Optimization Advisor

User Guide

Issue	01
Date	2026-04-22

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

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
1.1 Overview 1
1.2 Proactive Checks 2
1.3 Custom Check Rules 3
1.4 Risk Reports 4
1.5 Auto Checks 5
2 Architecture Design 7
2.1 Deployment Architecture 7
2.1.1 Creating a Deployment Architecture 7
2.1.2 Managing a Deployment Architecture 9
2.1.3 Enabling Capacity Risk Monitoring 9
2.1.4 Drawing a Deployment Architecture 11
2.1.5 Exporting the Resource List 14
2.2 Business Architectures 15
2.2.1 Creating a Business Architecture 15
2.2.2 Drawing a Business Architecture 16
2.3 Recycle Bin 18
3 Capacity Optimization 20
3.1 Daily Risk Prediction 20
3.2 KEA Period Risk Prediction 24
3.3 Viewing Monitoring Data 25
3.4 Capacity Reports 26
4 Resource Groups 27
4.1 Creating a Resource Group 27
4.2 Managing Resource Groups 27
5 Permissions Management 29
5.1 Using IAM to Grant Access to Optimization Advisor 29
5.1.1 Using IAM Roles or Policies to Grant Access to Optimization Advisor 29
5.1.2 Using IAM Identity Policies to Grant Access to OA 30
5.2 Permissions and Supported Actions 33
5.2.1 Introduction 33
5.2.2 Actions Supported by Policy-based Authorization 34

5.2.3 Actions Supported by Identity Policy-based Authorization..... 41

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 supports dedicated checks by cloud service type. This feature 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 checks
- Check report download
- Single-item checks and check report download
- Auto checks: You can enable scheduled checks and subscribe to check reports.
- Custom check rules
- Optimization suggestions

Check Results

There are three types of check results:

- **Risky**: Services are affected to different degrees after a fault.
- **Secure**: No risk is found. A periodic check is recommended.
- **N/A**: The related service or function is not enabled or is ignored. The check is unnecessary or irrelevant to your resource settings or service scenarios.
- **Warning**: An internal system exception occurs. You can try again. If the problem persists, **submit a service ticket** to contact technical support.

Risk Levels

There are two risk levels:

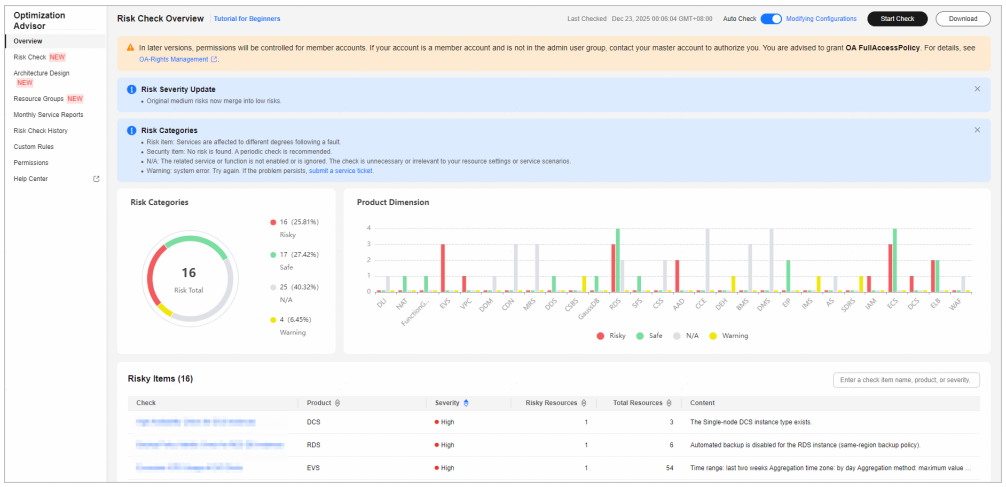
- **High-risk**: Services are interrupted after a fault.
- **Low-risk**: Services are slightly affected after a fault.

NOTE

Original medium risks now merge into low risks.

1.2 Proactive Checks

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



Procedure

Step 1 Go to the **Overview** page.

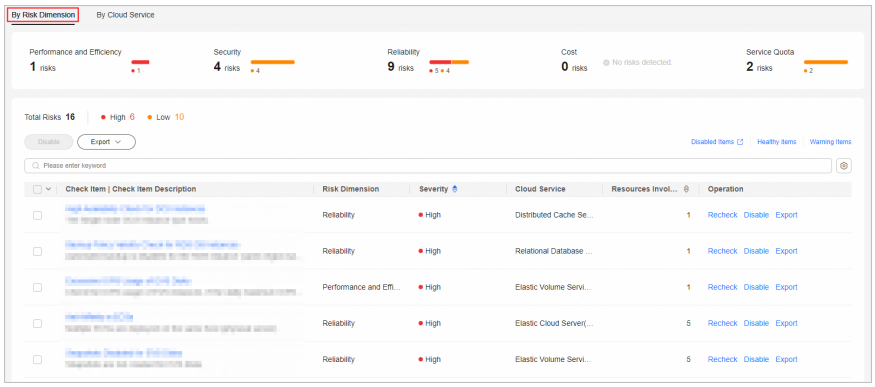
Step 2 Click **Start Check** in the upper right corner, set the check account and risk dimensions, and start the check.

Step 3 After the check progress reaches 100%, check that the check results are automatically updated on the risk check overview page.

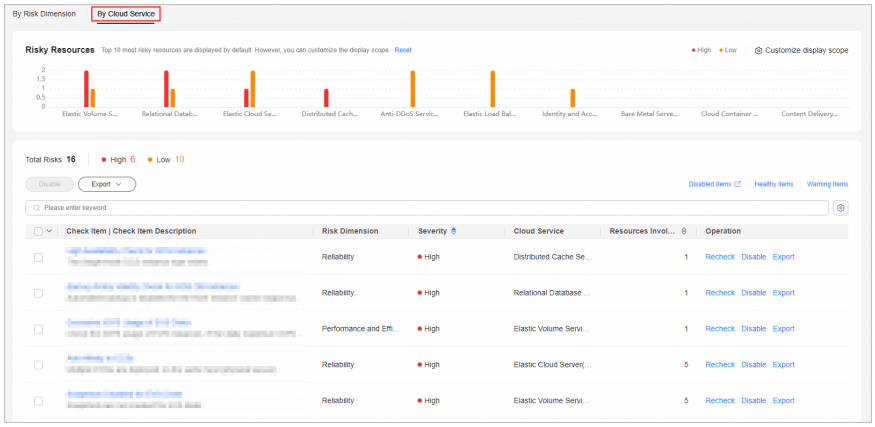
The check results include risk dimension statistics, risky product statistics, and the risky item list. You can click a check item to view its details.

Step 4 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.

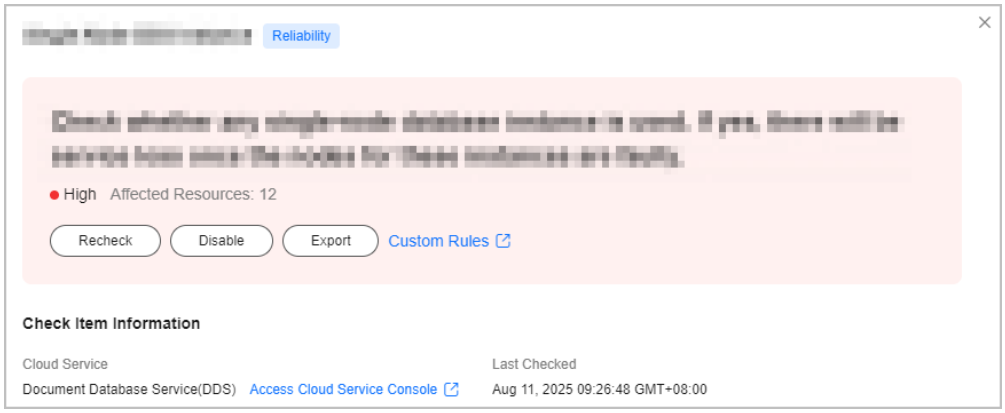
- **By Risk Dimension**: The check results include risk dimension statistics, risk levels, and the risky item list. You can click a risky item to view its details.



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



Step 5 After rectifying risky resources, re-check your resources using a single check item to verify the rectification. Click **Recheck** to refresh the check result.



----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 your specific needs. You can customize check rules as needed.

Procedure

Step 1 Go to the **Custom Rules** page.

Step 2 **Customize a single check rule.**

In the custom rule list, locate a check rule and click **Enable** in the **Operation** column.

To disable the check rule, click **Disable** in the **Operation** column.

To modify the risk threshold of the check rule, click **Configure Threshold**.

Step 3 **Customize check rules in batches.**

Select one or more check rules and click **Enable** above the list.

To disable the check rules, click **Disable**.

To restore the thresholds of the selected check rule to their default values, click **Restore Initial Settings**.

NOTE

- Blue actions are available and gray ones are unavailable After you enable a rule, only the **Disable** option is available. After you disable a rule, only the **Enable** option is available.
- You can only customize thresholds for some check items specific to performance and costs, or for cost-related items if you have purchased Business, Enterprise, or Enterprise On-Ramp support plans.
- Enabling or disabling a check item will take effect in the next check and will not impact the results of the previous check.

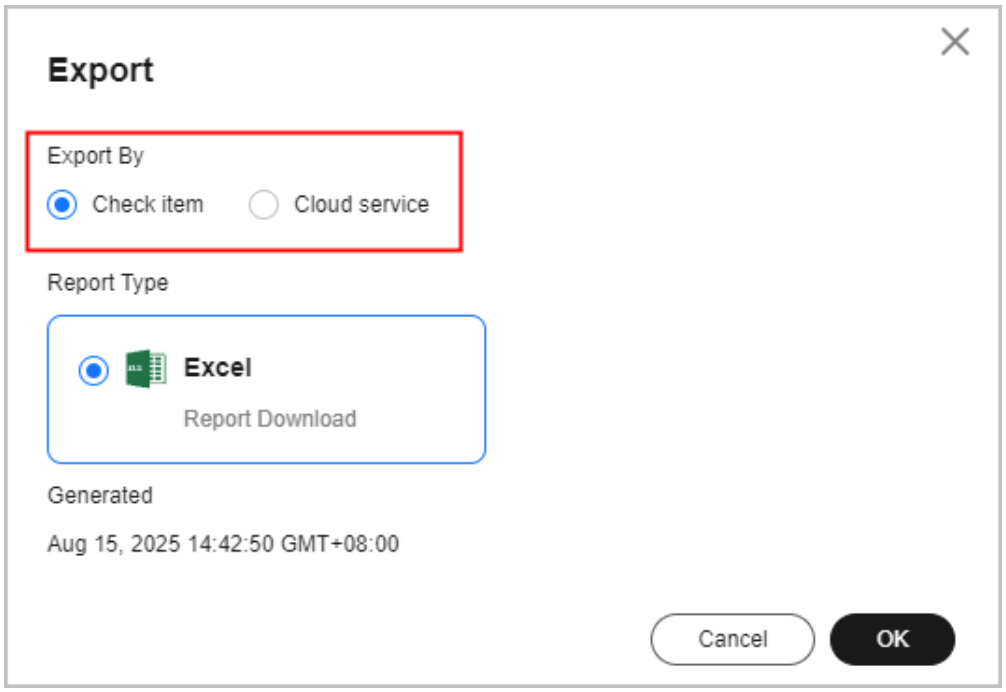
----End

1.4 Risk Reports

Procedure

Step 1 Go to the **Overview** page.

Step 2 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 report includes the check overview on the "Risk Check Overview" sheet and separated sheets for checked items.



Step 3 Export check 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 in the past month are displayed. Click a task ID to go to its details page. Click **Download** in the upper right corner to download the check report.

