Enterprise Self-Service Management

User Guide

Issue 01

Date 2025-10-30

HUAWEI

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are the property 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 Cloud 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.

Contents

1 Before You Start

Enterprise Self-Service Management (ESM) allows you to manage operations of your Huawei dedicated cloud sites on your own. It also offers a broad set of dashboards you can use to gain comprehensive, multi-dimensional data insights into the status and health of those sites.

NOTE

This document walks you through how to use all ESM functions. You can choose what functions you need. If you have any questions, contact Huawei Cloud customer service .

2 Login and Logout

Scenario

This chapter describes how to log in to and log out of ESM.

Prerequisites

- Google Chrome 57 or later must be available.
- You have obtained the ESM domain name.

Login

Step 1 Open the Google Chrome.

Step 2 Enter the login address in the address box.

URL: **https://***{ESM domain name}*, for example, **https://esm.demo.com**

Step 3 On the login page, enter your account information to log in.

----End

Logout

NOTE

- You can set a session timeout period on the **Security Settings** > **Login Authentication Policy** page of IAM. The default timeout period is 1 hour.
- You will be automatically logged out after being inactive for the specified timeout period.

Step 1 Click the username in the upper right corner of the page.

Step 2 Select **Log Out**.

You will be redirected to the login page.

----End

3 Home Page

On the **Home** page, you can view the ESM wizard, click the buttons under key steps to quickly perform those steps, and quickly access common dashboards, best practices, and documentation.

NOTE

The home page function is not available in specific scenarios. To use the home page, contact technical support.

Prerequisites

You have logged in to ESM as an administrator.

Procedure

Step 1 Choose **Home** from the main menu and view:

- **Wizard**: a step-by-step process that guides you to easily get started using ESM. You can click the buttons under key steps to quickly perform those steps.
- **Common Dashboards**: preset common dashboards. You can click the name of a dashboard to access it or click **More** to view all dashboards on the **Visualization** > **Operations Dashboards** page.
- **Best Practices**: best practices for using dashboards, managing tenants, or performing other tasks
- **Documentation**: documents providing guidance on how to use ESM, function introduction, FAQs, or other ESM-related information

----End

4 Sites

You can manage site information.

Prerequisites

You have logged in to ESM as an administrator.

Procedure

Step 1 Choose **Sites** from the main menu.

Step 2 On the **Sites** page, locate the row that contains a site, click **Modify** in the **Operation** column, and change its name in the **Site Name** column.

After changing the name, you can click **Save** or **Cancel** to save or cancel your change.

----End

5 Organizations

You can manage tenants in organizations, for example, view tenant information, create, pre-deregister, and suspend tenants, reset tenant passwords, and configure quotas for tenants.

NOTE

- The organization function is not available in specific scenarios. To use the home page, contact technical support.
- ESM allows up to 1,000 tenants.

5.1 Viewing Tenant Information

You can view tenant information.

Prerequisites

- You have logged in to ESM as an administrator.
- OBS has been interconnected for exporting tenants or projects.

Procedure

Step 1 Choose **Organization** from the main menu.

Step 2 On the **Tenants** page, perform the tasks described in **Table 5-1** as needed.

Table 5-1 Related tasks

Task	Description	Procedure
Viewing tenant information	You can view names, statuses, and descriptions of tenants in the tenant list.	View basic information about tenants.

Task	Description	Procedure
Exporting tenant information	You can export basic information about tenants to your local system for backup and statistics collection.	Click **Export** and select **Export Tenants**. By default, information about all tenants is exported.
Exporting project information	You can export information about all projects in a tenant.	Click **Export** and select **Export Projects**. By default, information about all projects is exported.

----End

5.2 Creating a Tenant

You can create one or more tenants.

Prerequisites

You have logged in to ESM as an administrator.

Procedure

Step 1 Choose **Organization** from the main menu.

Step 2 On the **Tenants** page, click **Create Tenant**.

Step 3 Set the parameters described in **Table 5-2**.

Table 5-2 Descriptions of key parameters

Parameter	Description
Site	Select a site where the tenant is to be created.
Tenant Name	Enter a tenant name.
Password	Enter a tenant password.
Confirm Password	Enter the password again.
Description	Enter a description of the tenant to be created.

