

Optimization Advisor OA

Service Overview

Issue 01
Date 2026-02-26



Copyright © Huawei Technologies Co., Ltd. 2026. All rights reserved.

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

Trademarks and Permissions



HUAWEI 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 Service Overview.....	1
2 OA Features.....	3
3 Billing and Constraints.....	4
4 Security and Permissions.....	5
4.1 Identity Authentication and Access Control.....	5
4.2 Permissions.....	5
5 Concepts.....	23

1 Service Overview

OA is an architecture optimization platform that helps you quickly identify and fix potential risks of your cloud resource deployment architectures. Bolstered by Huawei's IT best practice experience and a rich repository of public cloud solutions in the industry, OA provides capabilities such as risk check, capacity analysis, and architecture design. With OA, you can intuitively view your cloud resource deployment status, identify resource risks, and optimize your services based on suggestions provided by OA to improve your cloud service stability.

OA Benefits

- **Self-service requesting**
You can enable OA by yourself. Log in to the Huawei Cloud console and choose **Products > Management & Governance > Optimization Advisor (OA)**. On the displayed page, click **Try Now** to enable OA. Then you can check and analyze your cloud resources with ease and view the check results.
- **Real-time and reliable monitoring**
OA monitors and samples your cloud resource data in real time, providing timely and up-to-date insights in the check results.
- **Visualized check results**
OA provides you with various charts and tables to help you visualize and monitor data in different scenarios.
- **Custom settings**
You can enable or disable check items as needed. You can also configure custom thresholds for performance and cost checks.

Scenarios

- **Prevention and strengthening**
You can learn about the running statuses of cloud resources in real time at a low cost, identify risks in advance, and take preventive and hardening measures to ensure service continuity.
- **Key event assurance**
Before major online events such as regular sales and holiday promotions, you can use OA to identify risks in advance. This helps you ensure successful event execution and protect your brand value.

- **Architecture adjustment**

You can adjust the resource deployment architectures and verify the rationality and security of the architectures to ensure that they meet your service needs.

2 OA Features

Main features of OA:

- **Risk check:** OA scans your cloud resources for risks in terms of performance efficiency, reliability, security, cost optimization (available only for those who have purchased Business, Enterprise, or Enterprise On-Ramp support plan), and service quotas, and provides optimization recommendations. You can download the check results to your local PC for analysis.
- **Auto check:** You can enable auto checks on the risk check page and configure an execution interval and time to perform automatic checks on schedule. You can also send the check results to your email address.
- **User-defined check rules:** You can disable or enable a check item, and modify thresholds in check rules for performance and cost check.
- **Historical check records:** You can view the check records and results of your resources within the last one month.
- **Architecture design:** You can draw your service architecture and deployment architecture of cloud resources with ease using architecture design. With only a few clicks, you can represent the capacity risk monitoring data, associated resources, and all links in your architectures.
- **Capacity optimization:** OA analyzes your cloud resource usage and identifies cloud service or resource capacity risks, such as insufficient CPU, memory, and hard disk resources.
- **Resource groups:** You can create resource groups to centrally manage different types of resources, such as ECSs, EVS disks, EIPs, bandwidths, and databases by group, and identify capacity risks by service, improving O&M efficiency.
- **Monthly service reports:** You can view the usage and changes of all your resources within the last one month and export a monthly report to your local PC. Note: This feature is being improved.

3 Billing and Constraints

Billing

All users can use the basic OA functions. Capacity optimization and cost optimization are available only for users who have enabled the Business, Enterprise, or Enterprise On-Ramp support plan.

Constraints

You can check your cloud resources in limited scenarios, but cannot identify all risks of your cloud resources.

4 Security and Permissions

[4.1 Identity Authentication and Access Control](#)

[4.2 Permissions](#)

4.1 Identity Authentication and Access Control

Basic Access Permissions

Basic functions of OA are available to all users.

- Account administrators can use OA directly.
- IAM users can access and use OA only after being authorized by their account administrators in IAM.

Advanced Features

To use advanced features such as capacity optimization and cost optimization, enable the Business, Enterprise, or Enterprise On-Ramp support plan for your account first.

4.2 Permissions

If you need to assign different permissions to employees in your enterprise to access your Optimization Advisor (OA) resources purchased on Huawei Cloud, Identity and Access Management (IAM) is a good choice for fine-grained permissions management. IAM provides identity authentication, fine-grained permissions management, and access control. It helps you secure access to your Huawei Cloud resources. If your HUAWEI ID does not require IAM for permissions management, you can skip this section.

