must be met before the resource is considered as a risky instance.
Monitoring Scope	Risky resource scope. You can select **Resource Groups** or **Resource**.
Metric Name	Name of the metric to be analyzed.
Monitoring Policy	1. **Metric value type** can be: a. **Average** is the value calculated by averaging raw data over an aggregation period. b. **Maximum value** is the maximum value of raw data over an aggregation period. c. **Minimum value** is the minimum value of raw data over an aggregation period. 2. **Safety Threshold** indicates the threshold set for an analysis metric. 3. **Operator** compares the metric value with the threshold. Supported operators: >, >=, <, and <=

Step 5 Click **Risk Analysis** to configure risk analysis.

1. **Set parameters in batches.**

   You can set the monitoring date, aggregation period, trigger condition, and pressure coefficient to set risk analysis parameters.

   NOTE

   An instance appears in the analysis result list only after the threshold is reached for *n* consecutive times.

2. **Configure capacity thresholds.**

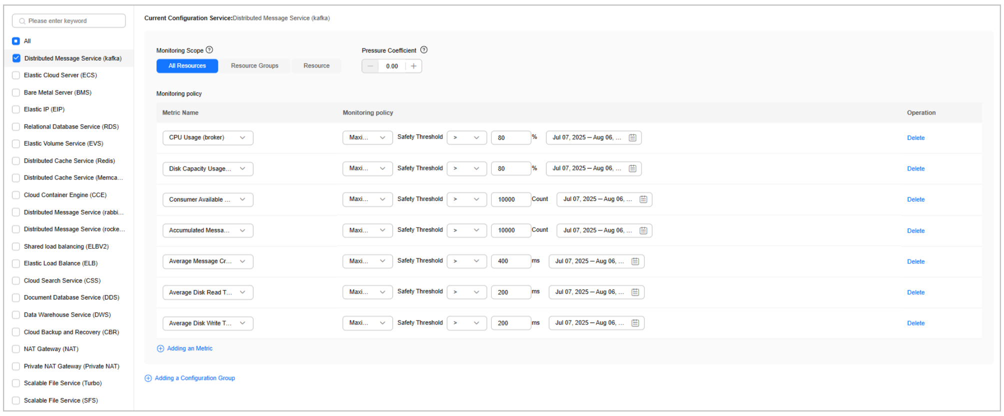
   a. **Selecting a cloud service**: After you select the target cloud service, the system provides metric parameters by default. You can click **Adding a Configuration Group** to add, delete, or change metrics as needed.

   b. **Configuring the monitoring scope**: You can set different pressure coefficients and monitoring scopes for the selected cloud service. The monitoring scope can be **All Resources**, **Resource Groups**, or **Resource**.

      - **All Resources**: All resources of the cloud service in your account are selected by default.

      - **Resource Groups**: You can select resource groups created for the service. If no resource group is available, you are advised to create one by referring to **Creating a Resource Group**.

      - **Resource**: You can query all resource instances of the service and select the desired ones.


Please enter keyword
All
Distributed Message Service (kafka)
Elastic Cloud Server (ECS)
Bare Metal Server (BMS)
Elastic IP (EIP)
Relational Database Service (RDS)
Elastic Volume Service (EVS)
Distributed Cache Service (Redis)
Distributed Cache Service (Memca...
Cloud Container Engine (CCE)
Distributed Message Service (rabbi...
Distributed Message Service (rocke...
Shared load balancing (ELBV2)
Elastic Load Balance (ELB)
Cloud Search Service (CSS)
Document Database Service (DDS)
Data Warehouse Service (DWS)
Cloud Backup and Recovery (CBR)
NAT Gateway (NAT)
Private NAT Gateway (Private NAT)
Scalable File Service (Turbo)
Scalable File Service (SFS)
Resource Groups
Resource
Adding an Metric
Adding a Configuration Group

Current Configuration Service: Distributed Message Service (kafka)