Step 4 Click **OK**.

----End

5.3 Modifying Information About a Tenant

You can modify the description about a created tenant.

Prerequisites

You have logged in to ESM as an administrator.

Procedure

Step 1 Choose **Organization** from the main menu.

Step 2 On the **Tenants** page, locate the row that contains a tenant and click **Modify** in the **Operation** column.

Step 3 Change the tenant description.

NOTE

When configuring a whitelist, you can change a tenant name.

Step 4 Click **Confirm**.

----End

5.4 Resetting a Tenant Password

You can reset a tenant password.

Prerequisites

You have logged in to ESM as an administrator.

Procedure

Step 1 Choose **Organization** from the main menu.

Step 2 On the **Tenants** page, locate the row that contains a tenant and click **Reset Password** in the **Operation** column.

Step 3 Specify **New Password** and **Confirm Password** and click **Confirm**.

----End

5.5 Configuring Quotas

You can configure resource quotas for a tenant to control how many resources are available for the tenant.

NOTE

The professional edition of ESM must be available at your site.

Prerequisites

You have logged in to ESM as an administrator.

Procedure

Step 1 Choose **Organization** from the main menu.

Step 2 On the **Tenants** page, locate the row that contains a tenant and click **Configure Quota** in the **Operation** column. On the displayed page, set filter criteria on the right.

Step 3 Click **Change Allocated Quota**. Locate the row that contains each metric item of each service and enter a number in the **Total Quota** column.

Step 4 Click **Save**. In the displayed dialog box, confirm your quota changes.

Step 5 Click **OK**.

----End

5.6 Pre-deregistering a Tenant

You can pre-deregister a tenant.

NOTE

Pre-deregistration management is enabled by default to quickly restore tenants or to prevent tenants from being deleted by mistake. For details about how to manage pre-deregistrations, see **Managing Pre-deregistrations**.

Prerequisites

You have logged in to ESM as an administrator.

Procedure

Step 1 Choose **Organization** from the main menu.

Step 2 On the **Tenants** page, locate the row that contains the tenant to be pre-deregistered and choose **More** > **Pre-deregister**.

Step 3 In the displayed dialog box, click **OK**.

Step 4 On the **Pre-deregistrations** tab page displayed by default, verify that the status of the tenant changes to **Pre-deregistered**.

----End

5.7 Freezing or Unfreezing a Tenant

You can freeze a tenant to prevent the tenant from buying or operating new cloud services. Existing cloud services and resources of a frozen tenant can still be used.

Prerequisites

You have logged in to ESM as an administrator.

Procedure

Step 1 Choose **Organization** from the main menu.

Step 2 Locate the row that contains the tenant to be frozen or unfrozen and choose **More** > **Freeze** or **More** > **Unfreeze**.

NOTE

Only normal tenants can be frozen.

Only frozen tenants can be unfrozen.

Step 3 Click **OK**.

----End

5.8 Managing Pre-deregistrations

You can manage pre-deregistrations for tenants.

NOTE

Pre-deregistration management is enabled by default to quickly restore tenants or to prevent tenants from being deleted by mistake.

Prerequisites

- You have logged in to ESM as an administrator.
- A tenant has been pre-deregistered.

Procedure

Step 1 Choose **Organization** from the main menu.

Step 2 On the **Tenants** page, click the **Pre-deregistrations** tab.

Step 3 Perform the tasks listed **Table 5-3** as needed.

Table 5-3 Pre-deregistration management tasks

Task	Description	Procedure
Enabling or disabling frozen period configuration	You can choose whether to enable frozen period configuration.	Toggle on **Set Frozen Period**. Toggle off **Set Frozen Period**.