IAM is a free service. You only pay for the resources in your account.

With IAM, you can control access to specific Huawei Cloud resources. For example, some software developers in your enterprise need to use OA resources but are not allowed to perform any high-risk operations, such as deleting OA resources. To

this end, you can create IAM users for software developers and grant them only the permissions to use OA but not permission to delete it.

IAM supports role/policy-based authorization and identity policy-based authorization.

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

Table 4-1 Differences between role/policy-based and identity policy-based authorization

Authorization Model	Core Relationship	Permissions	Authorization Method	Scenario
Role/Policy	User-permission-authorization scope	<ul style="list-style-type: none"> • 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.
Identity policy	User-policy	<ul style="list-style-type: none"> • System-defined identity policies • Custom identity policies 	<ul style="list-style-type: none"> • 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. For details about system-defined permissions, see [Role/Policy-based Authorization](#) and [Identity Policy-based Authorization](#).

For more information about IAM, see [IAM Service Overview](#).

Role/Policy-based Authorization

OA supports role/policy-based authorization. New IAM users do not have any permissions assigned by default. You need to first add them to one or more groups and then attach policies or roles to these groups. The users then inherit permissions from the groups and can perform specified operations on cloud services based on the permissions they have been assigned.

OA is a global service deployed for all regions. When the authorization scope is set to **Global services**, you have the permission to access OA resources in all regions.

Table 4-2 lists all system-defined permissions for OA. System-defined policies in role/policy-based authorization are not interoperable with those in identity policy-based authorization.

Table 4-2 System-defined permissions for OA

Role/Policy Name	Description	Type	Dependencies
OA FullAccessPolicy	Has all permissions of OA.	System-defined policies	None
OA AdvancedOperationsPolicy	Has the permissions to perform advanced operations using OA, such as performing availability check. With this policy, the cross-account availability check function is available.	System-defined policies	None
OA CommonOperationsPolicy	Has the permissions to perform regular operations using OA, such as performing availability check. The cross-account availability check function is unavailable for users with this policy.	System-defined policies	None
OA ReadOnlyAccessPolicy	Read-only permissions for OA. Users who are assigned this policy can only view check results and resource groups, but cannot create or execute tasks.	System-defined policies	None

Table 4-3 lists the common operations supported by system-defined policies for OA.

Table 4-3 Common operations supported by system-defined permissions

Function	Operation	OA FullAccessPolicy	OA AdvancedOperationsPolicy	OA CommonOperationsPolicy	OA ReadOnlyAccessPolicy
Risk check overview	View the risk check result overview.	Supported	Supported	Supported	Supported
	Enable or disable automatic check.	Supported	Supported	Supported	Not supported
	View a notification topic.	Supported	Supported	Supported	Supported
	Select accounts.	Supported	Supported	Not supported	Not supported
	Execute check tasks.	Supported	Supported	Supported	Not supported
	Download the risk check result report.	Supported	Supported	Supported	Supported
Risk check dimensions	View risk check dimensions.	Supported	Supported	Supported	Supported
	View the check result details of a single check item.	Supported	Supported	Supported	Supported
	Perform a check for a single item.	Supported	Supported	Supported	Not supported
	Download the check report of a single check item.	Supported	Supported	Supported	Supported
Architecture design	View the architecture diagrams.	Supported	Supported	Supported	Supported

Function	Operation	OA FullAccessPolicy	OA AdvancedOperationsPolicy	OA CommonOperationsPolicy	OA ReadOnlyAccessPolicy
	View architecture diagrams in the recycle bin.	Supported	Supported	Supported	Supported
	View details about the architecture diagrams in the recycle bin.	Supported	Supported	Supported	Supported
	Restore architecture diagrams from the recycle bin.	Supported	Supported	Supported	Not supported
	Delete architecture diagrams from the recycle bin.	Supported	Supported	Supported	Not supported
	Create an architecture diagram.	Supported	Supported	Supported	Not supported
	Rename an architecture diagram.	Supported	Supported	Supported	Not supported
	Export an architecture diagram.	Supported	Supported	Supported	Supported
	Copy an architecture diagram.	Supported	Supported	Supported	Not supported
	Delete an architecture diagram.	Supported	Supported	Supported	Not supported
	Enable capacity risk monitoring.	Supported	Supported	Supported	Not supported