----End

1.5 Auto Checks

Scenarios

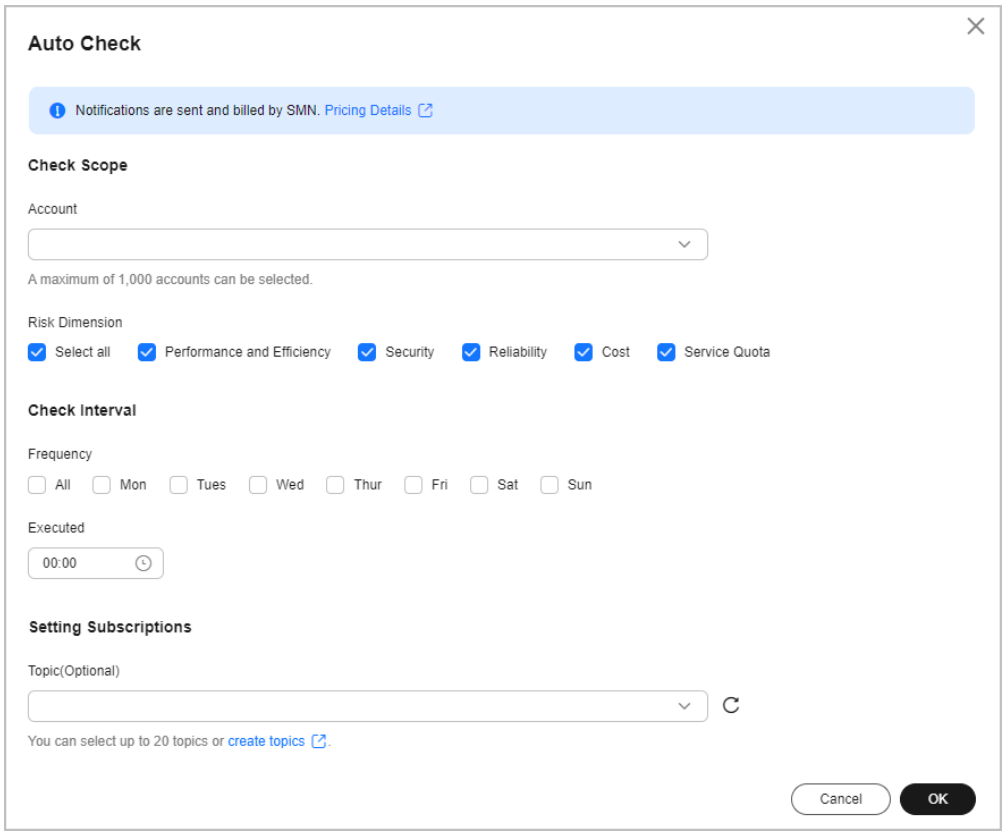
Auto Check lets you schedule regular risk checks by setting the interval and time. You can also receive risk check reports. This eases cloud resource management and ensures service stability.

Procedure

Step 1 Go to the **Overview** page.

Step 2 Enable **Auto Check** in the upper right corner.

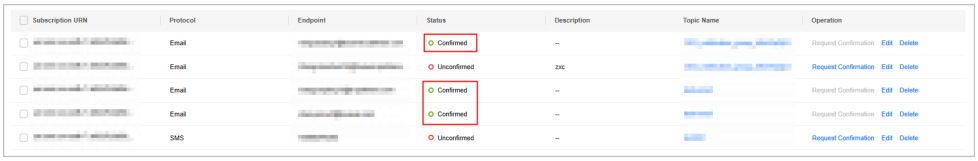
Step 3 In the displayed dialog box, set the risk dimension, execution frequency, and execution time.



Step 4 (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**.



----End

2 Architecture Design

2.1 Deployment Architecture

2.1.1 Creating a Deployment Architecture

Procedure

Step 1 Go to the **Architecture Design** page and click the **Architecture Design** tab.

Step 2 Click **Create Deployment Architecture** in the upper left corner. On the displayed page, select the architecture type, enter the architecture name, select the system type (no impact on drawing), enter a description about the architecture, and select the applicable platform (no impact on drawing).

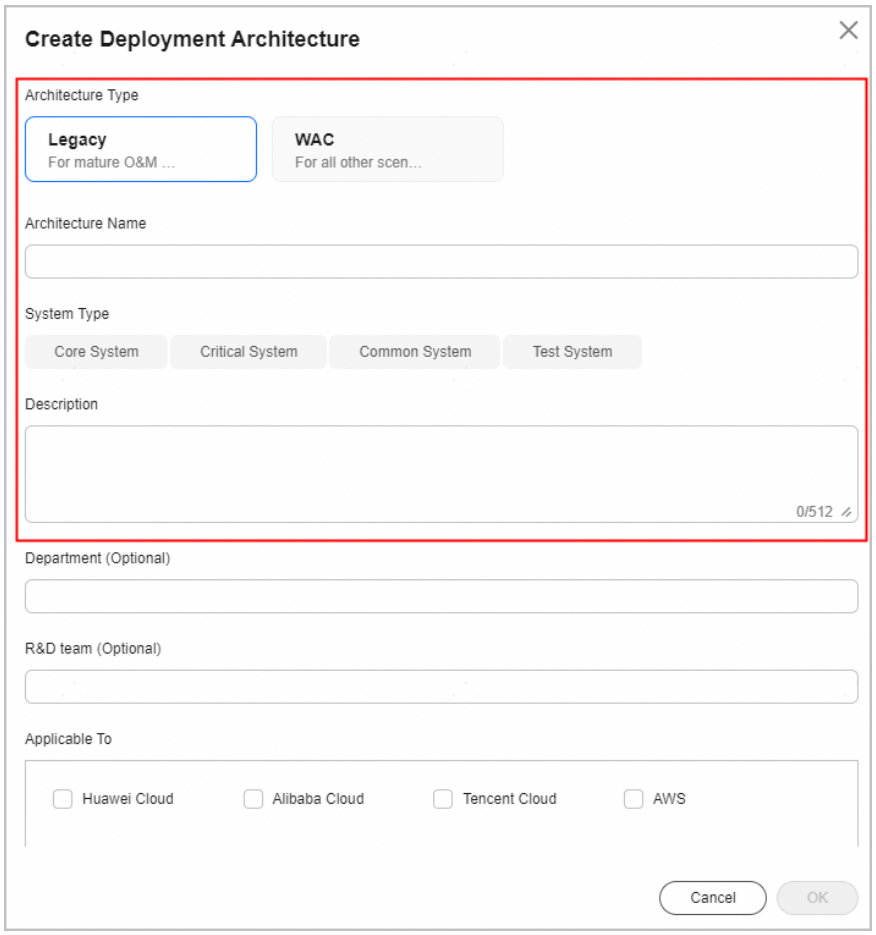
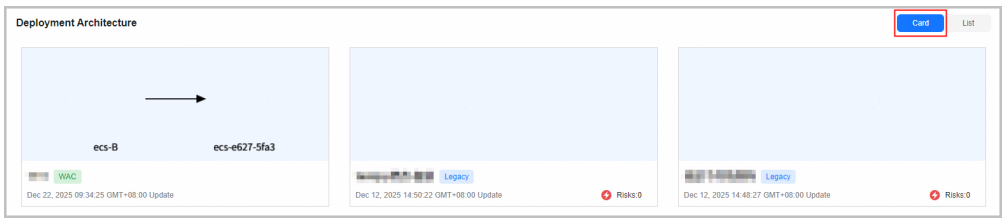


Table 2-1 Architecture type parameters

Parameter	Description
Legacy	For mature O&M systems needing high stability, consistency, and compliance and deep customization.
WAC	For all other scenarios. **NOTE** Only WAC architectures are displayed as thumbnails.

Step 3 View that the created deployment architecture is displayed in the **Card** view by default.



----End

2.1.2 Managing a Deployment Architecture

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

Procedure

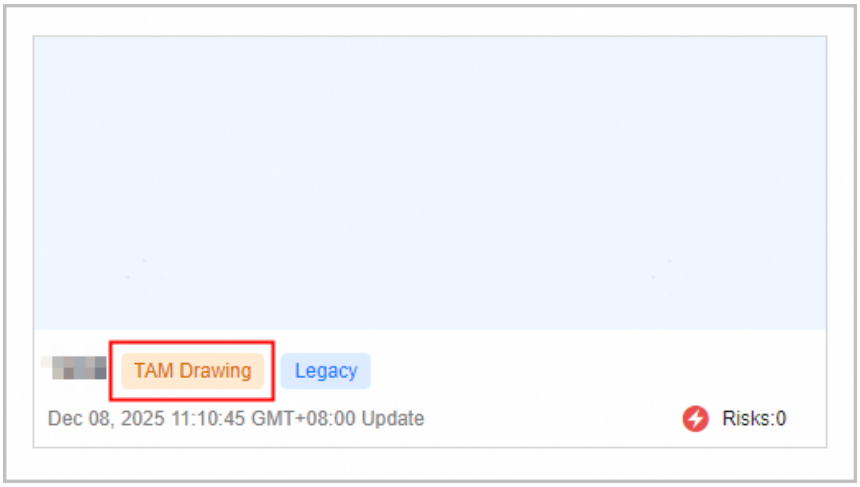
Step 1 Go to the **Architecture Design** page and click the **Architecture Design** tab.

Step 2 In the **Card** view of **Deployment Architecture**, hover the cursor over the target architecture to view, rename, export, copy, or delete the architecture.

Step 3 Click the target architecture to go to its details page. Click **Architecture Drawings** above the canvas to start drawing.

NOTE

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



----End

2.1.3 Enabling Capacity Risk Monitoring

This section describes how to enable capacity risk monitoring.

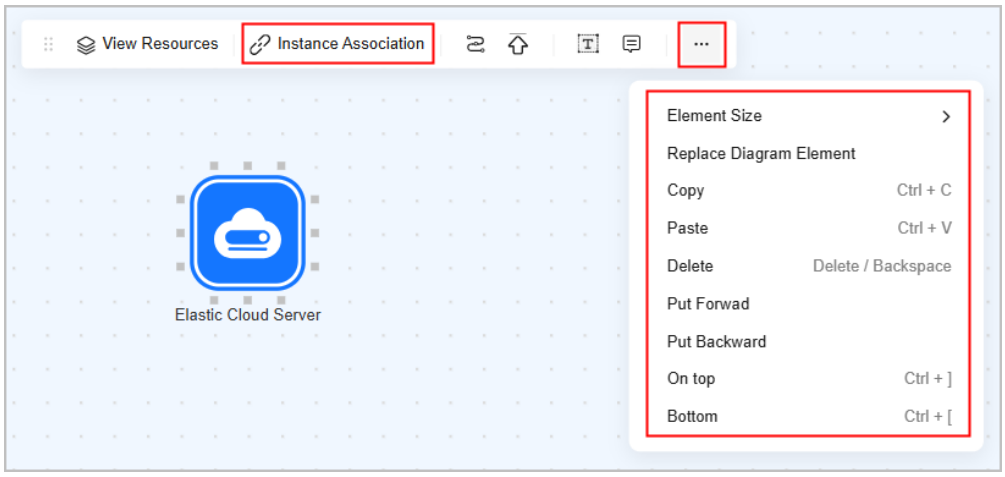
Procedure

Step 1 Go to the **Architecture Design** page and click the **Architecture Design** tab.

Step 2 In the card view of **Deployment Architecture**, click the target traditional architecture. On its details page, click **Architecture Drawings** above the canvas to start drawing.

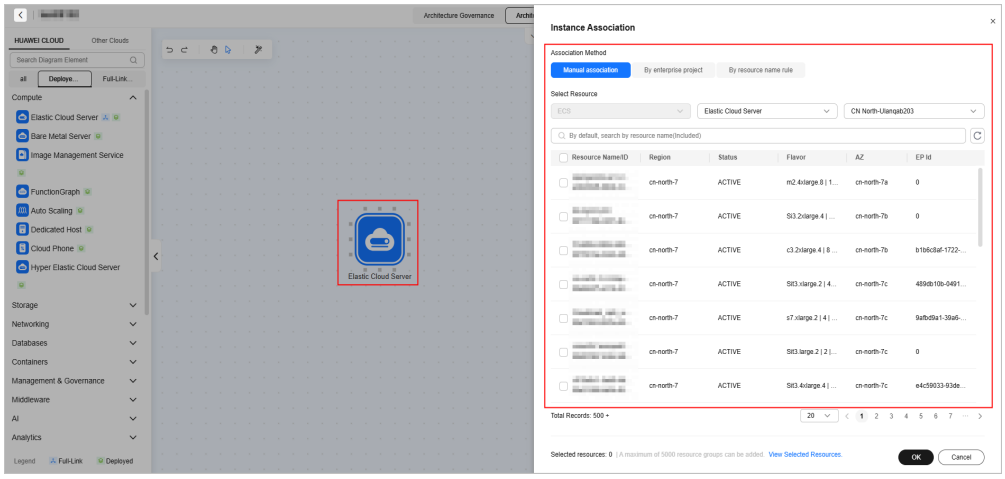
Step 3 On the left pane, choose **HUAWEI CLOUD** > **Deployed as Instances** in the drawing toolbar, and drag a cloud service diagram element (for example, **Elastic Cloud Server**) to the canvas.