Task	Description	Procedure
Configuring a frozen period	You can configure a frozen period for all tenants except the pre-deregistered ones whose frozen periods have started.	1. Toggle on **Set Frozen Period**. 2. Configure a frozen period before deregistration. 3. Click **OK**.
Restoring a tenant	You can restore a pre-deregistered tenant. **NOTE** Only tenants in the **Frozen** state can be restored.	Locate the row that contains a pre-deregistered tenant and click **Restore** in the **Operation** column. You can also select multiple tenants and click **Restore** on the left above the list to restore them.
Deleting a tenant	You can permanently delete a tenant that is no longer in use. **NOTE** ● Before deleting a tenant, ensure that the site that the tenant belongs to has been connected to Resource Operation Service (ROS). ● Only the tenants whose frozen periods have ended can be deleted. ● After a tenant is permanently deleted, all resource data and configurations of the tenant cannot be restored.	1. Locate the row that contains the tenant and click **Permanently Delete**. 2. In the displayed dialog box, enter *Tenant name*+**DELETE** and click **OK**.

----End

6 Audits

6.1 Operations That Can Be Recorded by CTS

ESM can connect to Cloud Trace Service (CTS) to provide tenants with records of sensitive operations on cloud services. Using the records, tenants can query, audit, and backtrack operations with ease.

Prerequisites

ESM has connected to CTS.

Key Operations That Can Be Audited

Table 6-1 Key operations that can be recorded

Operation Name	Event Name
Update HCSO Information	updateHcso
Create an Account	createHcsoTenantAccount
Update an Account	updateHcsoTenantAccount
Delete an Account	deleteHcsoTenantAccount
Suspend an Account	suspendHcsoTenantAccount
Unsuspend an Account	unsuspendHcsoTenantAccount
Update Tenant Quota	updateHcsoTenantQuota
Restore a Re-registered Tenant	restoreHcsoDomain
Create an HCSO Tenant	createHcsoDomain
Modify an HCSO Tenant	updateHcsoDomain
Delete an HCSO Tenant	deleteHcsoDomain

Operation Name	Event Name
Freeze/Unfreeze a Tenant	suspendHcsoDomain
Pre-deregister a Tenant	deregisterHcsoDomain
Create an HCSO Tenant User	createOwnerUser
Reset User Password	updateOwnerUser
Modify the Frozen Period	updateHcsoFreezingPeriod
Add HCSO Information	esm:CreateCustomerInfo
Modify HCSO Information	updateHcso
Delete HCSO Information	esm:DeleteCustomerInfo
Restore Deleted HCSO Information	esm:RollbackCustomerInfo
Modify the Account for Connecting to HCSO	updateHcsoAccount
Export Information of All Services Interconnected with ROS from HCSO	esm:ListRosService
Add HCSO Services to ROS Interconnection Exceptions	exceptHcsoRosService
Add a Quota Configuration	esm:CreateQuotaMetaInfo
Delete a Quota Configuration	esm:DeleteQuotaMetaInfo
Restore a Deleted Quota Configuration	esm:RollbackQuotaMetaInfo
Export Tenant Information	exportHcsoDomain
Export Project Information	exportHcsoProject
Update Baseline Connection Information of ROS	updateRosConfiguration
Update Cloud Services Connected to ROS	updateRosServices
Add or Delete HCSO Services to or from ROS Interconnection Exceptions	exceptRosService
Import Information of Cloud Services Connected to ROS	importRosServices
Export Information of Cloud Services Connected to ROS	exportRosServices
Enable ESM	openService

Operation Name	Event Name
Delete Tasks of a Tenant	createCleanupDomainJob
Add an SDR Configuration	createMeterApp
Modify an SDR Configuration	updateMeterApp
Delete an SDR Configuration	deleteMeterApp
Retry a Task	retrySdr
Create a Query Task	createQueryJob
Add HCSO Edition Information	createHcsoEdition
Modify HCSO Edition Information	UpdateHcsoEdition
Add Information of Virtual HCSO	createVirtualHcso
Modify Information of Virtual HCSO	UpdateVirtualHcso
Delete Information of Virtual HCSO	DeleteVirtualHcso
Restore Deleted Virtual HCSO Site Details	RollebackVirtualHcso
Export Dashboard Information	DlvDataExport

6.2 Viewing Audit Logs

After you enable CTS, it starts recording operations on ESM. CTS stores operation records for the last seven days.

This section describes how to view the operation records on the CTS console.

Procedure

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner and choose **Management & Governance** > **Cloud Trace Service**.

Step 3 In the navigation pane, choose **Trace List**.