Function	Operation	OA FullAccessPolicy	OA AdvancedOperationsPolicy	OA CommonOperationsPolicy	OA ReadOnlyAccessPolicy
	View details of an architecture diagram.	Supported	Supported	Supported	Supported
	Edit an architecture diagram.	Supported	Supported	Supported	Not supported
	View the historical editing records of an architecture diagram.	Supported	Supported	Supported	Supported
	View the historical editing details of an architecture diagram.	Supported	Supported	Supported	Supported
	Restore a historical architecture diagram.	Supported	Supported	Supported	Not supported
	Delete the historical editing records of an architecture diagram.	Supported	Supported	Supported	Not supported
	View all links of a diagram element.	Supported	Supported	Supported	Supported
	View the list of selected resources.	Supported	Supported	Supported	Supported
	Export selected resources.	Supported	Supported	Supported	Supported

Function	Operation	OA FullAccessPolicy	OA AdvancedOperationsPolicy	OA CommonOperationsPolicy	OA ReadOnlyAccessPolicy
	Associate resources to a diagram element.	Supported	Supported	Supported	Not supported
Capacity optimization	View the summary of capacity optimization analysis results.	Supported	Supported	Supported	Supported
	View the details of capacity optimization analysis results.	Supported	Supported	Supported	Supported
	Delete capacity optimization analysis results.	Supported	Supported	Supported	Not supported
	View monitoring details of a capacity optimization analysis result.	Supported	Supported	Supported	Supported
	Perform re-identification.	Supported	Supported	Supported	Not supported
	Stop analysis.	Supported	Supported	Supported	Not supported
	Export the capacity optimization analysis report.	Supported	Supported	Supported	Supported
	Query configurations for capacity optimization analysis.	Supported	Supported	Supported	Supported

Function	Operation	OA FullAccessPolicy	OA AdvancedOperationsPolicy	OA CommonOperationsPolicy	OA ReadOnlyAccessPolicy
	Modify configurations for capacity optimization analysis.	Supported	Supported	Supported	Not supported
	Query the list of capacity optimization analysis reports.	Supported	Supported	Supported	Supported
	Delete a capacity optimization analysis report.	Supported	Supported	Supported	Not supported
Resource groups	View resource groups.	Supported	Supported	Supported	Supported
	View resource group details.	Supported	Supported	Supported	Supported
	Modify a resource group.	Supported	Supported	Supported	Not supported
	Delete a resource group.	Supported	Supported	Supported	Not supported
	Add a resource group.	Supported	Supported	Supported	Not supported
	View the resource list.	Supported	Supported	Supported	Supported
Monthly service reports	View the monthly report list.	Supported	Supported	Supported	Supported
	View monthly report details.	Supported	Supported	Supported	Supported
	Export a monthly report.	Supported	Supported	Supported	Supported

Function	Operation	OA FullAccessPolicy	OA AdvancedOperationsPolicy	OA CommonOperationsPolicy	OA ReadOnlyAccessPolicy
Risk check history	View risk check reports.	Supported	Supported	Supported	Supported
	View risk check result details.	Supported	Supported	Supported	Supported
	Export a risk check report.	Supported	Supported	Supported	Supported
Custom rules	View the check item list.	Supported	Supported	Supported	Supported
	Enable check items.	Supported	Supported	Supported	Not supported
	Disable check items.	Supported	Supported	Supported	Not supported
	Restore initial configurations.	Supported	Supported	Supported	Not supported
	Customize configurations.	Supported	Supported	Supported	Not supported
	Add a resource exclusion rule.	Supported	Not supported	Supported	Not supported
	Delete a resource exclusion rule.	Supported	Not supported	Supported	Not supported
	Update a resource exclusion rule.	Supported	Not supported	Supported	Not supported
	Enable or disable a resource exclusion rule.	Supported	Not supported	Supported	Not supported
	Query details about a resource exclusion rule.	Supported	Not supported	Not supported	Supported

Function	Operation	OA FullAccessPolicy	OA AdvancedOperationsPolicy	OA CommonOperationsPolicy	OA ReadOnlyAccessPolicy
	Query details about resources in a resource exclusion rule.	Supported	Not supported	Not supported	Supported
	List enterprise projects in a resource exclusion rule.	Supported	Not supported	Not supported	Supported
Authorization	View the user authorization list.	Supported	Supported	Supported	Supported
	Disable or enable authorization.	Supported	Not supported	Not supported	Not supported
	Disable services.	Supported	Not supported	Not supported	Not supported

Identity Policy-based Authorization

OA supports identity policy-based authorization. [Table 4-4](#) lists all the system-defined identity policies for OA. System-defined policies in identity policy-based authorization are not interoperable with those in role/policy-based authorization.

