Optimization Advisor OA

Product Overview

Issue 1.2

Date 2025-09-05

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 Service Statement

1.1 Service Content

Optimization Advisor (OA) is a cloud service that helps you configure resources by following best practices. OA is built on Huawei's IT expertise. It leverages industry-leading public cloud solutions to help you analyze on-cloud resource deployment, including service performance, security, reliability, costs, and service quotas. It identifies risks and provides recommendations to improve cloud service stability.

1.2 Cooperation You Need to Provide

You understand and agree to authorize Huawei Cloud OA to analyze your cloud resource data, including resource deployment data, resource configurations, resource O&M data, and resource quotas. Such data is used only for the purpose of providing services and is retained for one month. If you have any questions about the authorization scope, contact Huawei Cloud customer service for assistance.

1.3 Disclaimers

The risky items and optimization recommendations in the check results of OA are for your reference only and may not resolve all your issues. Huawei Cloud does not promise that the OA service is flawless. However, Huawei Cloud promises to continuously improve the service quality and service level of OA. If any defect in the OA service is unavoidable due to technological limitations, it shall not be deemed as a breach of contract by Huawei Cloud, and you need to cooperate with Huawei Cloud to resolve the issue.

2 OA Features

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.

Main features of OA:

- **Risk check**: OA scans your cloud resources for risks in terms of performance, reliability, security, costs (available only for those who have purchased Business or Enterprise support plans), and service baseline, and provides optimization recommendations. You can download the check results to your local PC for analysis.
- **Automatic check**: You can enable automatic 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, or 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 OA Benefits

- **Self-service requesting**

  You can enable OA by yourself. You can log in to the Huawei Cloud console and choose **Products** > **Management & Governance** > **Optimization Advisor (OA)**. On the displayed page, click **Try Now** to go to the OA page. You can check and analyze your cloud resources with ease and view the check results on the page.

- **Real-time and reliable monitoring**

  The check results are based on real-time monitoring and sampling of your cloud resource data, ensuring timely and up-to-date insights.

- **Visualized check results**

  OA provides you with various charts and tables to help you visualize and monitor data across various situations.

- **Custom settings**

  You can enable or disable check items as needed. You can also configure custom thresholds for performance and cost checks.

4 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**

  In scenarios where there are major online activities such as common promotions and promotions on important holidays, you can use OA to identify risks in advance to ensure the smooth completion of the activities 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.

5 Billing

All users can use the basic OA functions. Capacity optimization and cost optimization can be used only after the Business or Enterprise support plan is enabled.

6 Constraints and Restrictions

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

7 Security

7.1 Shared Responsibilities

Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system for different regions and industries based on Huawei's unique software and hardware advantages, laws, regulations, industry standards, and security ecosystem.

Figure 1 illustrates the responsibilities shared by Huawei Cloud and you.

- **Huawei Cloud**: Ensure the security of the cloud services it provides. Huawei Cloud's security responsibilities include ensuring the security of our IaaS, PaaS, and SaaS services, as well as the physical environments of the Huawei Cloud data centers where our IaaS, PaaS, and SaaS services operate. Huawei Cloud is responsible not only for the security functions and performance of its infrastructure, cloud services, and technologies, but also for the overall cloud operational security and, in a broader sense, the security compliance of its infrastructure and services.
- **Tenants**: Use the cloud securely. Tenants of Huawei Cloud are responsible for the secure and effective management of the tenant-customized configurations of cloud services including IaaS, PaaS, and SaaS. This includes but is not limited to virtual networks, the OS of virtual machine hosts and guests, virtual firewalls, API Gateway, advanced security services, all types of cloud services, tenant data, identity accounts, and key management.

7.2 Identity Authentication and Access Control

All users can use the basic OA functions. Capacity optimization and cost optimization can be used only after the Business or Enterprise support plan is enabled.

8 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, and N/A. In terms of service loss, risky check results are further classified into high-risk, medium-risk, and low-risk.

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

- **Service Baselines**

  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 8-1 TAM drawing

9 Permissions

If you need to grant your enterprise personnel permission to access your OA resources, use Identity and Access Management (IAM). IAM provides identity authentication, fine-grained permissions management, and access control. IAM 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, if you want some software developers in your enterprise to use OA resources but do not want them to delete OA resources or perform any other high-risk operations, you can create IAM users and grant permission to use OA resources but not permission to delete them.