Step 4 On the **Trace List** page, use advanced search to query traces. You can combine one or more filters:

- **Trace Name**: Enter a trace name.

- **Trace ID**: Enter a trace ID.
- **Resource Name**: Enter a resource name. If the cloud resource involved in the trace does not have a resource name or the corresponding API operation does not involve the resource name parameter, leave this field empty.
- **Resource ID**: Enter a resource ID. Leave this field empty if the resource has no resource ID or if resource creation failed.
- **Trace Source**: Select a cloud service from the drop-down list.
- **Resource Type**: Select a resource type from the drop-down list.
- **Operator**: Select one or more operators from the drop-down list.
- **Trace Status**: Select **normal**, **warning**, or **incident**.
  - **normal**: The operation succeeded.
  - **warning**: The operation failed.
  - **incident**: The operation caused a fault that is more serious than the operation failure, for example, causing other faults.
- Time range: Select **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range within the past week.

Step 5 On the **Trace List** page, export and refresh the trace list, and customize the list display settings.

For more information about CTS, see the **Cloud Trace Service User Guide**.

----End

7 Visualizations

Visualizations display comprehensive real-time data to help improve operational agility and efficiency.

Visualization content and data presented to users vary depending on the permissions granted to those users.

7.1 Operations Dashboards

NOTE

All applications that support fuzzy searches allow for searches using wildcards, percent signs (%) and underscores (_). If exact searches are needed, you can add backslashes (\) for escape.

Procedure

Step 1 Choose **Visualization** from the main menu.

The **Operations Dashboards** page is displayed by default. **Table 7-1** describes the operations dashboards.

Step 2 Select a dashboard to access it.

You can click **Export** to export dashboard data to your local system.

NOTE

This export function is available only in the professional edition of ESM.

Table 7-1 Descriptions of visual operations dashboards

Dashboard Name	Description
Resource Summary	The **Resource Summary** dashboard displays the quantities of hardware resources and common cloud resources, cloud resource summary, physical resource usage, cloud resource quota statistics, cloud resource usage trend, virtual resource allocation rates, virtual resource allocation statistics, and virtual resource usage. You can select a time range from the drop-down list in the upper right corner of the dashboard to query physical resource usage, cloud resource usage trend, and virtual resource usage. You can drill down the **Resource Summary** dashboard to access the **Compute Node Capacity Details** and **Storage Node Capacity Details** dashboards. The displayed items in the three dashboards are similar and are described in **Table 7-2**.
Hardware Resources	The **Hardware Resources** dashboard displays the quantity, running statuses, and alarm statuses of hardware resources. This dashboard helps you keep abreast of resource statuses and adjust resource allocation in a timely manner to increase resource utilization and avoid potential risks. **Table 7-4** describes the items displayed in this dashboard.
Hardware Alarms	The **Hardware Alarms** dashboard displays the total number of alarms in the past month, overall alarm statuses, hardware alarm statistics, alarm growth trend in the past month, and uncleared alarms of hardware resources. This dashboard helps you keep abreast of hardware resource alarms and clear alarms in a timely manner. **Table 7-6** describes the items displayed in this dashboard.
Cloud Service Status	The **Cloud Service Status** dashboard displays the overall status and alarms of all cloud services in each region. It helps you quickly identify the cloud services that have high and potential risks and improve the operational efficiency. **Table 7-8** describes the items displayed in this dashboard. **NOTE** The cloud service statuses are described as follows: • **High-risk**: Deployed cloud services have critical alarms that are not cleared. • **Low-risk**: Deployed cloud services have major alarms (instead of critical alarms) that are not cleared. • **Healthy**: Deployed cloud services do not have critical or major alarms that are not cleared. • **Undeployed**: Cloud services have not been deployed.