Table 4-4 System-defined identity policies for OA

Identity Policy Name	Description	Type
OA FullAccessPolicy	Has all permissions of OA.	System-defined identity policies
OA AdvancedOperations-Policy	Has the permissions to perform advanced operations using OA, such as performing availability check. With this policy, the cross-account availability check function is available.	System-defined identity policies

Identity Policy Name	Description	Type
OA CommonOperationsPolicy	Has the permissions to perform regular operations using OA, such as performing availability check. The cross-account availability check function is unavailable for users with this policy.	System-defined identity policies
OA ReadOnlyAccessPolicy	Read-only permissions for OA. Users who are assigned this policy can only view check results and resource groups, but cannot create or execute tasks.	System-defined identity policies

Table 4-5 lists the common operations supported by system-defined identity policies for OA.

Table 4-5 Common operations supported by system-defined policies

Function	Operation	OA FullAccessPolicy	OA AdvancedOperationsPolicy	OA CommonOperationsPolicy	OA ReadOnlyAccessPolicy
Risk check overview	View the risk check result overview.	Supported	Supported	Supported	Supported
	Enable or disable automatic check.	Supported	Supported	Supported	Not supported
	View a notification topic.	Supported	Supported	Supported	Supported
	Select accounts.	Supported	Supported	Not supported	Not supported
	Execute check tasks.	Supported	Supported	Supported	Not supported
	Download the risk check result report.	Supported	Supported	Supported	Supported

Function	Operation	OA FullAccessPolicy	OA AdvancedOperationsPolicy	OA CommonOperationsPolicy	OA ReadOnlyAccessPolicy
Risk check dimensions	View risk check dimensions.	Supported	Supported	Supported	Supported
	View the check result details of a single check item.	Supported	Supported	Supported	Supported
	Perform a check for a single item.	Supported	Supported	Supported	Not supported
	Download the check report of a single check item.	Supported	Supported	Supported	Supported
Architecture design	View the architecture diagrams.	Supported	Supported	Supported	Supported
	View architecture diagrams in the recycle bin.	Supported	Supported	Supported	Supported
	View details about the architecture diagrams in the recycle bin.	Supported	Supported	Supported	Supported
	Restore architecture diagrams from the recycle bin.	Supported	Supported	Supported	Not supported
	Delete architecture diagrams from the recycle bin.	Supported	Supported	Supported	Not supported

Function	Operation	OA FullAccessPolicy	OA AdvancedOperationsPolicy	OA CommonOperationsPolicy	OA ReadOnlyAccessPolicy
	Create an architecture diagram.	Supported	Supported	Supported	Not supported
	Rename an architecture diagram.	Supported	Supported	Supported	Not supported
	Export an architecture diagram.	Supported	Supported	Supported	Supported
	Copy an architecture diagram.	Supported	Supported	Supported	Not supported
	Delete an architecture diagram.	Supported	Supported	Supported	Not supported
	Enable capacity risk monitoring.	Supported	Supported	Supported	Not supported
	View details of an architecture diagram.	Supported	Supported	Supported	Supported
	Edit an architecture diagram.	Supported	Supported	Supported	Not supported
	View the historical editing records of an architecture diagram.	Supported	Supported	Supported	Supported
	View the historical editing details of an architecture diagram.	Supported	Supported	Supported	Supported

Function	Operation	OA FullAccessPolicy	OA AdvancedOperationsPolicy	OA CommonOperationsPolicy	OA ReadOnlyAccessPolicy
	Restore a historical architecture diagram.	Supported	Supported	Supported	Not supported
	Delete the historical editing records of an architecture diagram.	Supported	Supported	Supported	Not supported
	View all links of a diagram element.	Supported	Supported	Supported	Supported
	View the list of selected resources.	Supported	Supported	Supported	Supported
	Export selected resources.	Supported	Supported	Supported	Supported
	Associate resources to a diagram element.	Supported	Supported	Supported	Not supported
Capacity optimization	View the summary of capacity optimization analysis results.	Supported	Supported	Supported	Supported
	View the details of capacity optimization analysis results.	Supported	Supported	Supported	Supported
	Delete capacity optimization analysis results.	Supported	Supported	Supported	Not supported

Function	Operation	OA FullAccessPolicy	OA AdvancedOperationsPolicy	OA CommonOperationsPolicy	OA ReadOnlyAccessPolicy
	View monitoring details of a capacity optimization analysis result.	Supported	Supported	Supported	Supported
	Perform re-identification.	Supported	Supported	Supported	Not supported
	Stop analysis.	Supported	Supported	Supported	Not supported
	Export the capacity optimization analysis report.	Supported	Supported	Supported	Supported
	Query configurations for capacity optimization analysis.	Supported	Supported	Supported	Supported
	Modify configurations for capacity optimization analysis.	Supported	Supported	Supported	Not supported
	Query the list of capacity optimization analysis reports.	Supported	Supported	Supported	Supported
	Delete a capacity optimization analysis report.	Supported	Supported	Supported	Not supported