Step 4 Click the cloud service diagram element. In the properties panel, you can modify its size, name, and remarks.



Step 5 Click **Instance Association** in the properties panel. In the displayed dialog box on the right, select an association method and resources.

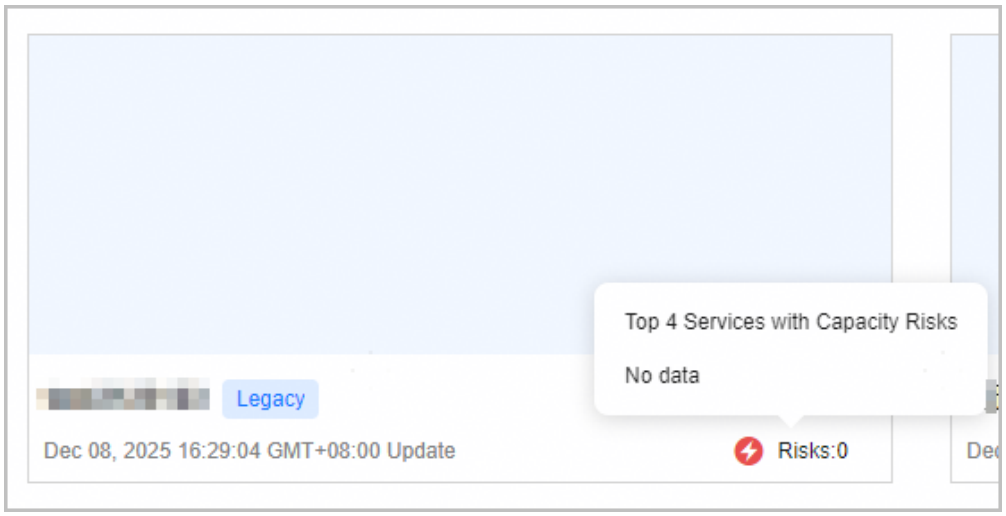
Select the resources to be monitored and click **OK**. The capacity risk monitoring is enabled for these resources.



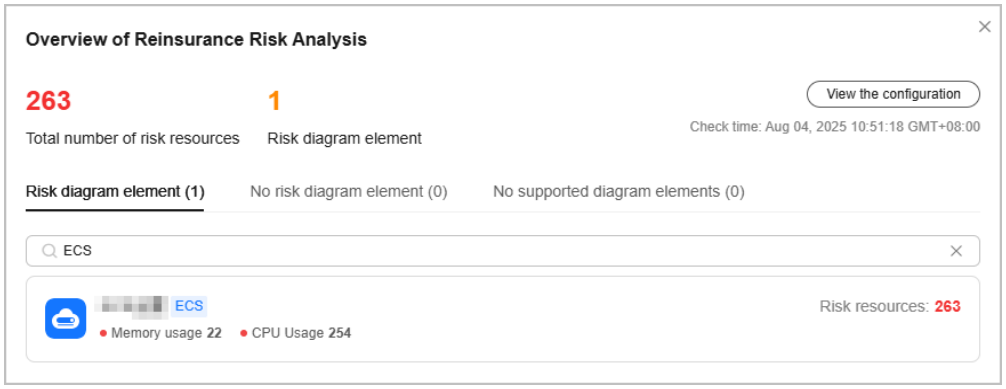
Step 6 Click **Architecture Governance** above the canvas. Click **Start Check** in **Resource Overview** on the left. In the **Configuring Capacity Monitoring Rules** dialog box on the right, select an analysis scenario, for example, **Routine risk analysis**. Click **Custom Risk Analysis**.

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 7 Click **Start Check**. The system analyzes the data and continuously monitors the check result. If risks are detected, the number of risks is displayed in the lower part of the deployment architecture card. Hover over the number to view the four cloud services with the most risks.

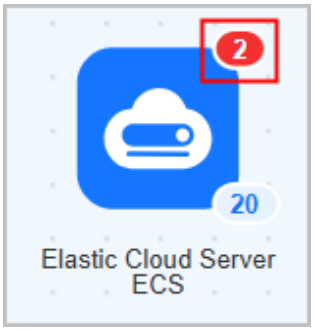


Step 8 Click the number next to a cloud service to go to the risk identification result page.



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 Go to the **Architecture Design** page and click the **Architecture Design** tab.

Step 2 Click **Create Deployment Architecture** in the upper left corner. On the displayed page, select the architecture type, enter the architecture name, select the system type (no impact on drawing), enter a description about the architecture, and select the applicable platform (no impact on drawing).

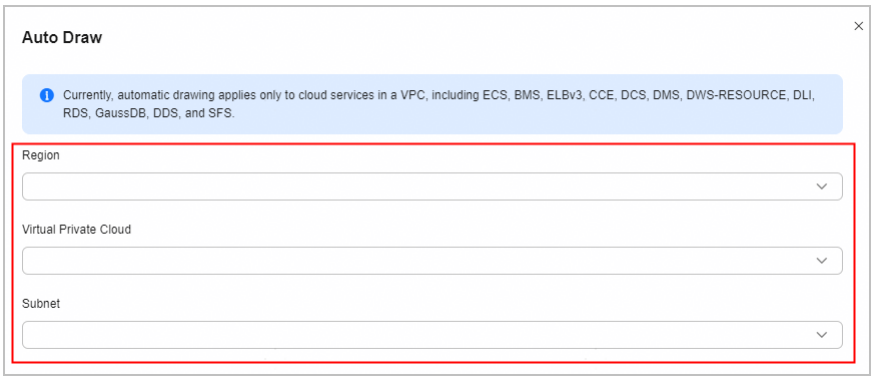
- Create a legacy architecture designed for mature O&M systems needing high stability, consistency, and compliance and deep customization.
- **Create a WAC architecture**, which is recommended for all other scenarios.

Step 3 **Create a legacy architecture.**

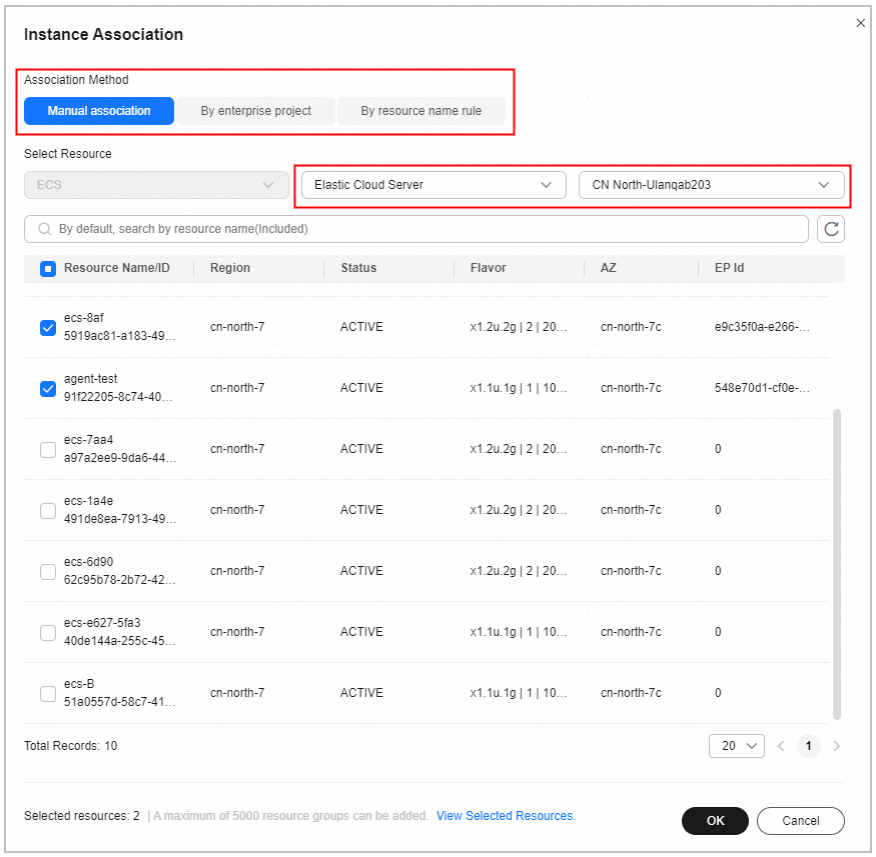
1. The created legacy architecture is displayed in card view by default. Click the created architecture to go to its details page. Then click **Architecture Drawings** above the canvas to start drawing.

2. On the left pane, view the basic diagram elements and cloud service diagram elements required for drawing.
3. 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.

4. In the **Auto Draw** dialog box, select a region, VPC, and subnet, and click **Start analysis**. The system will identify resources within the subnet and display them by layer according to the logical structure. If VPC flow logs are enabled, the system can also identify the relationships between resources.



5. 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 target region and resource type to search for ECS resources in the region, select the desired resources, and click **OK**.

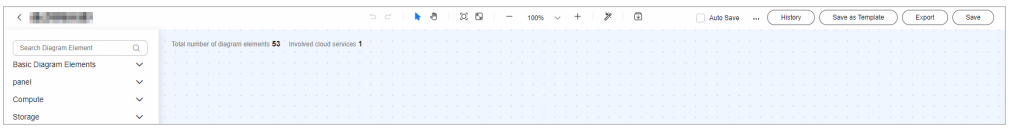


- **Full-link drawing**: Click the ECS diagram element and click  in the properties panel to draw a full-link diagram.

6. 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 target region and resource type to search for ECS resources in the region, select the desired resources, and click **OK**.

Step 4 Creating a WAC architecture.

1. By default, the created WAC architecture is displayed in card view. Click the created architecture to go to its details page.
2. On the left pane, view the basic diagram elements, panels, and cloud service diagram elements required for drawing.
3. The toolbar above the canvas provides multiple tools.



a.  : Use the default cursor mode.

b.  : Move the canvas.

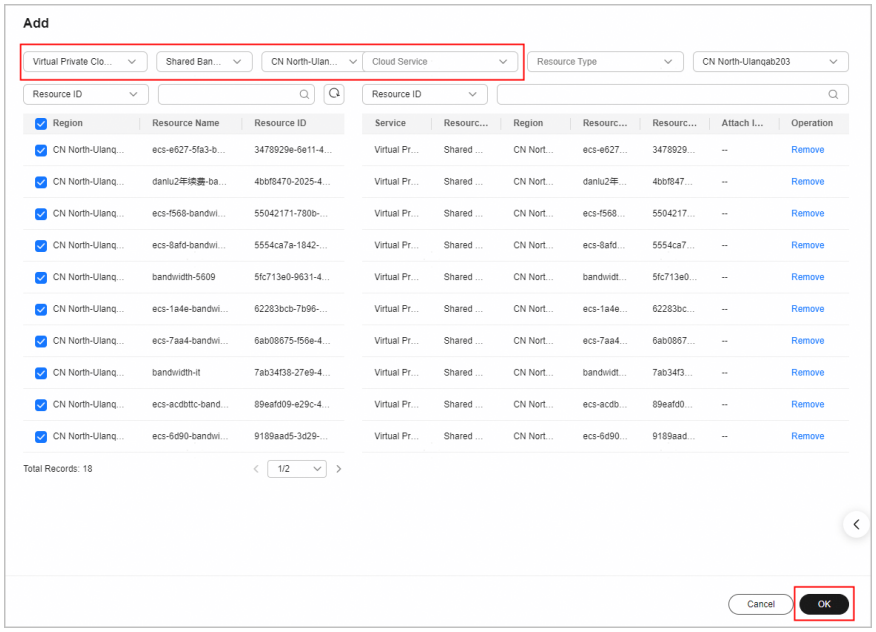
c.  : Center the canvas.

d.  : Enter full screen.

e.  : Polish the drawings.

f.  : Import inventory resources. (This will clear the canvas and generate an architecture based on the selected resources.)

After you click this icon, the page for adding resources is displayed. Set the cloud service, resource type, and region to search for resources. Select the required resources in the list, confirm the resource information on the right, and click **OK.** Then the system starts analysis.