Dashboard Name	Description
Tenant Resources	The **Tenant Resources** dashboard displays total number of each cloud resource, clouds of each tenant and cloud resource trends, and resource usage of each tenant, helping users learn about distribution and usage of resources from the tenant perspective. **Table 7-5** describes the items displayed in this dashboard.
Audit Logs	The **Audit Logs** dashboard displays statistics on operations by risk level as well as operation details, including operation names, resource types (such as servers, storage, and networks), and operation time. In the upper right corner of the dashboard, you can select a time range to view desired logs. **Table 7-7** describes the items displayed in this dashboard.
Service Capacity Details	This dashboard displays statistics of cloud services by resource types. It also displays how the total, allocated, and available capacities of physical and logical resources. The dashboard allows you to query information, such as the allocated capacities and used capacities, about resource pools based on VM specifications and to export query results. **Table 7-9** describes the items displayed in this dashboard.
Hardware Metrics	The **Hardware Monitoring Dashboard** dashboard displays key metrics of servers, including CPU usage, memory usage, disk I/O usage, packet loss rate, average system load, and load statistics of top 5 servers. Drill-down screens display hardware details, resource allocation, and monitoring information of servers. For details about the displayed items, see **Table 7-10**. **NOTE** The dashboard is available only to users of regions where the professional edition is enabled.
AI Resource Operation Dashboard	This dashboard displays compute resource statistics, including total GPUs, total NPUs, dedicated resource pools, and total AI nodes. It also displays compute capacity of the current site and public sites, top associated training jobs and inference tasks by usage, and resource usage trends. For details about the displayed items, see **Table 7-11**.
AI Resource Detail Dashboard	This dashboard is a drilldown dashboard of AI Resource Operation Dashboard. It displays resource details in the resource pool associated with the tenant. For details about the displayed items, see **Table 7-12**.

Table 7-2 Resource Summary

Item	Description
Hardware Resources	Displays quantities of all types of hardware resources.
Common Cloud Resources	Displays the quantities of provisioned ECSs, provisioned EVS disks, and other common cloud resources provisioned in the management and tenant zones. Click **Details** next to **EVS disks** to view details about storage node resource capacities in the tenant and management zones.
Cloud Resource Overview	Displays the quantities of provisioned ECSs, provisioned EVS disks, and other cloud resources provisioned in the management and tenant zones.
Physical Resource Usage	Displays the average CPU and memory usage per day within a selected time range. You can click **Details** next to this item to view details about compute node resource capacities in the tenant and management zones.
Cloud Resource Statistics	Displays the allocated and total quantities of cloud resources (only in the tenant zone).
Cloud Resource Usage	Displays how cloud resource usage changes (only in the tenant zone) within a selected time range by day.
Virtual Resource Allocate Rates	Displays the allocation rates of virtual resources (including vCPUs, memory, and disks) in both tenant and management zones.
Virtual Resource Statistics	Displays the allocated and total capacities of virtual resources (including vCPUs, memory, and disks) in both tenant and management zones.
Virtual Resource Usage	Displays the usage of virtual resources (including vCPUs, memory, and disks) in both tenant and management zones within the selected time range by day.
Compute Node Capacity Details	Displays details about capacities of ECS resources including vCPUs, memory, and vGPUs by AZ, cluster, and resource type in both tenant and management zones.
Storage Node Capacity Details	Displays details about capacities of EVS resources including common I/O, high I/O, and ultra-high I/O disks by AZ and resource type in both tenant and management zones. For details, see **Table 7-3**.

Table 7-3 Resource types

Parameter	Extreme SSD	General-Purpose SSD V2	Ultra-high I/O	General-Purpose SSD	High I/O	Common I/O
API Name[e]	ESSD	GPSSD2	SSD	GPSSD	SAS	SATA
Description	Superfast disks for workloads demanding ultra-high bandwidth and ultra-low latency	SSD-backed disks allowing for tailored IOPS and throughput and targeting for transactional workloads that demand high performance and low latency	High performance disks excellent for enterprise mission-critical services as well as workloads demanding high throughput and low latency	Cost-effective disks designed for enterprise applications with medium performance requirements	Disks suitable for commonly accessed workloads[f]	Disks suitable for less commonly accessed workloads

Table 7-4 Hardware resources

Item	Description
Servers	Displays the number of servers and their information such as server names, alarm statuses, running statuses, and management IP addresses.
Switches	Displays the number of switches and their information such as switch names, alarm statuses, running statuses, and management IP addresses.
Routers	Displays the number of routers and their information such as router names, alarm statuses, running statuses, and management IP addresses.
Firewalls	Displays the number of firewalls and their information such as firewall names, alarm statuses, running statuses, and management IP addresses.
Security Devices	Displays the number of security devices and their information such as security device names, alarm statuses, running statuses, and management IP addresses.