Monitoring Scope: All Resources

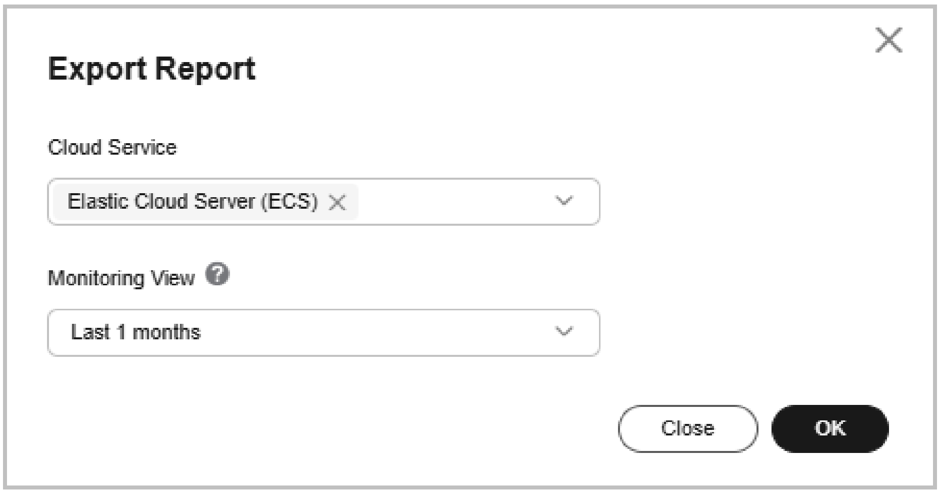
Pressure Coefficient: 0.00

Monitoring policy

Metric Name	Monitoring policy						Operation
CPU Usage (broker)	Maxi...	Safety Threshold	>	80	%	Jul 07, 2025 – Aug 06, ...	Delete
Disk Capacity Usage...	Maxi...	Safety Threshold	>	80	%	Jul 07, 2025 – Aug 06, ...	Delete
Consumer Available ...	Maxi...	Safety Threshold	>	10000	Count	Jul 07, 2025 – Aug 06, ...	Delete
Accumulated Messa...	Maxi...	Safety Threshold	>	10000	Count	Jul 07, 2025 – Aug 06, ...	Delete
Average Message Cr...	Maxi...	Safety Threshold	>	400	ms	Jul 07, 2025 – Aug 06, ...	Delete
Average Disk Read T...	Maxi...	Safety Threshold	>	200	ms	Jul 07, 2025 – Aug 06, ...	Delete
Average Disk Write T...	Maxi...	Safety Threshold	>	200	ms	Jul 07, 2025 – Aug 06, ...	Delete

Step 6 Click **Save and Analyze**. The system starts the capacity risk check process. After the check is complete, the check result is automatically updated on the homepage. You can click **Save** to store your settings. This allows you to revisit the risk analysis page later for quick capacity checks.

Step 7 Return to the **Custom Risk Analysis** page to view the check results. Click **Export** to download the check results.



Export Report

Cloud Service: Elastic Cloud Server (ECS)

Monitoring View: Last 1 months

----End

3.2 KEA Period Risk Prediction

Scenarios

KEA period risk prediction is available only to whitelisted users.

Procedure

Step 1 Log in to the Huawei Cloud management console.

Step 2 In the upper left corner of the homepage, click ☰ to expand the service list and choose **Management & Governance** > **Optimization Advisor**.

Step 3 In the navigation pane, choose **Capacity Optimization** > **KEA Period Risk Prediction**.

Step 4 Click **Risk Analysis** to configure risk analysis.

1. **Set parameters in batches.**

   You can set the activity time segment to set risk prediction parameters.

   > NOTE
   >
   > You are advised to predict the peak value within seven days. The prediction accuracy drops over longer periods.

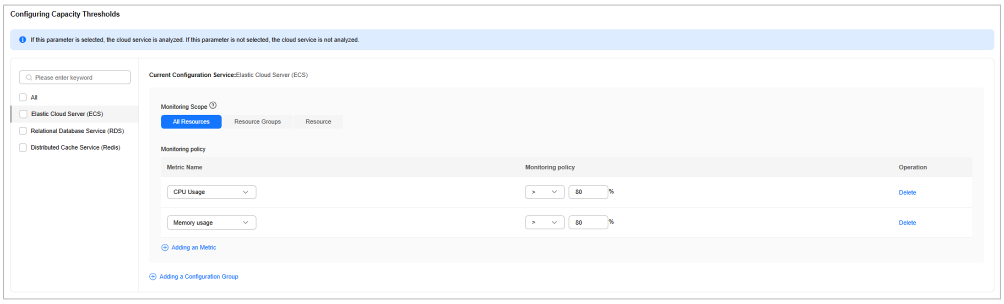
2. **Configure capacity thresholds.**

   a. **Selecting cloud services**: After you select the target cloud service, the system provides monitoring metric parameters by default.

   b. **Configuring the monitoring scope**: You can set different monitoring scopes for the selected cloud service. The monitoring scope can be **All Resources**, **Resource Groups**, or **Resource**.