4. Click **History** in the upper right corner of the canvas to view, restore, and delete the operation records of the architecture.
5. Click **Save as Template** in the upper right corner of the canvas to save the architecture to the template center. Then you can easily check data with the same search criteria.
6. Click **Export** in the upper right corner of the canvas to view data in the export format.

----End

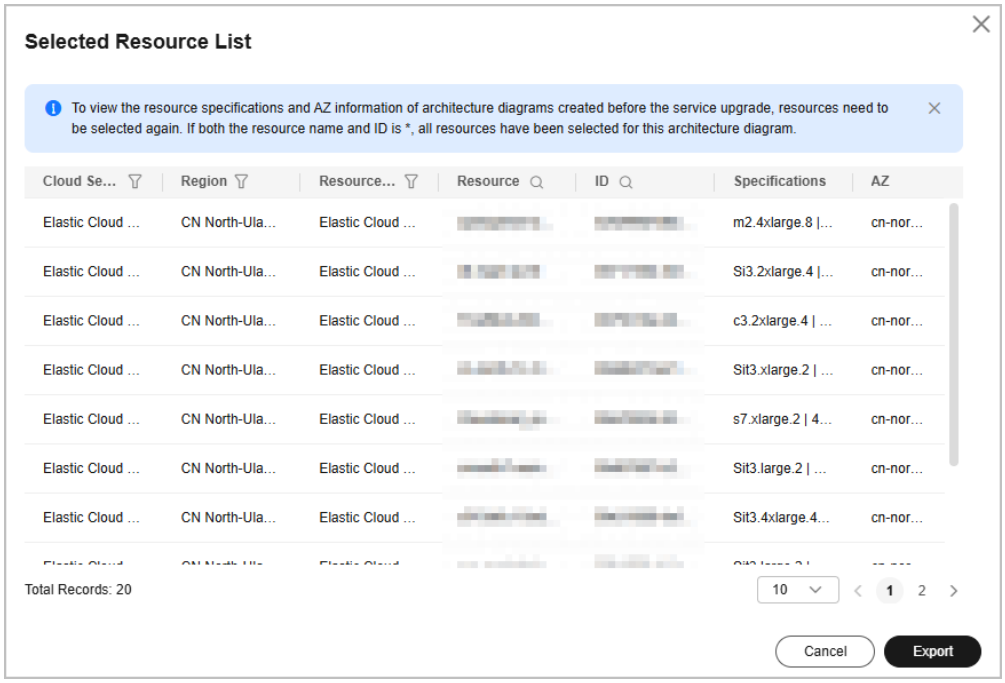
2.1.5 Exporting the Resource List

Procedure

Step 1 Go to the **Architecture Design** page and click the **Architecture Design** tab.

Step 2 In the card view of **Deployment Architecture**, click the target legacy architecture to go to its details page.

Step 3 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.



----End

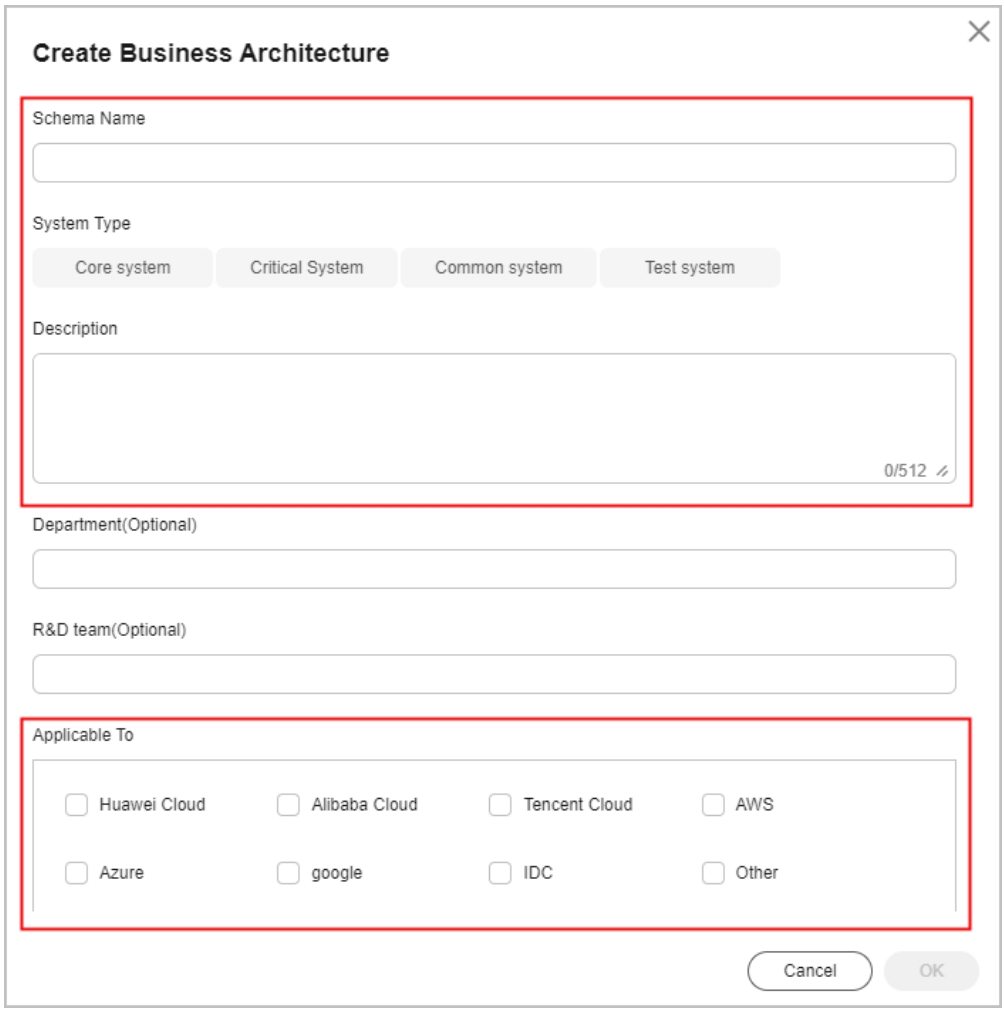
2.2 Business Architectures

2.2.1 Creating a Business Architecture

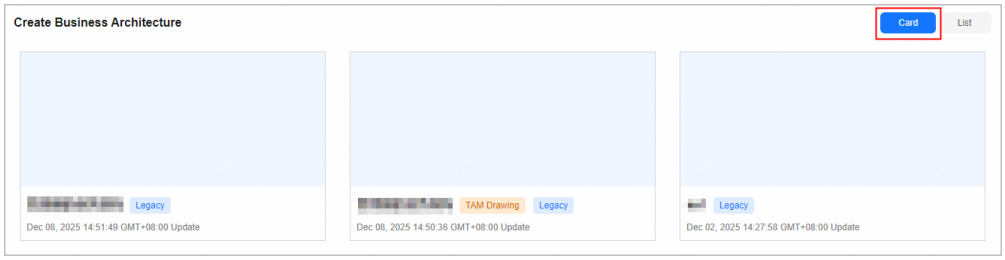
Procedure

Step 1 Go to the **Architecture Design** page and click the **Architecture Design** tab.

Step 2 Click **Create Business Architecture** in the upper left corner. On the displayed page, enter the architecture name, select the system type (no impact on drawing), enter a description about the architecture, and select the applicable platform (no impact on drawing).



Step 3 View that the created business architecture is displayed in the **Card** view by default.



----End

2.2.2 Drawing a Business Architecture

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

Procedure

Step 1 Go to the **Architecture Design** page and click the **Architecture Design** tab.

Step 2 Click **Create Business Architecture** in the upper left corner. On the displayed page, enter the architecture name, select the architecture type (no impact on

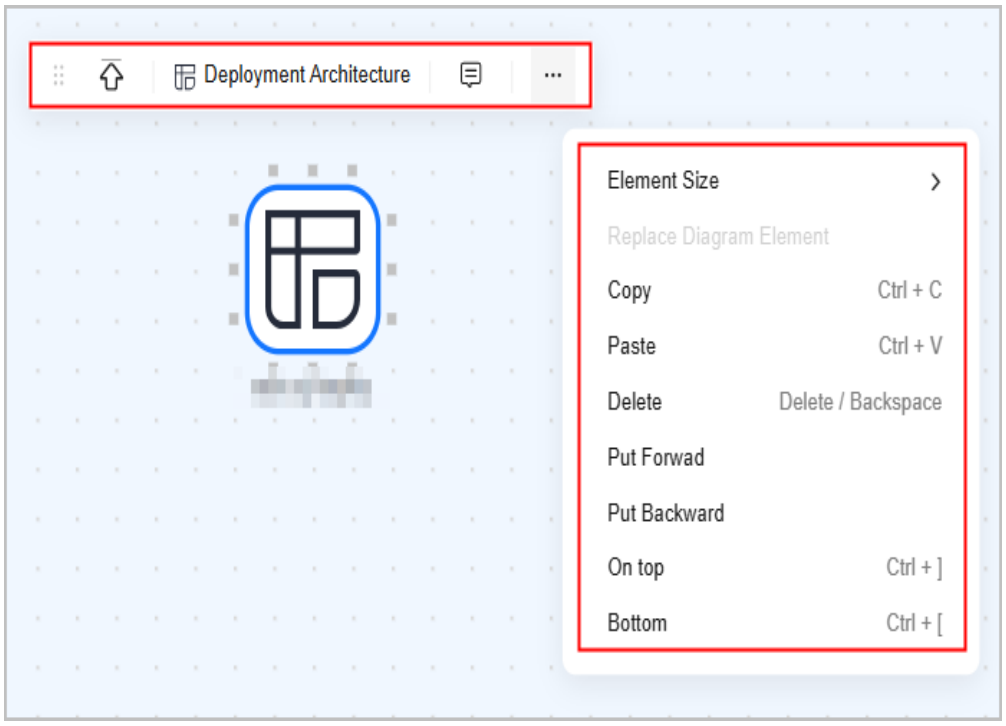
drawing), enter a description about the architecture, and select the deployment status (no impact on drawing).

Step 3 The created business architecture is displayed in the **Card** view by default. Hover the cursor over the created architecture to view, rename, export, copy, or delete the architecture.

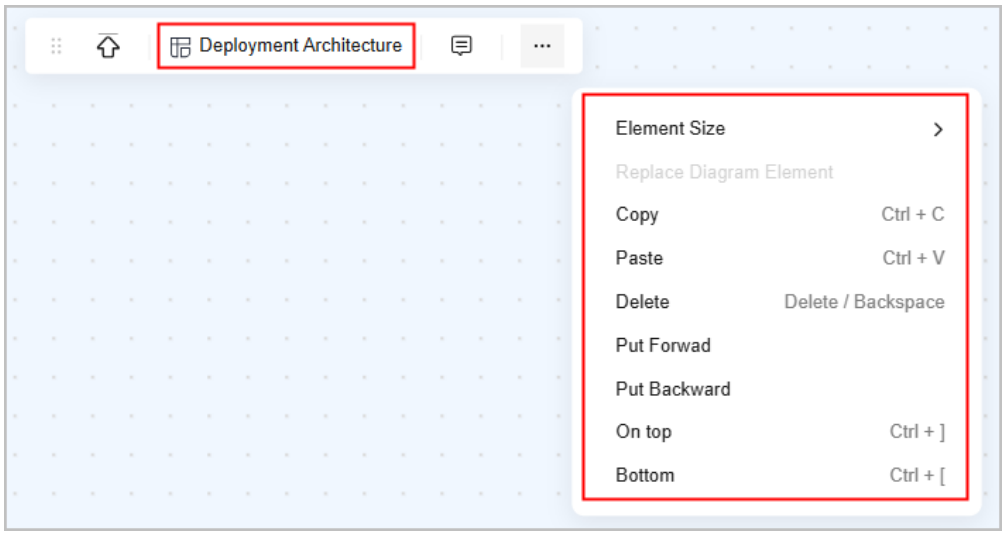
Step 4 Click the target architecture. On the displayed page, click **Browse** above the canvas to start editing.

Step 5 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.