Item	Description
Security software assets	Displays the number of security software assets and their information such as VM names, status, OS versions, and CPUs.

Table 7-5 Tenant resources

Item	Description
Cloud Resources TOP10	Displays statistics on quantity of cloud resources by tenant and top 10 cloud resources by quantity.
Resource Usage Trends	Displays daily changes on quantity of cloud resources.
Information	Displays quantity of each cloud resource.
List	Cloud resource details, displaying basic resource information.

Table 7-6 Hardware Alarms

Item	Description
Historical and Active Alarms	Displays the total number of historical alarms (cleared alarms) and active alarms (uncleared alarms) in the past month, and the number of alarms (cleared alarms and uncleared alarms) at each severity level.
Cleared and Uncleared Alarms	Displays the quantities of cleared and uncleared alarms and the percentages they account for in the total number of alarms in the past month.
Alarms by Device Type	Displays the quantities of alarms (including cleared and uncleared alarms) of network devices (including switches, routers, and firewalls) and physical hosts in the past month.
Alarm Change Trend in the Past Month	Displays how the number of alarms (including cleared alarms and uncleared alarms) at each severity level changes over the past month.
Current Alarms	Displays information about alarms uncleared in the past month, including the alarm names, severity levels, device IDs, first occurrence time, and last occurrence time. To check alarm details, click an alarm name.
History Alarms	Displays information about cleared and uncleared alarms in the past month, including the alarm names, severity levels, device IDs, first occurrence time, and last occurrence time. To check alarm details, click an alarm name.

Table 7-7 Audit Logs

Item	Description
Risks by Level	Displays respective quantities of operation risks at all levels (critical, major, minor, and warning).
Logs	Displays the operation log list, including the operation names, risk levels, and operators. If the list spans multiple pages, the pages will be displayed in a scrolling way. You can search for logs by operation name or region.

Table 7-8 Cloud Service Status

Item	Description
Status Distribution	Displays the quantities of cloud services in the **High-risk**, **Low-risk**, **Healthy**, and **Undeployed** states.
Alarm Status Overview	Displays the statuses and alarm quantities of all cloud services in each region. • If there are fewer than five regions, the regions are arranged horizontally. A grid below each region indicates a cloud service in that region. The quantities of uncleared critical and major alarms are displayed in the grid of each deployed cloud service. • If there are five or more regions, the alarm status overview is displayed in a two-dimensional table. Horizontal headers are regions, while the vertical headers are cloud services. When you move your pointer to the cell of a deployed cloud service in a region, the quantities of uncleared critical and major alarms of the cloud service are displayed.

Table 7-9 Service Capacity Details

Item	Description
Statistics by Resource Type	Displays a capacity view of frequently-used basic cloud services, including OBS, BMS, SFS, RDS, DeH, EIP, and VPN.
Resource Usage	Displays how the quantities of used resources from different cloud services change over time. You can select **Last week**, **Last month**, or **Last 3 months** in the upper right corner of the page to query resource usage statistics.

Table 7-10 Hardware metrics

Item	Description
Server usage metrics	Displays high CPU usage, high memory usage, high disk I/O usage, high packet loss rate during packet sending, and high average system load.
Top 5 resources by load	Displays top 5 resources with high usage metrics.
Hardware Details	Displays configuration details of the server, including CPUs, disks, memory, MAC address, and IP address.
Resource Allocation	Displays basic information of the server, including name, region, AZ, SN, and type.
Monitoring Information	Displays server metrics using data charts, such as disk I/O metrics and NIC metrics.

Table 7-11 AI Resource Operation Dashboard

Item	Description
Resource or Metric Statistics	Displays the AI nodes, GPUs, NPUs, dedicated resource pools, tasks, query requests per second (QPS), average response latency, and total requests (last 1 hour).
Computing Power	Displays the compute capacity of the current site and public sites, including CPU allocation, memory allocation, NPU usage, NPU (video memory) allocation, and GPU allocation.
Usage ranking (Top 10)	Displays top 10 tenants by usage of training jobs and inference tasks. Tenants can be ranked by compute usage or task quantity.
Resource usage trend statistics	Displays the resource usage trend chart. You can view the chart by last day, last week, last month, or last three months.