   - **All Resources**: All resources of the cloud service in your account are selected by default.
   - **Resource Groups**: You can select resource groups created for the service. If no resource group is available, you are advised to create one by referring to **Creating a Resource Group**.
   - **Resource**: You can query all resource instances of the service and select the desired ones.

   c. **Configuring monitoring policies**: You can click **Adding a Configuration Group** to add, delete, or change metrics as needed.



Configuring Capacity Thresholds

If this parameter is selected, the cloud service is analyzed. If this parameter is not selected, the cloud service is not analyzed.

Please enter keyword

□ All
□ Elastic Cloud Server (ECS)
□ Relational Database Service (RDS)
□ Distributed Cache Service (Redis)

Current Configuration Service:Elastic Cloud Server (ECS)

Monitoring Scope

Monitoring policy

Metric Name	Monitoring policy	Operation
CPU Usage	> 80 %	Delete
Memory usage	> 80 %	Delete

Step 5 Click **Save and Analyze**. The system starts KEA period risk prediction. After the check is complete, the check result is automatically updated on the homepage. You can click **Save** to store your settings. This allows you to re-access the risk analysis page later for quick KEA period risk prediction.

Step 6 Return to the **KEA Period Risk Prediction** page to view the check results. Click **Export** to download the check results.

----End

3.3 Viewing Monitoring Data

Procedure

Step 1 Log in to the Huawei Cloud management console.

Step 2 In the upper left corner of the homepage, click ☰ to expand the service list and choose **Management & Governance** > **Optimization Advisor**.

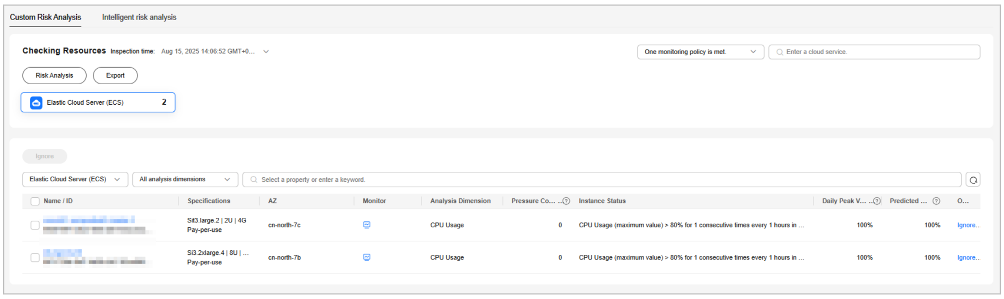
Step 3 In the navigation pane, choose **Capacity Optimization** > **Daily Risk Prediction** or **Key Period Risk Prediction**.

Step 4 In the upper right corner of the page, select a resource condition to search for resources.

NOTE

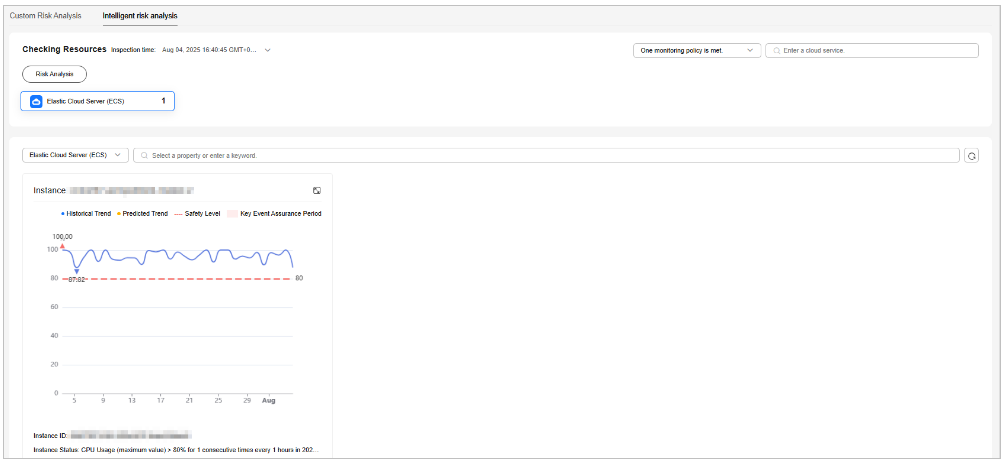
Each prediction mode generates unique risk reports with distinct styles for displaying the risk list.