Function	Operation	OA FullAccessPolicy	OA AdvancedOperationsPolicy	OA CommonOperationsPolicy	OA ReadOnlyAccessPolicy
Resource groups	View resource groups.	Supported	Supported	Supported	Supported
	View resource group details.	Supported	Supported	Supported	Supported
	Modify a resource group.	Supported	Supported	Supported	Not supported
	Delete a resource group.	Supported	Supported	Supported	Not supported
	Add a resource group.	Supported	Supported	Supported	Not supported
	View the resource list.	Supported	Supported	Supported	Supported
Monthly service reports	View the monthly report list.	Supported	Supported	Supported	Supported
	View monthly report details.	Supported	Supported	Supported	Supported
	Export a monthly report.	Supported	Supported	Supported	Supported
Risk check history	View risk check reports.	Supported	Supported	Supported	Supported
	View risk check result details.	Supported	Supported	Supported	Supported
	Export a risk check report.	Supported	Supported	Supported	Supported

Function	Operation	OA FullAccessPolicy	OA AdvancedOperationsPolicy	OA CommonOperationsPolicy	OA ReadOnlyAccessPolicy
Custom rules	View the check item list.	Supported	Supported	Supported	Supported
	Enable check items.	Supported	Supported	Supported	Not supported
	Disable check items.	Supported	Supported	Supported	Not supported
	Restore initial configurations.	Supported	Supported	Supported	Not supported
	Customize configurations.	Supported	Supported	Supported	Not supported
	Add a resource exclusion rule.	Supported	Not supported	Supported	Not supported
	Delete a resource exclusion rule.	Supported	Not supported	Supported	Not supported
	Update a resource exclusion rule.	Supported	Not supported	Supported	Not supported
	Enable or disable a resource exclusion rule.	Supported	Not supported	Supported	Not supported
	Query details about a resource exclusion rule.	Supported	Not supported	Not supported	Supported

Function	Operation	OA FullAccessPolicy	OA AdvancedOperationsPolicy	OA CommonOperationsPolicy	OA ReadOnlyAccessPolicy
	Query details about resources in a resource exclusion rule.	Supported	Not supported	Not supported	Supported
	List enterprise projects in a resource exclusion rule.	Supported	Not supported	Not supported	Supported
Authorization	View the user authorization list.	Supported	Supported	Supported	Supported
	Disable or enable authorization.	Supported	Not supported	Not supported	Not supported
	Disable services.	Supported	Not supported	Not supported	Not supported

Helpful Links

- [IAM Service Overview](#)
- [Authorization Using IAM](#)
- [Identity Policy-based Authorization](#)

5 Concepts

- **Risk Check Dimensions**

There are two dimensions: risk dimension and product dimension. The risk dimension consists of five sub-dimensions: performance efficiency, reliability, security, cost optimization, and service quota. The check results are classified into risky, secure, N/A, and warning. In terms of service loss, risky check results are further classified into high-risk and low-risk.

 **NOTE**

Original medium risks now merge into low risks.

- **High-risk:** Risks of this level can cause service system damage, and major incidents such as service interruption, asset damage, and data loss.
- **Low-risk:** Risks of this level require your attention.

- **Service Quota**

OA uses this feature to check whether your account is about to reach the service quota limit and remind you to expand your service quotas as soon as possible. Otherwise, resources cannot be created during scale-out, which affects system availability.

- **Risk Identification**

OA identifies capacity risks of your services or resources and predicts possible capacity risks based on the pressure coefficient.

- **Aggregation Period**

In an aggregation period, Cloud Eye calculates the average, maximum, minimum, sum, or variance value based on sample raw data reported by each cloud service.

- **Capacity Reports**

After risk identification is complete, a capacity report is automatically generated for you to download.

- **Pressure Coefficient**

Pressure coefficient indicates the pressure multiplier of a resource in a special scenario or period.

- **TAM Drawing**

After a Technical Account Manager (TAM) draws an architecture diagram using the architecture design feature of the management tool module and

synchronizes the architecture diagram to the architecture design of OA. Architectures labeled **Expert Drawing** can only be viewed but cannot be edited, as shown in [Figure 1](#).

Figure 5-1 TAM drawing