Table 7-12 AI Resource Detail Dashboard

Item	Description
Resource or Metric Statistics	Displays resource pools, AI nodes, tasks, training jobs, inference tasks, Notebooks, NPU compute capacity, NPUs, GPU compute capacity, and GPUs.

Item	Description
Resource Pool Statistics	Displays tasks, AI nodes, users, NPUs, allocated NPUs, NPU allocation, GPU allocation, NPU video memory allocation, total CPU, average CPU usage, total memory, and average memory usage.
Trend Chart	Displays the trends of the NPU allocation, NPU video memory allocation, GPU allocation, CPU allocation, and memory allocation.
Node Information	Displays node details, such as the node name, node IP address, and total NPUs.

----End

7.2 Dashboard Management

Prerequisites

You have logged in to ESM as an administrator.

Procedure

Step 1 Choose **Visualization** > **Dashboards Management** from the main menu.

Step 2 Perform operations by referring to **Table 7-13**.

Table 7-13 Dashboards management items

Item	Description	Procedure
Custom Logo	Custom dashboard logos can be uploaded. **NOTE** This function is available only to users of regions where the professional edition is enabled.	1. In the navigation pane, choose **Dashboards Management** > **Custom Logo**. 2. Click **Change**. 3. After selecting a file, click **Upload**. **NOTE** The logo image format can be JPG, JPEG, or PNG. The logo resolution cannot exceed 120 x 120 pixels, and the image cannot be larger than 50 KB. A transparent background is recommended.

Item	Description	Procedure
Subscription	Dashboards can be authorized to sub-users of the tenant account. **NOTE** This function is available only when you have the te_admin and "sec_admin" roles.	1. In the navigation pane, choose **Dashboards Management** > **Subscription**. 2. Select a dashboard and choose **Modify** in the **Operation** column. 3. Add a sub-user to the subscriber list. **NOTE** A maximum of 10 sub-users can be added. 4. Click **OK**.

----End

8 Personal Center

8.1 Configuring Message Notifications

You can configure message notification rules and templates on ESM so that notifications can be sent to specified users based on your configuration. The notifications allow the receivers to keep abreast of how cloud services are running, how many available resources there are, how many resources have been used, and if there are alarms related to cloud services.

NOTE

To configure message notifications, you must enable the professional edition of ESM first.

8.1.1 Obtaining or Canceling Authorization for Using SMN

ESM uses SMN to send message notifications. Before configuring message notifications, you need to obtain the authorization for using SMN.

Prerequisites

- You have purchased the professional edition of ESM.
- You have logged in to ESM as an administrator.

Authorization

Step 1 In the upper right corner of the page, click the username and select **Notification**.

Step 2 On the displayed authorization page, read the authorization information.

NOTE

- You will be billed based on how many notifications will be sent using SMN. Before confirming authorization, you need to learn about **SMN billing**.
- After you click **Confirm Authorization**, ESM calls Simple Message Notification (SMN) to create an agency on Identity and Access Management (IAM). For details, see **Delegating Resource Access to Another Account**. Before an agency is created, ensure that you have the permission to create agencies on IAM. For details, see **Creating a User Group and Assigning Permissions**.

Step 3 Select **I have read and understood the preceding description** and click **Confirm Authorization**.

Step 4 After the authorization is successful, verify that you have been redirected to the **Message Notification Settings** page.

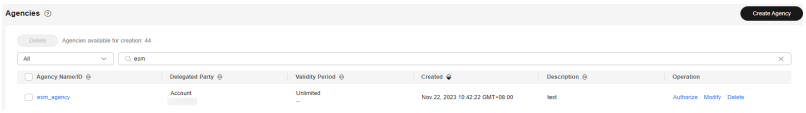
----End

Canceling the Authorization for Using SMN

Step 1 Log in to the **IAM console**.

Step 2 In the navigation pane, choose **Agencies**.

Figure 8-1 Agency



Step 3 In the agency list, locate the row that contains the **esm_agency** agency and click **Delete** in the **Operation** column.