- **Custom risk analysis reports**: The risky instance list is displayed, as shown in the following figure.


Custom Risk Analysis
Intelligent risk analysis
Checking Resources
Inspection time: Aug 15, 2025 14:06:52 GMT+0...
One monitoring policy is met.
Enter a cloud service.
Risk Analysis
Export
Elastic Cloud Server (ECS) 2
Ignore
Elastic Cloud Server (ECS)
All analysis dimensions
Select a property or enter a keyword.

Name / ID	Specifications	AZ	Monitor	Analysis Dimension	Pressure Co...	Instance Status	Daily Peak V...	Predicted ...	O...
[redacted]	Sit3.large.2 | 2U | 4G Pay-per-use	cn-north-7c		CPU Usage	0	CPU Usage (maximum value) > 80% for 1 consecutive times every 1 hours in ...	100%	100%	Ignore..
[redacted]	Si3.2xlarge.4 | 8U | ... Pay-per-use	cn-north-7b		CPU Usage	0	CPU Usage (maximum value) > 80% for 1 consecutive times every 1 hours in ...	100%	100%	Ignore..

- **Intelligent risk analysis reports**: The risky instance list is displayed, as shown in the following figure.



Custom Risk Analysis | Intelligent risk analysis

Checking Resources Inspection time: Aug 04, 2025 16:40:45 GMT+0...

One monitoring policy is met. | Enter a cloud service.

Risk Analysis

Elastic Cloud Server (ECS) 1

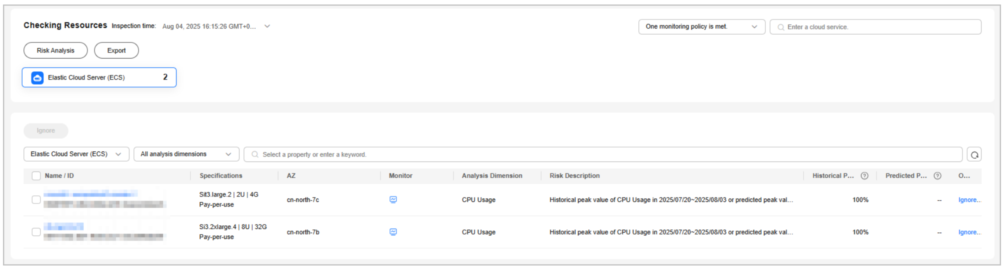
Elastic Cloud Server (ECS) | Select a property or enter a keyword.

Instance [redacted]

Instance ID: [redacted]

Instance Status: CPU Usage (maximum value) > 80% for 1 consecutive times every 1 hours in 202...

- **KEA period risk prediction**: The risky instance list is displayed.



Checking Resources Inspection time: Aug 04, 2025 16:15:26 GMT+0...

One monitoring policy is met. | Enter a cloud service.

Risk Analysis | Export

Elastic Cloud Server (ECS) 2

Ignore

Elastic Cloud Server (ECS) | All analysis dimensions | Select a property or enter a keyword.

Name / ID	Specifications	AZ	Monitor	Analysis Dimension	Risk Description	Historical P...	Predicted P...	O...
[redacted]	Sit3.large.2 | 2U | 4G Pay-per-use	cn-north-7c		CPU Usage	Historical peak value of CPU Usage in 2025/07/20~2025/08/03 or predicted peak val...	100%	--	Ignore...
[redacted]	Si3.2xlarge.4 | 8U | 32G Pay-per-use	cn-north-7b		CPU Usage	Historical peak value of CPU Usage in 2025/07/20~2025/08/03 or predicted peak val...	100%	--	Ignore...

Step 5 Click **Export** in the upper left corner to export the capacity risk report.

----End

3.4 Capacity Reports

Procedure

Step 1 Log in to the Huawei Cloud management console.

Step 2 In the upper left corner of the homepage, click ☰ to expand the service list and choose **Management & Governance** > **Optimization Advisor**.

Step 3 Perform a **daily risk prediction** or **KEA period risk prediction**.

Step 4 In the navigation pane, choose **Capacity Optimization** > **Capacity Reports**.

Step 5 Locate a report and click **Download** in the **Operation** column to download the capacity report. You can also export reports on the **Daily Risk Prediction** and **KEA Period Prediction** pages.

Step 6 Click **Delete** on the right of the report to delete it. You can also select all or desired reports and click **Batch Delete** above the list to delete them.