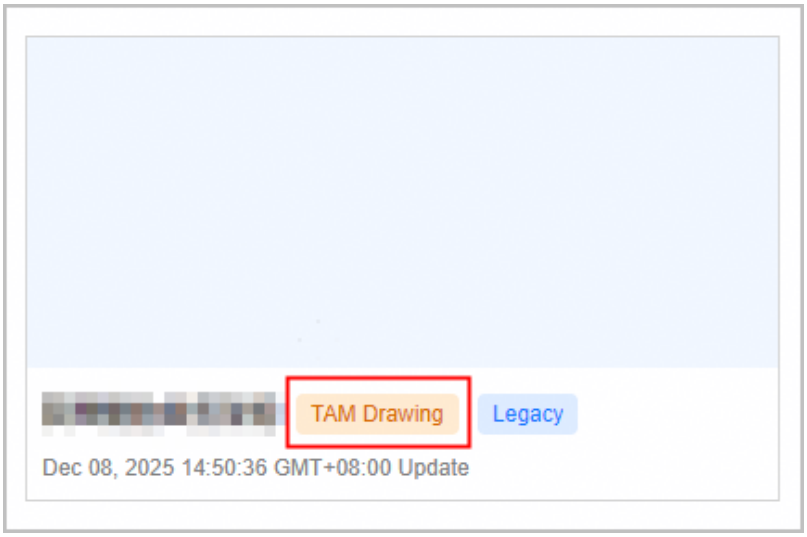
Step 6 In the left navigation pane, choose **Deployment Architecture** to display all created deployment architectures. You can directly drag one to the canvas for drawing. Click the **Deployment Architecture** diagram element in the canvas. In the properties panel, you can modify its size and remarks.



Step 7 Click **Deployment Architecture** in the properties panel. 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 lower 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.

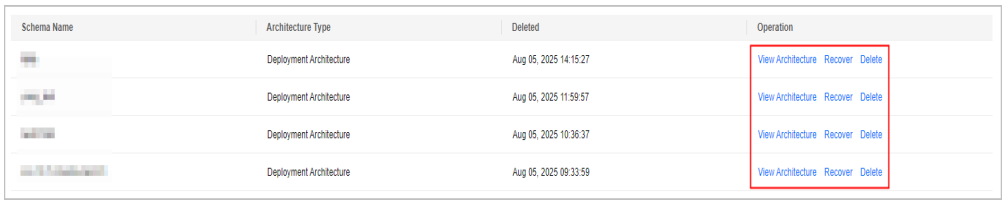


----End

2.3 Recycle Bin

Step 1 On the **Architecture Design** page, click **Recycle Bin** in the upper right corner.

Step 2 Filter and query deleted architectures by deletion time and architecture type, view deleted architectures in the list, and restore or permanently delete them.



NOTE

Deleted business and deployment architectures can be retained in the recycle bin for up to six months. After this 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 Go to the **Daily Risk Prediction** page.

Step 2 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 3 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

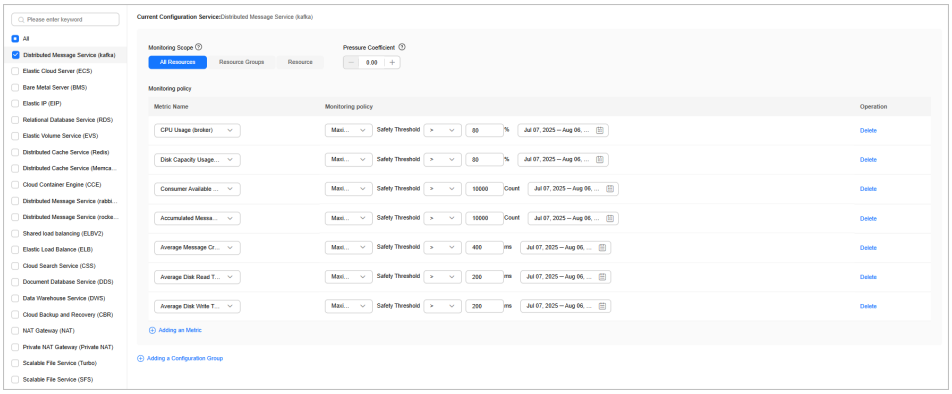
   An instance appears in the analysis result list only after the threshold is reached for *n* consecutive times.

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.

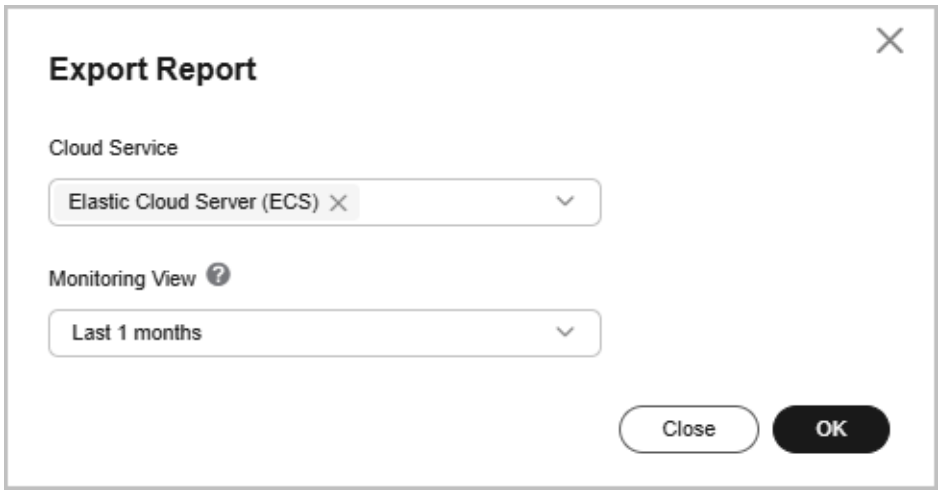
b. **Configuring the monitoring scope**: You can set different pressure coefficients and monitoring scopes for the selected cloud service. The monitoring scope can be **All Resources**, **Resource Groups**, or **Resource**.

- **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.



Step 4 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 5 Return to the **Custom Risk Analysis** page to view the check results. Click **Export** to download the check results.



----End

3.2 KEA Period Risk Prediction

Scenarios

KEA period risk prediction is available only to whitelisted users.

Procedure

Step 1 Go to the **KEA Period Risk Prediction** page.

Step 2 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.

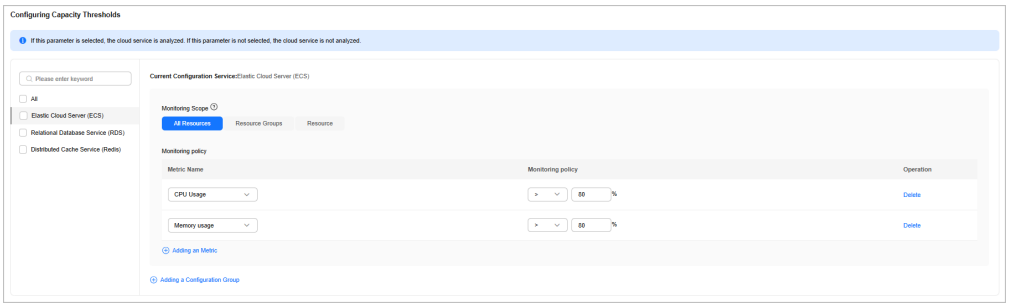
2. **Configure capacity thresholds.**

   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.



Step 3 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 4 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 Go to the **Optimization Advisor** page.

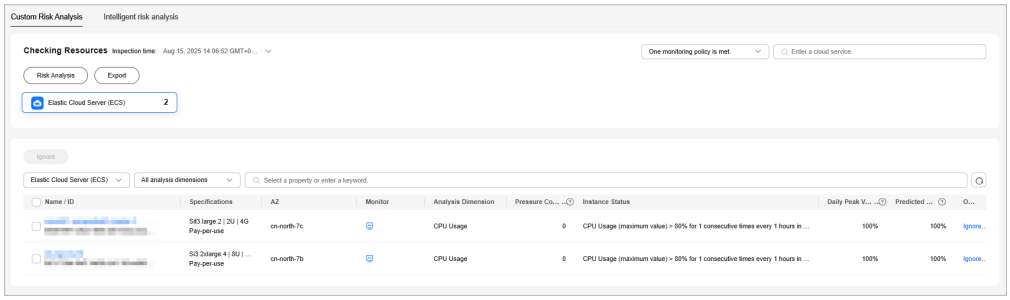
Step 2 In the navigation pane, choose **Capacity Optimization** > **Daily Risk Prediction** or **Key Period Risk Prediction**.

Step 3 In the upper right corner of the page, select a resource condition to search for resources.

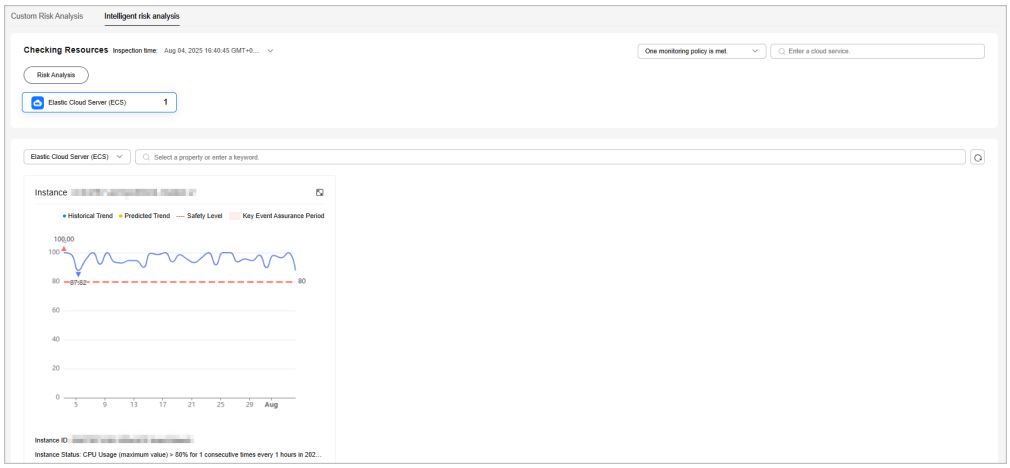
NOTE

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

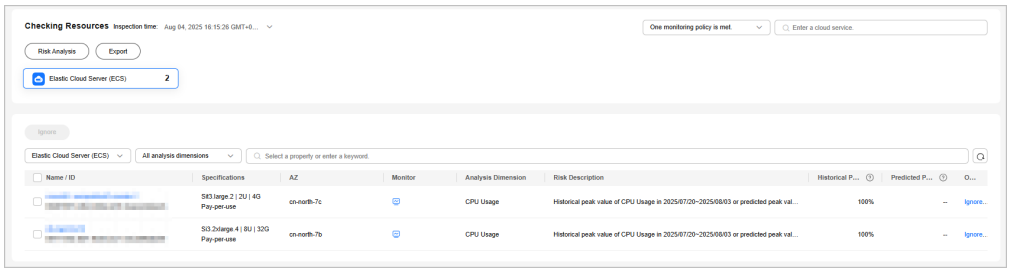
- **Custom risk analysis reports**: The risky instance list is displayed, as shown in the following figure.



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



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



Step 4 Click **Export** in the upper left corner to export the capacity risk report.

----End

3.4 Capacity Reports

Procedure

Step 1 Go to the **Optimization Advisor** page.

Step 2 Perform a **daily risk prediction** or **KEA period risk prediction**.

Step 3 In the navigation pane, choose **Capacity Optimization** > **Capacity Reports**.

Step 4 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 5 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

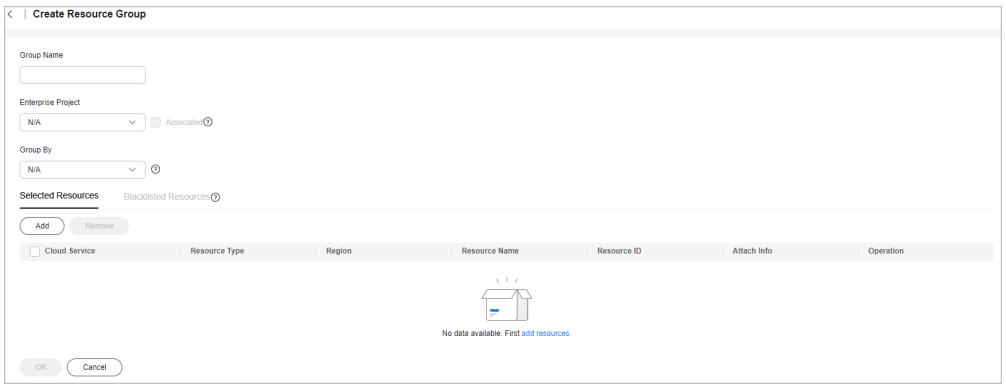
Procedure

Step 1 Go to the **Resource Groups** page.