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

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

Table 9-1 Differences between role/policy-based and identity policy-based authorization

Authorization Model	Core Relationship	Permissions	Authorization Method	Scenario
Role/Policy	User-permission-authorization scope	• 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	• 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. 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 9-2 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 9-2 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, cross-account availability check is available.	System-defined policies	None
OA CommonOperationsPolicy	Has the permissions to perform regular operations using OA, such as performing availability check. Cross-account availability check 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 9-3 lists the common operations supported by system-defined policies for OA.

Table 9-3 Common operations supported by system-defined permissions

Function	Operation	OA FullAccessPolicy	OA AdvancedOperationsPolicy	OA CommonOperationsPolicy	OA ReadOnlyAccessPolicy
Risk check overview	Viewing the risk check result overview	Supported	Supported	Supported	Supported
	Enabling or disabling automatic check	Supported	Supported	Supported	Not supported
	Viewing a notification topic	Supported	Supported	Supported	Supported
	Selecting accounts	Supported	Supported	Not supported	Not supported
	Performing a check	Supported	Supported	Supported	Not supported
	Downloading the risk check report	Supported	Supported	Supported	Supported
Risk check dimensions	Viewing risk check dimensions	Supported	Supported	Supported	Supported
	Viewing the check result details of a single check Item	Supported	Supported	Supported	Supported
	Performing a check for a single item.	Supported	Supported	Supported	Not supported
	Downloading the check report of a single check item.	Supported	Supported	Supported	Supported
Architecture design	Viewing the architecture list	Supported	Supported	Supported	Supported

Function	Operation	OA FullAccessPolicy	OA AdvancedOperationsPolicy	OA CommonOperationsPolicy	OA ReadOnlyAccessPolicy
	Viewing architectures in the recycle bin	Supported	Supported	Supported	Supported
	Viewing details about the architectures in the recycle bin	Supported	Supported	Supported	Supported
	Restoring architectures from the recycle bin	Supported	Supported	Supported	Not supported
	Deleting architectures from the recycle bin	Supported	Supported	Supported	Not supported
	Creating an architecture	Supported	Supported	Supported	Not supported
	Renaming an architecture	Supported	Supported	Supported	Not supported
	Exporting an architecture	Supported	Supported	Supported	Supported
	Copying an architecture	Supported	Supported	Supported	Not supported
	Deleting an architecture	Supported	Supported	Supported	Not supported
	Enabling capacity risk monitoring	Supported	Supported	Supported	Not supported
	Viewing details of an architecture	Supported	Supported	Supported	Supported
	Editing an architecture	Supported	Supported	Supported	Not supported

Function	Operation	OA FullAccessPolicy	OA AdvancedOperationsPolicy	OA CommonOperationsPolicy	OA ReadOnlyAccessPolicy
	Viewing the historical editing records of an architecture	Supported	Supported	Supported	Supported
	Viewing the historical editing details of an architecture	Supported	Supported	Supported	Supported
	Restoring a historical architecture	Supported	Supported	Supported	Not supported
	Deleting the historical records of an architecture	Supported	Supported	Supported	Not supported
	Viewing all links of a diagram element	Supported	Supported	Supported	Supported
	Viewing selected resources	Supported	Supported	Supported	Supported
	Exporting selected resources	Supported	Supported	Supported	Supported
	Associating resources to a diagram element	Supported	Supported	Supported	Not supported
Capacity optimization	Viewing the summary of capacity optimization analysis results	Supported	Supported	Supported	Supported

Function	Operation	OA FullAccessPolicy	OA AdvancedOperationsPolicy	OA CommonOperationsPolicy	OA ReadOnlyAccessPolicy
	Viewing the details of capacity optimization analysis results	Supported	Supported	Supported	Supported
	Deleting capacity optimization analysis results	Supported	Supported	Supported	Not supported
	Viewing monitoring details of a capacity optimization analysis result	Supported	Supported	Supported	Supported
	Performing re-identification	Supported	Supported	Supported	Not supported
	Stopping analysis	Supported	Supported	Supported	Not supported
	Exporting a capacity optimization analysis report	Supported	Supported	Supported	Supported
	Querying capacity optimization analysis settings	Supported	Supported	Supported	Supported
	Modifying capacity optimization analysis settings	Supported	Supported	Supported	Not supported