NOTE

Deleted reports cannot be recovered.

----End

4 Resource Groups

4.1 Creating a Resource Group

Procedure

Step 1 Log in to the Huawei Cloud management console.

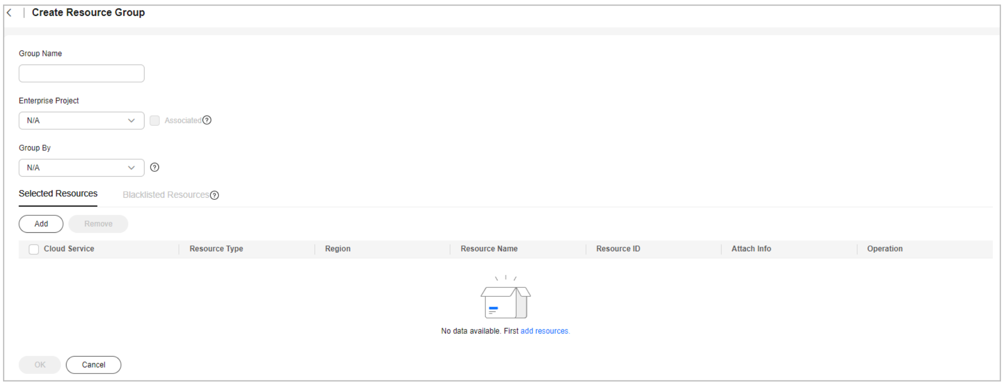
Step 2 In the upper left corner of the homepage, click ☰ to expand the service list and choose **Management & Governance** > **Optimization Advisor**.

Step 3 In the navigation pane, choose **Resource Groups**.

Step 4 Click **Create** in the upper left corner. On the **Create Resource Group** page, set the group name, enterprise project, and grouping rules.

Step 5 Click **Add**. In the displayed dialog box, select a cloud service, resource type, and region to search for resources, select desired instances, and click **OK**.

Step 6 Click **OK**. The resource group is created.



Create Resource Group

Group Name

Enterprise Project: N/A □ Associated

Group By: N/A

□ Cloud Service	Resource Type	Region	Resource Name	Resource ID	Attach Info	Operation

No data available. First add resources.

----End

4.2 Managing Resource Groups

Procedure

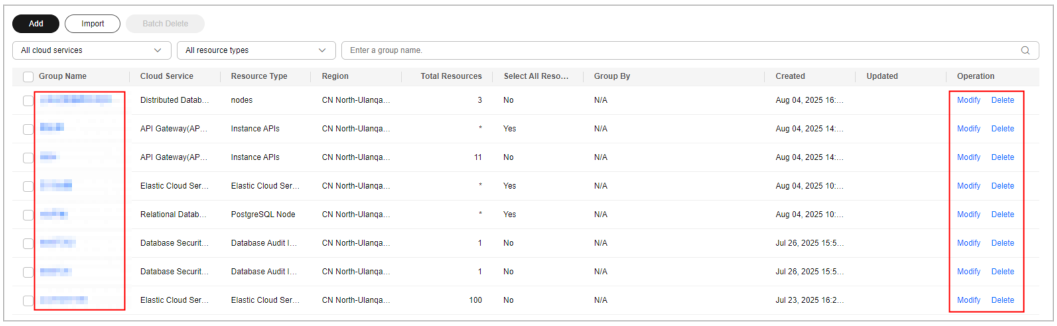
Step 1 Log in to the Huawei Cloud management console.

Step 2 In the upper left corner of the homepage, click ☰ to expand the service list and choose **Management & Governance** > **Optimization Advisor**.

Step 3 In the navigation pane, choose **Resource Groups**.

Step 4 Query and manage the created resource groups.

1. Click the name of a resource group to go to the **Resource Details** page. The asterisk (*) indicates all resources.
2. Locate the target resource group and click **Modify** in the **Operation** column to modify all information about the resource group.
3. Click **Delete** in the **Operation** column to delete the resource group.
4. Select one or more resource groups and click **Batch Delete** above the list to delete them.