Step 2 Click **Create** in the upper left corner. On the **Create Resource Group** page, set the group name, enterprise project, and grouping rules.

Step 3 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 4 Click **OK**. The resource group is created.



----End

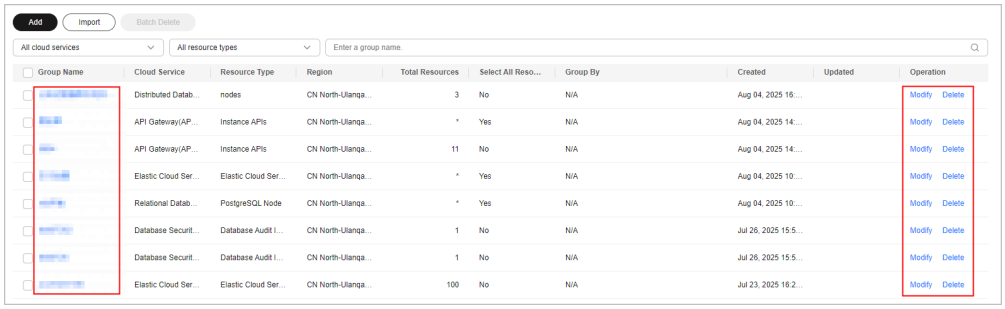
4.2 Managing Resource Groups

Procedure

Step 1 Go to the **Resource Groups** page.

Step 2 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.



----End

5 Permissions Management

5.1 Using IAM to Grant Access to Optimization Advisor

5.1.1 Using IAM Roles or Policies to Grant Access to Optimization Advisor

You can use **Identity and Access Management (IAM)** to implement fine-grained permissions control for your Optimization Advisor (OA) resources. With IAM, you can:

- Create IAM users or user groups for personnel based on your enterprise's organizational structure. Each IAM user has their own identity credentials for accessing OA.
- Grant users only the permissions required to perform a given task based on their job responsibilities.
- Entrust a Huawei Cloud account to perform efficient O&M on OA.

If your Huawei Cloud account meets your permissions requirements, you can skip this section.

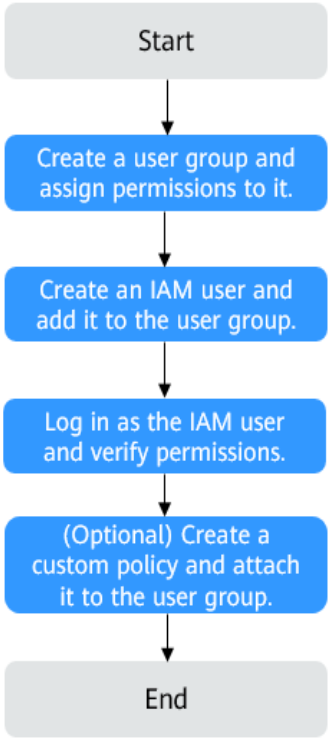
Figure 5-1 shows the process flow of role/policy-based authorization.

Prerequisites

Before granting permissions to user groups, learn about permissions supported by OA and select appropriate ones as needed. To grant permissions for other services, learn about all **system-defined permissions** supported by IAM.

Process Flow

Figure 5-1 Process of granting OA permissions to a user



1. On the IAM console, **create a user group and grant it permissions** (**BSS Administrator** as an example).

   Create a user group on the IAM console, and assign the **OA FullAccessPolicy** (recommended), **OA AdvancedOperationsPolicy**, **OA CommonOperationsPolicy**, or **OA ReadOnlyAccessPolicy** permission to the group.

2. **Create an IAM user and add it to the created user group**.

   On the IAM console, create a user and add it to the user group created in **1**.

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

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

5.1.2 Using IAM Identity Policies to Grant Access to OA

System-defined permissions in identity-based authorization provided by **Identity and Access Management (IAM)** let you control access to OA. With IAM, you can:

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

- Entrust a Huawei Cloud account to perform efficient O&M on OA.

If your Huawei Cloud account meets your permissions requirements, you can skip this section.

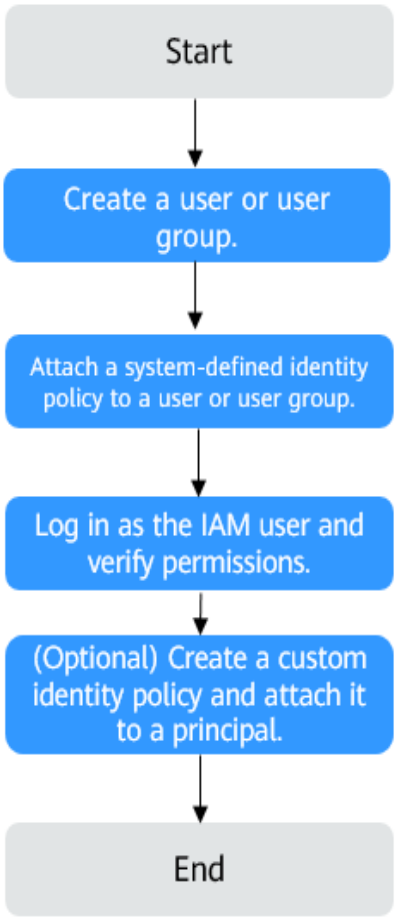
Figure 5-2 shows the process flow of identity policy-based authorization.

Prerequisites

Before granting permissions, learn about the **system-defined identity policies supported by OA**. To grant permissions for other services, learn about all **system-defined permissions** supported by IAM.

Process Flow

Figure 5-2 Process of granting OA permissions to a user



1. On the IAM console, **create an IAM user** or **create a user group**.
2. **Attach a system-defined identity policy** (**CostCenterReadOnlyPolicy** as an example) to the user or user group.

Assign the permissions defined in the system-defined identity policy **OAReadOnlyPolicy** to the user or group, or attach the system-defined identity policy to it.

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

   In the authorized region, perform the following operations:

   - On the Huawei Cloud official website, select **Optimization Advisor** from the drop-down list of your login account. Check whether you have the query permission. If so, the **OA ReadOnlyPolicy** policy is applied.
   - Add or delete data on any page in OA. If a message appears indicating that you have insufficient permissions to perform the operation, the **OA ReadOnlyPolicy** policy is in effect.

Example Custom Identity Policy for OA

You can create custom identity policies to supplement the system-defined identity policies of OA. For details about actions supported in custom identity policies, see **Actions Supported by Identity Policy-based Authorization**.

To create a custom identity policy, choose either visual editor or JSON.

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy grammar.
- JSON: Create a JSON policy or edit an existing one.

For details, see **Creating a Custom Identity Policy and Attaching It to a Principal**. The following provides examples of custom OA identity policies.

- Example 1: Grant the permission to perform a check for check items and obtain the check results.

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "oa:riskItemCheck:createTask",
        "oa:riskItemCheck:getTaskProgress",
        "oa:riskItemCheck:getTaskResult",
      ]
    }
  ]
}
```

- Example 2: Grant the permission to delete an architecture diagram, obtain architecture diagram details, create a single risk check task, obtain the progress of a single-item risk check task, and obtain the check results of a single risky item.

  A custom policy can contain the actions of one or multiple services.

  Example policy containing multiple actions:

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "oa:applications:delete",
        "oa:applications:get"
      ]
```



```
        },
        {
            "Effect": "Allow",
            "Action": [
                "oa:riskItemCheck:createTask",
                "oa:riskItemCheck:getTaskProgress",
                "oa:riskItemCheck:getTaskResult"
            ]
        }
    ]
}
```

5.2 Permissions and Supported Actions

5.2.1 Introduction

You can use Identity and Access Management (IAM) for fine-grained permissions management of your OA. If your account does not need individual IAM users, you can skip this section.

With IAM, you can control access to Huawei Cloud resources from principals (IAM users, groups, IAM agencies, or trust agencies) IAM supports role/policy-based authorization and identity policy-based authorization.

The following table describes the differences between these two authorization models.

Table 5-1 Differences between role/policy-based and identity policy-based authorization

Authorization Model	Core Relationship	Permissions	Authorization Method	Description
Role/Policy	User-permission-authorization scope	• System-defined roles • System-defined policies • Custom policies	Assigning roles or policies to principals	To authorize a user, you need to add it to a user group first and then specify the scope of authorization. It provides a limited number of condition keys and cannot meet the requirements of fine-grained permissions control. This method is suitable for small- and medium-sized enterprises.

Authorization Model	Core Relationship	Permissions	Authorization Method	Description
Identity policy	User-policy	• System-defined identity policies • Custom identity policies	• Assigning identity policies to principals • Attaching identity policies to principals	You can authorize a user by attaching an identity policy to it. User-specific authorization and a variety of key conditions allow for more fine-grained permissions control. However, this model can be hard to set up. It requires a certain amount of expertise and is suitable for medium- and large-sized enterprises.

Policies/identity policies and actions in the two authorization models are not interoperable. You are advised to use the identity policy-based authorization model.

5.2.2 Actions Supported by Policy-based Authorization

This section describes the actions supported by OA in policy-based authorization.

Supported Actions

OA provides system-defined policies that can be directly used in IAM. You can also create custom policies to supplement system-defined policies for more refined access control.

OA supports the following actions in custom policies.

Table 5-2 Actions supported by OA

Action	Description
oa:authorizations:list	Obtain the user authorization list.
oa:authorizations:update	Modify user authorizations.
oa:authorizations:delete	Delete user authorizations.
oa:monthReports:list	Obtain the monthly report list.
oa:monthReports:get	Obtain details about a monthly report.
oa:monthReports:download	Download a monthly report.

Action	Description
oa:checkItemRules:update	Modify check item rules.
oa:checkItemRules:list	Obtain check item rules.
oa:autoCheckRule:update	Modify auto check rules.
oa:autoCheckRule:get	Obtain auto check rules.
oa:riskItemsCheck:createTask	Create a risk check task.
oa:riskItemsCheck:getTaskProgress	Obtain the progress of a risk check task.
oa:riskItemsCheck:getTaskResult	Obtain the risk check results.
oa:riskItemsCheck:getTaskResultDimension	Obtain the dimensions of risk check results.
oa:riskItemsCheck:listReportSubscriptions	Obtain subscriptions to risk check reports.
oa:riskItemsCheck:getRiskItemNum	Obtain the number of risky items.
oa:riskItemsCheck:exportCheckItemResult	Export a risk check report.
oa:riskItemsCheck:getExportProgress	Obtain the progress of exporting a risk check report.
oa:riskItemsCheck:downloadCheckItemResult	Download a risk check report.
oa:riskItemCheck:createTask	Create a single-item risk check task.
oa:riskItemCheck:getTaskProgress	Obtain the progress of a single-item risk check task.
oa:riskItemCheck:getTaskResult	Obtain the check results of a single risky item.
oa:riskItemCheck:listTaskResultRegions	Obtain the list of sites for a single-item risk check report.
oa:wellArchitected:saveRecord	Save the well-architected questionnaire.
oa:wellArchitected:deleteRecord	Delete the well-architected questionnaire.
oa:wellArchitected:listRecord	View the well-architected questionnaire list.
oa:wellArchitected:getRecordDetail	Obtain well-architected questionnaire details.
oa:wellArchitected:generateReport	Generate a well-architected report.