Function	Operation	OA FullAccessPolicy	OA AdvancedOperationsPolicy	OA CommonOperationsPolicy	OA ReadOnlyAccessPolicy
	Querying the list of capacity optimization analysis reports	Supported	Supported	Supported	Supported
	Deleting a capacity optimization analysis report	Supported	Supported	Supported	Not supported
Resource groups	Viewing resource groups	Supported	Supported	Supported	Supported
	Viewing resource group details	Supported	Supported	Supported	Supported
	Modifying a resource group	Supported	Supported	Supported	Not supported
	Deleting a resource group	Supported	Supported	Supported	Not supported
	Adding a resource group	Supported	Supported	Supported	Not supported
	Viewing the resource list	Supported	Supported	Supported	Supported
Monthly service reports	Viewing the monthly report list	Supported	Supported	Supported	Supported
	Viewing monthly report details	Supported	Supported	Supported	Supported
	Exporting a monthly report	Supported	Supported	Supported	Supported

Function	Operation	OA FullAccessPolicy	OA AdvancedOperationsPolicy	OA CommonOperationsPolicy	OA ReadOnlyAccessPolicy
Risk check history	Viewing risk check reports	Supported	Supported	Supported	Supported
	Viewing risk check result details	Supported	Supported	Supported	Supported
	Exporting a risk check report	Supported	Supported	Supported	Supported
Custom rules	Viewing the check item list	Supported	Supported	Supported	Supported
	Enabling check items	Supported	Supported	Supported	Not supported
	Disabling check items	Supported	Supported	Supported	Not supported
	Initializing configurations	Supported	Supported	Supported	Not supported
	Customizing configurations	Supported	Supported	Supported	Not supported
Permission authorization	Viewing the user authorization list	Supported	Supported	Supported	Supported
	Enabling or disabling authorization	Supported	Not supported	Not supported	Not supported
	Disabling services	Supported	Not supported	Not supported	Not supported

Identity Policy-based Authorization

OA supports identity policy-based authorization. **Table 9-4** 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 9-4 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, cross-account availability check is available.	System-defined identity policies
OA CommonOperationsPo-licy	Has the permissions to perform regular operations using OA, such as performing availability check. Cross-account availability check is unavailable for users with this policy.	System-defined identity policies
OA ReadOnlyAccessPo-licy	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 9-5 lists the common operations supported by system-defined identity policies for OA.

Table 9-5 Common operations supported by system-defined policies

Function	Operation	OA FullAccessPolicy	OA AdvancedOperationsPolicy	OA CommonOperationsPolicy	OA ReadOnlyAccessPolicy
Risk check overview	Viewing the risk check result overview	Supported	Supported	Supported	Supported
	Enabling or disabling automatic check	Supported	Supported	Supported	Not supported

Function	Operation	OA FullAccessPolicy	OA AdvancedOperationsPolicy	OA CommonOperationsPolicy	OA ReadOnlyAccessPolicy
	Viewing a notification topic	Supported	Supported	Supported	Supported
	Selecting accounts	Supported	Supported	Not supported	Not supported
	Performing a check	Supported	Supported	Supported	Not supported
	Downloading the risk check report	Supported	Supported	Supported	Supported
Risk check dimensions	Viewing risk check dimensions	Supported	Supported	Supported	Supported
	Viewing the check result details of a single check Item	Supported	Supported	Supported	Supported
	Performing a check for a single item.	Supported	Supported	Supported	Not supported
	Downloading the check report of a single check item	Supported	Supported	Supported	Supported
Architecture design	Viewing the architecture list	Supported	Supported	Supported	Supported
	Viewing architectures in the recycle bin	Supported	Supported	Supported	Supported
	Viewing details about the architectures in the recycle bin	Supported	Supported	Supported	Supported