□	Group Name	Cloud Service	Resource Type	Region	Total Resources	Select All Reso...	Group By	Created	Updated	Operation
□	[redacted]	Distributed Datab...	nodes	CN North-Ulanqa...	3	No	N/A	Aug 04, 2025 16:...		Modify Delete
□	[redacted]	API Gateway(AP...	Instance APIs	CN North-Ulanqa...	*	Yes	N/A	Aug 04, 2025 14:...		Modify Delete
□	[redacted]	API Gateway(AP...	Instance APIs	CN North-Ulanqa...	11	No	N/A	Aug 04, 2025 14:...		Modify Delete
□	[redacted]	Elastic Cloud Ser...	Elastic Cloud Ser...	CN North-Ulanqa...	*	Yes	N/A	Aug 04, 2025 10:...		Modify Delete
□	[redacted]	Relational Datab...	PostgreSQL Node	CN North-Ulanqa...	*	Yes	N/A	Aug 04, 2025 10:...		Modify Delete
□	[redacted]	Database Securit...	Database Audit I...	CN North-Ulanqa...	1	No	N/A	Jul 26, 2025 15:5...		Modify Delete
□	[redacted]	Database Securit...	Database Audit I...	CN North-Ulanqa...	1	No	N/A	Jul 26, 2025 15:5...		Modify Delete
□	[redacted]	Elastic Cloud Ser...	Elastic Cloud Ser...	CN North-Ulanqa...	100	No	N/A	Jul 23, 2025 16:2...		Modify Delete

----End

5 Permissions

5.1 Creating a User and Granting OA Permissions

You can use **Identity and Access Management (IAM)** for fine-grained permissions management of your OA. With IAM, you can:

- Create IAM users for personnel based on your enterprise's organizational structure. Each IAM user has their own identity credentials for accessing OA resources.
- Grant only the permissions required for users to perform a specific task.

If your Huawei Cloud account does not require individual IAM users, you can skip this section.

This section describes the procedure for granting permissions. **Figure 1** shows the process flow.

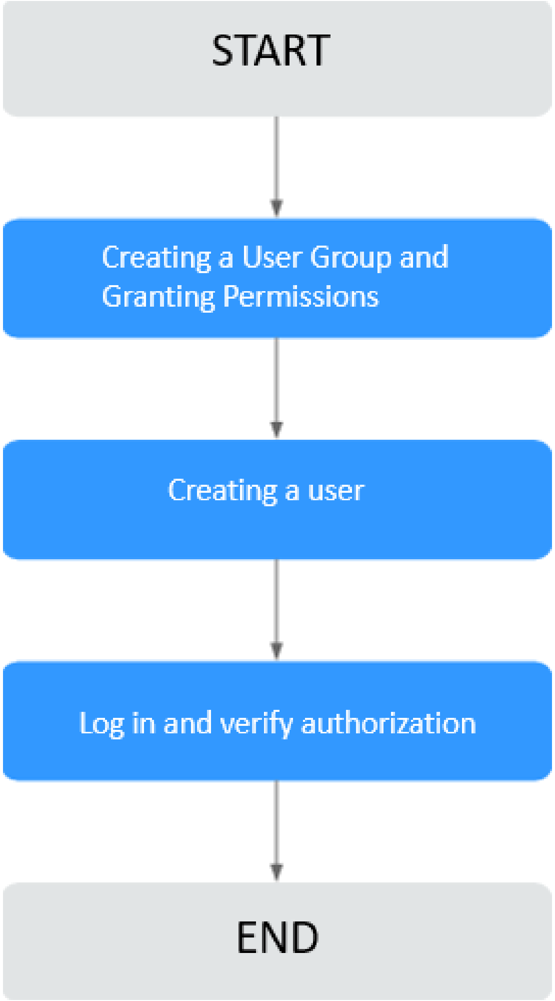
Prerequisites

Before granting permissions to user groups, learn about system-defined permissions for OA and choose policies based on your needs.

For details about supported system-defined policies and their differences, see **Permissions Management**. To grant permissions for other services, learn about all **system-defined permissions** supported by IAM.

Process Flow

Figure 5-1 Process for granting OA permissions


START
Creating a User Group and Granting Permissions
Creating a user
Log in and verify authorization
END

1. Create a user group on the IAM console, and assign the **OA FullAccessPolicy**, **OA AdvancedOperationsPolicy**, **OA CommonOperationsPolicy**, and **OA ReadOnlyAccessPolicy** permissions to the group. You are advised to assign the **OA FullAccessPolicy** permission to the group.

   NOTE

   - All permissions for OA are listed above. For more information, see **Permissions Management**.

2. **Create a user**.

   Create a user on the IAM console and add the user to the group created in **1**.

3. **Log in as the IAM user** and verify permissions.

   Log in to OA as the created user, and verify that it has the **OA FullAccessPolicy** permission.