Action	Description
oa:wellArchitected:getReportDetail	View well-architected report details.
oa:capacityAnalysis:getConfig	Obtain capacity optimization analysis settings.
oa:capacityAnalysis:updateConfig	Modify capacity optimization analysis settings.
oa:capacityAnalysis:listResourceTypes	Obtain the resource types for applying the capacity optimization analysis settings.
oa:capacityAnalysis:listResources	Obtain the resources for applying the capacity optimization analysis settings.
oa:capacityAnalysis:listResourceGroups	Obtain the resource groups for applying the capacity optimization analysis settings.
oa:capacityAnalysis:createJob	Create a capacity optimization analysis task.
oa:capacityAnalysis:getJobProgress	Obtain the progress of a capacity optimization analysis task.
oa:capacityAnalysis:stopJob	Stop a capacity optimization analysis task.
oa:capacityAnalysis:getResultSummary	Obtain the summary of capacity optimization analysis results.
oa:capacityAnalysis:listResultDetails	Obtain the details of capacity optimization analysis results.
oa:capacityAnalysis:deleteResultDetails	Delete the details of capacity optimization analysis results.
oa:capacityAnalysis:listReports	Obtain the list of capacity optimization analysis reports.
oa:capacityAnalysis:deleteReport	Delete a capacity optimization analysis report.
oa:capacityAnalysis:getReportExport-Progress	Obtain the progress for exporting a capacity optimization analysis report.
oa:capacityAnalysis:downloadReport	Download a capacity optimization analysis report.
oa:capacityAnalysis:exportReport	Export a capacity optimization analysis report.
oa:capacityAnalysis:exportExpertReport	Export an expert analysis report on capacity optimization.

Action	Description
oa:capacityAnalysis:startAvailability-CheckCapacityAnalysisJob	Create a capacity analysis task for availability check.
oa:applications:listCapacityAnalysis-SupportedServices	Obtain supported services from the capacity optimization dashboard.
oa:applications:listCapacityAnalysisRe-sults	Obtain the analysis results from the capacity optimization dashboard.
oa:capacityAnalysis:getListMetrics	Obtain metrics of risky resources for capacity optimization.
oa:capacityAnalysis:getListMonitor	Obtain the monitoring data of risky resources for capacity optimization.
oa:applications:list	Obtain the list of architecture diagrams.
oa:applications:get	Obtain architecture diagram details.
oa:applications:update	Modify basic information about an architecture diagram.
oa:applications:delete	Delete an architecture diagram.
oa:applications:updateView	Modify the settings of architecture diagram elements.
oa:applications:listServiceConfigs	Obtain the service configuration list of an architecture diagram.
oa:applications:getResourceConfig	Obtain resource parsing settings of an architecture diagram.
oa:resourceGroups:listApplicationRe-sources	Obtain resources by group from an architecture diagram via pagination.
oa:applications:downloadAttachedRe-sources	Export resources from an architecture diagram.
oa:applications:updateRiskSwitchStatus	Enable or disable risk statistics of an architecture diagram.
oa:applications:listRisks	Obtain the number of risks in an architecture diagram.
oa:applications:listHistorys	Obtain the list of historical records of an architecture diagram.
oa:applications:getHistory	Obtain the details of historical records of an architecture diagram.
oa:applications:restoreHistory	Restore a historical architecture diagram.

Action	Description
oa:applications:deleteHistory	Delete the historical records of an architecture diagram.
oa:applications:listRecycleApplications	List architecture diagrams in the recycle bin.
oa:system:listCesMetrics	Obtain Cloud Eye metrics.
oa:system:listCesMetricData	Obtain Cloud Eye metric details.
oa:system:getConfigItem	Obtain configuration items in the configuration center.
oa:capacityAnalysis:listHistoryReports	Obtain the list of historical capacity optimization analysis records.
oa:capacityAnalysis:listMetrics	Obtain metrics of risky resources for capacity optimization.
oa:capacityAnalysis:listMonitor	Obtain the monitoring data of risky resources for capacity optimization.
oa:system:getAutoloadData	Obtain the auto-loaded data.
oa:capacityAnalysis:listResultMonitorData	Obtain the monitoring data from KEA risk analysis results.
oa:applications:getSummary	Obtain the architecture diagram summary.
oa:applications:startAutomaticDrawAnalysis	Create an automatic drawing analysis task.
oa:applications:getAutomaticDrawAnalysisProgress	Obtain the progress of an automatic drawing analysis task.
oa:applications:getAutomaticDrawAnalysisResult	Obtain the result of an automatic drawing analysis task.
oa:applications:getVpcFlowLogsDockingStatus	Obtain the interconnection status of VPC flow logs.
oa:resourceGroups:list	Obtain the resource group list.
oa:resourceGroups:get	Obtain resource group details.
oa:resourceGroups:update	Modify a resource group.
oa:resourceGroups:delete	Delete a resource group.
oa:resourceGroups:listRegions	List the regions that the resource groups belong to.
oa:resourceGroups:listResources	List the resources in a resource group.
oa:resourceGroups:listEnterpriseProjectResources	List the resources of an enterprise project.

Action	Description
oa:system:listServiceMetrics	List metrics of a cloud service.
oa:system:listAlarmMetrics	List alarm metrics.
oa:applications:listServiceResources	List cloud service resources of an architecture design.
oa:applications:saveResourceGroup	Save resource groups of an architecture design.
oa:system:listResourceTypes	List resource types.
oa:resourceGroups:listAll	List all resource groups.
oa:applications:downloadResourceTemplate	Download the resource import template for an architecture design.
oa:applications:importResources	Import resources for an architecture design.
oa:applications:getResourcesImportResult	Obtain the resource import results of an architecture design.
oa:applications:saveResourceGroupsBatch	Save resource groups in an architecture design in batches.
oa:applications:getBatchSaveResourceGroupsResult	Obtain the results for batch saving resource groups in an architecture design.
oa:resourceGroups:downloadResourceTemplate	Download resource import template for a resource group.
oa:resourceGroups:importResources	Import resources to a resource group.
oa:resourceGroups:getResourcesImportResult	Obtain the resource import results of a resource group.
oa:applications:startServiceRecommendAnalysis	Start service recommendation analysis.
oa:applications:getServiceRecommendAnalysisResult	Obtain the service recommendation analysis results.
oa:applications:listAttachedResources	List resources associated with an architecture diagram.
oa:applications:listNodeAttachedResources	List resources corresponding to a diagram element.
oa:riskItemsCheck:listReportsV4	Obtain risk check reports.
oa:riskItemsCheck:listReports	Obtain risk check reports.
oa:riskItemsCheck:getReportSubscriptionRule	Obtain the subscription rules for risk check reports.

Action	Description
oa:applications:deleteAll	Delete all architecture diagrams.
oa:riskItemsCheck:updateReportSubscriptionRule	Modify the subscription rules for risk check reports.
oa:riskItemsCheck:listMeters	Obtain availability check CDRs.
oa:applications:saveResourceChanges	Save changes to architecture diagram resources.
oa:capacityAnalysis:deleteAll	Delete all capacity optimization analysis reports.
oa:resourceGroups:deleteAll	Delete all resource groups.
oa:applications:listResources	List cloud service resources of an architecture diagram.
oa:system:listMetrics	List metrics.
oa:riskItemsCheck:listCheckItems	List check items.
oa:riskItemsCheck:listOrgAccounts	List organization member accounts.
oa:system:listMetricData	List metric data.
oa:system:getAutoloadResources	Obtain auto-access resource data.
oa:applications:listApplicationNames	Query architecture diagram names.
oa:system:getAutoloadConfigs	Obtain system auto-loaded configurations.
oa::getTask	Query job progress.
oa:ignoredResourceConfig:create	Add a resource exclusion rule.
oa:ignoredResourceConfig:delete	Delete a resource exclusion rule.
oa:ignoredResourceConfig:update	Update a resource exclusion rule.
oa:ignoredResourceConfig:enable	Enable or disable a resource exclusion rule.
oa:ignoredResourceConfig:get	Query details about resources in a resource exclusion rule.
oa:ignoredResourceConfig:list	Query details about a resource exclusion rule.
oa:ignoredResourceConfig:listEnterpriseProjects	List enterprise projects in a resource exclusion rule.

5.2.3 Actions Supported by Identity Policy-based Authorization

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the **Organizations** service also provides **service control policies (SCPs)** for access control.

SCPs do not actually grant any permissions to a principal. They only set the permissions boundary for the principal. When SCPs are attached to a member account or an organizational unit (OU), they do not directly grant permissions to that member account or OU. Instead, the SCPs just determine what permissions are available for that member account or the member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM policies are different from Organizations SCPs, see **What Are the Differences Between IAM Policies and Organizations SCPs?**

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see **Creating a Custom Identity Policy**.
- For details about how to use these elements to edit a custom SCP policy, see **Creating an SCP**.

Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The **Access Level** column describes how the action is classified (such as **list**, **read**, or **write**). This classification helps you understand the level of access that an action grants when you use it in a policy.
- The **Resource Type** column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your statements.
  - Required resources are marked with asterisks (*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

  For details about the resource types defined by OA, see **Resources**.
- The **Condition Key** column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the **Resource Type** column has values for an action, the condition key takes effect only for the listed resource types.
  - If the **Resource Type** column is empty (-) for an action, the condition key takes effect for all resources that action supports.

  - If the **Condition Key** column is empty (-) for an action, the action does not support any condition keys.

  For details about the condition keys defined by OA, see **Conditions**.

- The **Alias** column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see **Policies and Identity Policies**.

The following table lists the actions that you can define in identity policy statements for OA.

Table 5-3 Actions supported by OA

Action	Description	Access Level	Resource Type (Must Specify All Using "*")	Condition Key	Alias
oa::listAuthorizations	Grants permission to obtain the user authorization list.	read	-	-	oa:authorizations:list
oa::updateAuthorizations	Grants permission to modify user authorizations.	write	-	-	oa:authorizations:update
oa::deleteAuthorizations	Grants permission to delete user authorizations.	write	-	-	oa:authorizations:delete
oa:monthReports:list	Grants permission to obtain the monthly report list.	read	-	-	-
oa:monthReports:get	Grants permission to get details about a monthly report.	read	-	-	-
oa:monthReports:download	Grants permission to download a monthly report.	read	-	-	-
oa:checkItemRules:update	Grants permission to modify check item rules.	write	-	-	-

Action	Description	Access Level	Resource Type (Must Specify All Using "*")	Condition Key	Alias
oa:checkItemRules:list	Grants permission to obtain check item rules.	read	-	-	-
oa:autoCheckRule:update	Grants permission to modify auto check rules.	write	-	-	-
oa:autoCheckRule:get	Grants permission to get auto check rules.	read	-	-	-
oa:riskItemsCheck:createTask	Grants permission to create a risk check task.	write	-	-	-
oa:riskItemsCheck:getTaskProgress	Grants permission to obtain the progress of a risk check task.	read	-	-	-
oa:riskItemsCheck:getTaskResult	Grants permission to obtain the risk check results.	read	-	-	-
oa:riskItemsCheck:getTaskResultDimension	Grants permission to obtain the dimensions of risk check results.	read	-	-	-
oa:riskItemsCheck:listReportSubscriptions	Grants permission to obtain subscriptions to risk check reports.	read	-	-	-
oa:riskItemsCheck:getReportSubscriptionRule	Grants permission to obtain the subscription rules for risk check reports.	read	-	-	-

Action	Description	Access Level	Resource Type (Must Specify All Using "*")	Condition Key	Alias
oa:riskItemsCheck:updateReportSubscriptionRule	Grants permission to modify the subscription rules for risk check reports.	write	-	-	-
oa:riskItemsCheck:getRiskItemNum	Grants permission to obtain the number of risky items.	read	-	-	-
oa:riskItemsCheck:exportCheckItemResult	Grants permission to export a risk check report.	read	-	-	-
oa:riskItemsCheck:getExportProgress	Grants permission to obtain the progress of exporting a risk check report.	read	-	-	-
oa:riskItemsCheck:downloadCheckItemResult	Grants permission to download a risk check report.	read	-	-	-
oa:riskItemCheck:createTask	Grants permission to create a single-item risk check task.	write	-	-	-
oa:riskItemCheck:getTaskProgress	Grants permission to obtain the progress of a single-item risk check task.	read	-	-	-
oa:riskItemCheck:getTaskResult	Grants permission to obtain the check results of a single risky item.	read	-	-	-

Action	Description	Access Level	Resource Type (Must Specify All Using "*")	Condition Key	Alias
oa:riskItemCheck:listTaskResultRegions	Grants permission to obtain the list of sites for a single-item risk check report.	read	-	-	-
oa:riskItemsCheck:listCheckItems	Grants permission to obtain the list of check item rules.	read	-	-	-
oa::saveWellArchitectedRecord	Grants permission to save the well-architected questionnaire.	write	-	-	oa:wellArchitected:saveRecord
oa::deleteWellArchitectedRecord	Grants permission to delete the well-architected questionnaire.	write	-	-	oa:wellArchitected:deleteRecord
oa::listWellArchitectedRecord	Grants permission to view the well-architected questionnaire list.	read	-	-	oa:wellArchitected:listRecord
oa::getWellArchitectedRecordDetail	Grants permission to obtain well-architected questionnaire details.	read	-	-	oa:wellArchitected:getRecordDetail
oa::generateWellArchitectedReport	Grants permission to generate a well-architected report.	write	-	-	oa:wellArchitected:generateReport
oa::getWellArchitectedReportDetail	Grants permission to view well-architected report details.	read	-	-	oa:wellArchitected:getReportDetail