Function	Operation	OA FullAccessPolicy	OA AdvancedOperationsPolicy	OA CommonOperationsPolicy	OA ReadOnlyAccessPolicy
	Restoring architectures from the recycle bin	Supported	Supported	Supported	Not supported
	Deleting architectures from the recycle bin	Supported	Supported	Supported	Not supported
	Creating an architecture	Supported	Supported	Supported	Not supported
	Renaming an architecture	Supported	Supported	Supported	Not supported
	Exporting an architecture	Supported	Supported	Supported	Supported
	Copying an architecture	Supported	Supported	Supported	Not supported
	Deleting an architecture	Supported	Supported	Supported	Not supported
	Enabling capacity risk monitoring	Supported	Supported	Supported	Not supported
	Viewing details of an architecture	Supported	Supported	Supported	Supported
	Editing an architecture	Supported	Supported	Supported	Not supported
	Viewing the historical editing records of an architecture	Supported	Supported	Supported	Supported
	Viewing the historical editing details of an architecture	Supported	Supported	Supported	Supported

Function	Operation	OA FullAccessPolicy	OA AdvancedOperationsPolicy	OA CommonOperationsPolicy	OA ReadOnlyAccessPolicy
	Restoring a historical architecture	Supported	Supported	Supported	Not supported
	Deleting the historical records of an architecture	Supported	Supported	Supported	Not supported
	Viewing all links of a diagram element	Supported	Supported	Supported	Supported
	Viewing selected resources	Supported	Supported	Supported	Supported
	Exporting selected resources	Supported	Supported	Supported	Supported
	Associating resources to a diagram element	Supported	Supported	Supported	Not supported
Capacity optimization	Viewing the summary of capacity optimization analysis results	Supported	Supported	Supported	Supported
	Viewing the details of capacity optimization analysis results	Supported	Supported	Supported	Supported
	Deleting capacity optimization analysis results	Supported	Supported	Supported	Not supported

Function	Operation	OA FullAccessPolicy	OA AdvancedOperationsPolicy	OA CommonOperationsPolicy	OA ReadOnlyAccessPolicy
	Viewing monitoring details of a capacity optimization analysis result	Supported	Supported	Supported	Supported
	Performing re-identification	Supported	Supported	Supported	Not supported
	Stopping analysis	Supported	Supported	Supported	Not supported
	Exporting a capacity optimization analysis report	Supported	Supported	Supported	Supported
	Querying capacity optimization analysis settings	Supported	Supported	Supported	Supported
	Modifying capacity optimization analysis settings	Supported	Supported	Supported	Not supported
	Querying the list of capacity optimization analysis reports	Supported	Supported	Supported	Supported
	Deleting a capacity optimization analysis report	Supported	Supported	Supported	Not supported

Function	Operation	OA FullAccessPolicy	OA AdvancedOperationsPolicy	OA CommonOperationsPolicy	OA ReadOnlyAccessPolicy
Resource groups	Viewing resource groups	Supported	Supported	Supported	Supported
	Viewing resource group details	Supported	Supported	Supported	Supported
	Modifying a resource group	Supported	Supported	Supported	Not supported
	Deleting a resource group	Supported	Supported	Supported	Not supported
	Adding a resource group	Supported	Supported	Supported	Not supported
	Viewing the resource list	Supported	Supported	Supported	Supported
Monthly service reports	Viewing the monthly report list	Supported	Supported	Supported	Supported
	Viewing monthly report details	Supported	Supported	Supported	Supported
	Exporting a monthly report	Supported	Supported	Supported	Supported
Risk check history	Viewing risk check reports	Supported	Supported	Supported	Supported
	Viewing risk check result details	Supported	Supported	Supported	Supported
	Exporting a risk check report	Supported	Supported	Supported	Supported
Custom rules	Viewing the check item list	Supported	Supported	Supported	Supported

Function	Operation	OA FullAccessPolicy	OA AdvancedOperationsPolicy	OA CommonOperationsPolicy	OA ReadOnlyAccessPolicy
	Enabling check items	Supported	Supported	Supported	Not supported
	Disabling check items	Supported	Supported	Supported	Not supported
	Initializing configurations	Supported	Supported	Supported	Not supported
	Customizing configurations	Supported	Supported	Supported	Not supported
Permission authorization	Viewing the user authorization list	Supported	Supported	Supported	Supported
	Enabling or disabling authorization	Supported	Not supported	Not supported	Not supported
	Disabling services	Supported	Not supported	Not supported	Not supported

Helpful Links

- IAM Service Overview
- Authorization Using IAM