Action	Description	Access Level	Resource Type (Must Specify All Using "*")	Condition Key	Alias
oa::listOrgAccounts	Grants permission to obtain the list of organization member accounts.	read	-	-	oa:riskItemsCheck:listOrgAccounts
oa:capacityAnalysis:getConfig	Grants permission to obtain capacity optimization analysis settings.	read	-	-	-
oa:capacityAnalysis:updateConfig	Grants permission to modify capacity optimization analysis settings.	write	-	-	-
oa:capacityAnalysis:listResourceTypes	Grants permission to obtain the resource types for applying the capacity optimization analysis settings.	read	-	-	-
oa:capacityAnalysis:listResources	Grants permission to obtain the resources for applying the capacity optimization analysis settings.	read	-	-	-
oa:capacityAnalysis:listResourceGroups	Grants permission to obtain the resource groups for applying the capacity optimization analysis settings.	read	-	-	-

Action	Description	Access Level	Resource Type (Must Specify All Using "*")	Condition Key	Alias
oa:capacityAnalysis:createJob	Grants permission to create a capacity optimization analysis task.	write	-	-	-
oa:capacityAnalysis:getJobProgress	Grants permission to obtain the progress of a capacity optimization analysis task.	read	-	-	-
oa:capacityAnalysis:stopJob	Grants permission to stop a capacity optimization analysis task.	write	-	-	-
oa:capacityAnalysis:getResultSummary	Grants permission to obtain the summary of capacity optimization analysis results.	read	-	-	-
oa:capacityAnalysis:listResultDetails	Grants permission to obtain the details of capacity optimization analysis results.	read	-	-	-
oa:capacityAnalysis:deleteResultDetails	Grants permission to delete the details of capacity optimization analysis results.	write	-	-	-
oa:capacityAnalysis:listReports	Grants permission to obtain the list of capacity optimization analysis reports.	read	-	-	-

Action	Description	Access Level	Resource Type (Must Specify All Using "*")	Condition Key	Alias
oa:capacityAnalysis:deleteReport	Grants permission to delete a capacity optimization analysis report.	write	-	-	-
oa:capacityAnalysis:getReportExport-Progress	Grants permission to obtain the progress for exporting a capacity optimization analysis report.	read	-	-	-
oa:capacityAnalysis:downloadReport	Grants permission to download a capacity optimization analysis report.	read	-	-	-
oa:capacityAnalysis:exportReport	Grants permission to export a capacity optimization analysis report.	read	-	-	-
oa:capacityAnalysis:exportExpertReport	Grants permission to export an expert analysis report on capacity optimization.	read	-	-	-
oa:applications:list	Grants permission to obtain the list of architecture diagrams.	read	-	-	-
oa:applications:get	Grants permission to obtain architecture diagram details.	read	-	-	-

Action	Description	Access Level	Resource Type (Must Specify All Using "*")	Condition Key	Alias
oa:applications:update	Grants permission to modify basic information about an architecture diagram.	write	-	-	-
oa:applications:delete	Grants permission to delete an architecture diagram.	write	-	-	-
oa:applications:updateView	Grants permission to modify the settings of architecture diagram elements.	write	-	-	-
oa:applications:listServiceConfigs	Grants permission to obtain the service configuration list of an architecture diagram.	read	-	-	-
oa:applications:getResourceConfig	Grants permission to obtain resource parsing settings of an architecture diagram.	read	-	-	-
oa:applications:updateRiskSwitchStatus	Grants permission to enable or disable risk statistics of an architecture diagram.	write	-	-	-
oa:applications:listRisks	Grants permission to obtain the number of risks in an architecture diagram.	read	-	-	-

Action	Description	Access Level	Resource Type (Must Specify All Using "*")	Condition Key	Alias
oa:applications:listHistorys	Grants permission to obtain the list of historical records of an architecture diagram.	read	-	-	-
oa:applications:getHistory	Grants permission to obtain the details of historical records of an architecture diagram.	read	-	-	-
oa:applications:restoreHistory	Grants permission to restore a historical architecture diagram.	write	-	-	-
oa:applications:deleteHistory	Grants permission to delete the historical records of an architecture diagram.	write	-	-	-
oa:applications:listRecycleApplications	Grants permission to list architecture diagrams in the recycle bin.	read	-	-	-
oa::listSystemCesMetrics	Grants permission to obtain Cloud Eye metrics.	read	-	-	oa:system:listCesMetrics
oa::listSystemCesMetricData	Grants permission to obtain Cloud Eye metric details.	read	-	-	oa:system:listCesMetricData

Action	Description	Access Level	Resource Type (Must Specify All Using "*")	Condition Key	Alias
oa::getSystemConfigItem	Grants permission to obtain configuration items in the configuration center.	read	-	-	oa:system:getConfigItem
oa:capacityAnalysis:listHistoryReports	Grants permission to obtain the list of historical capacity optimization analysis records.	read	-	-	-
oa:capacityAnalysis:listMetrics	Grants permission to obtain metrics of risky resources for capacity optimization.	read	-	-	-
oa:capacityAnalysis:listMonitor	Grants permission to obtain the monitoring data of risky resources for capacity optimization.	read	-	-	-
oa::getAutoloadData	Grants permission to obtain the auto-loaded data.	read	-	-	oa:system:getAutoloadData
oa:capacityAnalysis:listResultMonitor-Data	Grants permission to obtain the monitoring data from KEA risk analysis results.	read	-	-	-
oa:applications:getSummary	Grants permission to obtain the architecture diagram summary.	read	-	-	-

Action	Description	Access Level	Resource Type (Must Specify All Using "*")	Condition Key	Alias
oa:applications:listCapacityAnalysis-SupportedServices	Grants permission to obtain supported services from the capacity optimization dashboard.	read	-	-	-
oa:applications:listCapacityAnalysis-Results	Grants permission to obtain the analysis results from the capacity optimization dashboard.	read	-	-	-
oa:applications:startAutomaticDrawA-nalysis	Grants permission to create an automatic drawing analysis task.	write	-	-	-
oa:applications:getAutomaticDrawAnalysisProgress	Grants permission to obtain the progress of an automatic drawing analysis task.	read	-	-	-
oa:applications:getAutomaticDrawAnalysisResult	Grants permission to obtain the result of an automatic drawing analysis task.	read	-	-	-
oa:applications:getVpcFlowLogsDock-ingStatus	Grants permission to obtain the interconnection status of VPC flow logs.	read	-	-	-
oa::listResourceGroups	Grants permission to obtain the resource group list.	read	-	-	oa:resourceGroups:list

Action	Description	Access Level	Resource Type (Must Specify All Using "*")	Condition Key	Alias
oa::getResourceGroups	Grants permission to obtain resource group details.	read	-	-	oa:resourceGroups:get
oa::updateResourceGroups	Grants permission to modify a resource group.	write	-	-	oa:resourceGroups:update
oa::deleteResourceGroups	Grants permission to delete a resource group.	write	-	-	oa:resourceGroups:delete
oa::listResourceGroupsRegions	Grants permission to list the regions that the resource groups belong to.	read	-	-	oa:resourceGroups:listRegions
oa::listResourceGroupsResources	Grants permission to list the resources in a resource group.	read	-	-	oa:resourceGroups:listResources
oa::listEnterpriseProjectResources	Grants permission to list the resources of an enterprise project.	read	-	-	oa:resourceGroups:listEnterpriseProjectResources
oa::listServiceMetrics	Grants permission to list metrics of a cloud service.	read	-	-	oa:system:listServiceMetrics
oa::listAlarmMetrics	Grants permission to list alarm metrics.	read	-	-	oa:system:listAlarmMetrics
oa:applications:listServiceResources	Grants permission to list cloud service resources of an architecture design.	read	-	-	-

Action	Description	Access Level	Resource Type (Must Specify All Using "*")	Condition Key	Alias
oa:applications:saveResourceGroup	Grants permission to save resource groups of an architecture design.	write	-	-	-
oa::listResourceTypes	Grants permission to list resource types.	read	-	-	oa:system:listResourceTypes
oa::listAllResourceGroups	Grants permission to list all resource groups.	read	-	-	oa:resourceGroups:listAll
oa:applications:downloadResourceTemplate	Grants permission to download the resource import template for an architecture design.	read	-	-	oa:applications:downloadResourceTemplate
oa:applications:importResources	Grants permission to import resources for an architecture design.	read	-	-	-
oa:applications:getResourcesImportResult	Grants permission to obtain the resource import results of an architecture design.	read	-	-	-
oa:applications:saveResourceGroups-Batch	Grants permission to save resource groups in an architecture design in batches.	write	-	-	-

Action	Description	Access Level	Resource Type (Must Specify All Using "*")	Condition Key	Alias
oa:applications:getBatchSaveResourceGroupsResult	Grants permission to obtain the results for batch saving resource groups in an architecture design.	read	-	-	-
oa::downloadResourceTemplate	Grants permission to download the resource import template for a resource group.	read	-	-	oa:resourceGroups:downloadResourceTemplate
oa::importResourceGroups	Grants permission to import resources to a resource group.	read	-	-	oa:resourceGroups:importResources
oa::getResourcesGroupsImportResult	Grants permission to obtain the resource import results of a resource group.	read	-	-	oa:resourceGroups:getResourcesImportResult
oa:applications:startServiceRecommendAnalysis	Grants permission to start service recommendation analysis.	write	-	-	-
oa:applications:getServiceRecommendAnalysisResult	Grants permission to obtain the service recommendation analysis results.	read	-	-	-
oa:applications:listAttachedResources	Grants permission to list resources associated with an architecture diagram.	read	-	-	-

Action	Description	Access Level	Resource Type (Must Specify All Using "*")	Condition Key	Alias
oa:applications:listNodeAttachedResources	Grants permission to list resources corresponding to a diagram element.	read	-	-	-
oa:applications:downloadAttachedResources	Grants the permission to export resources from an architecture diagram.	write	-	-	-
oa::getAutoloadConfigs	Grants permission to obtain system auto-loaded configurations	read	-	-	oa:system:getAutoloadConfigs
oa::listRiskItemsCheckReportsV4	Grants permission to obtain risk check reports.	read	-	-	oa:riskItemsCheck:listReportsV4
oa::getResources	Grants permission to obtain auto-access resource data.	read	-	-	oa:system:getAutoloadResources
oa:capacityAnalysis:getListMetrics	Grants permission to obtain metrics of risky resources for capacity optimization.	read	-	-	-
oa:capacityAnalysis:getListMonitor	Grants permission to obtain the monitoring data of risky resources for capacity optimization.	read	-	-	-
oa::getTask	Grants permission to query job progress.	read	-	-	-

Action	Description	Access Level	Resource Type (Must Specify All Using "*")	Condition Key	Alias
oa:ignoredResourceConfig:create	Grants permission to add a resource exclusion rule.	write	-	-	-
oa:ignoredResourceConfig:delete	Grants permission to delete a resource exclusion rule.	write	-	-	-
oa:ignoredResourceConfig:update	Grants permission to update a resource exclusion rule.	write	-	-	-
oa:ignoredResourceConfig:enable	Grants permission to enable or disable a resource exclusion rule.	write	-	-	-
oa:ignoredResourceConfig:get	Grants permission to query details about resources in a resource exclusion rule.	read	-	-	-
oa:ignoredResourceConfig:list	Grants permission to query details about a resource exclusion rule.	read	-	-	-
oa:ignoredResourceConfig:listEnterpriseProjects	Grants permission to list enterprise projects in a resource exclusion rule.	read	-	-	-

Resources

OA does not support resource-level authorization. To allow access to OA, use a wildcard (*) in the Resource element of the identity policy, indicating that the policy will be applied to all resources.

Conditions

OA does not support service-specific condition keys in identity policies. It can only use global condition keys applicable to all services. For details, see **Global Condition Keys**.