Step 4 Click **Yes**.

To obtain the authorization again, see **Authorization**.

----End

8.1.2 Managing Agencies

You can update or modify an SMN agency.

Prerequisites

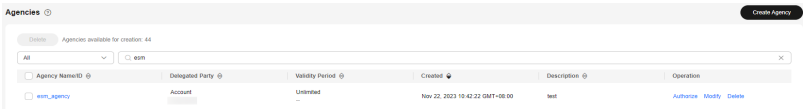
- You have purchased the professional edition of ESM.
- You have logged in to ESM as an administrator.

Procedure

Step 1 Log in to the **IAM console**.

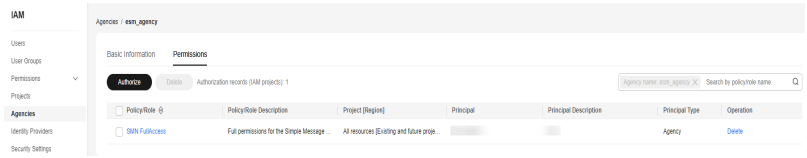
Step 2 In the navigation pane, choose **Agencies**.

Figure 8-2 Agency



Step 3 In the agency list, locate the row that contains the **esm_agency** agency and click its name.

Step 4 Click the **Permissions** tab, locate **SMN FullAccess**, and click **Delete** in the **Operation** column.



Step 5 Click **OK**.

Step 6 Log in to ESM. In the upper right corner of the page, click the username and select **Notification**.

Step 7 On the displayed authorization page, read the authorization information. For details, see **Authorization**.

Step 8 After the authorization is successful, check whether the minimum and necessary permissions required by SMN are displayed.

----End

8.1.3 Creating a Notification Rule

You can create a message notification rule.

NOTE

Up to 50 rules are allowed.

Prerequisites

- You have obtained the authorization for using SMN.
- You have purchased the professional edition of ESM.
- You have logged in to ESM as an administrator.

Procedure

Step 1 In the upper right corner of the page, click the username and select **Notification**.

NOTE

If you have not obtained authorization yet, read authorization information and confirm authorization first. For details about authorization, see **Obtaining or Canceling Authorization for Using SMN**.

Step 2 Click **Create Rule**. Set parameters based on **Table 8-1**.

Table 8-1 Parameter descriptions

Parameter	Description
Notification Name	Enter a notification name.
Region	Select regions.
Message Type	Select message types.
Message Template	Select a message template.

Parameter	Description
Severity	Select alarm severity, which can be **Critical**, **Major**, **Minor**, or **Warning**.
Topic	Select an event type for notifications. For details, see **SMN Topic Management**.
Description	Enter supplementary information.

Step 3 Click **OK**.

----End

8.1.4 Creating a Message Template

You can create a message template.

NOTE

Up to 10 templates are allowed.

Prerequisites

- You have obtained the authorization for using SMN.
- You have purchased the professional edition of ESM.
- You have logged in to ESM as an administrator.

Procedure

Step 1 In the upper right corner of the page, click the username and select **Notification**.

Step 2 Select the **Message Template** tab and click **Create Template**.

Step 3 Set the parameters described in **Table 8-2**.

Table 8-2 Parameter descriptions

Parameter		Description
Template Name		Enter a template name.
Description		Enter a brief description about the template.
Email or **SMS**	Subject	Enter the content of an email topic. This parameter is available only when **Email** is selected.

Parameter		Description
	Body	Alarm notifications can be sent by email or SMS. The variables and value ranges supported by the notification template are as follows: • **EventName**: **${*alarm_name_en*}** **NOTE** If the service that reports the alarm does not report the English alarm name, obtain the value from the Chinese alarm name. • **EventId**: **${*alarm_id*}** • **Region**: *${region_code}* • **EventCategory**: **${*event_category*}**. The value can be **HARDWARE** (for a hardware alarm) and **SERVICE_ALARM** (for a cloud service alarm). • **EventSeverity**: **${*event_severity*}**. The value can be **Critical**, **Major**, **Minor**, or **Warning**. • **EventObject**: **${*event_object*}** • **ClearCategory**: **${clear_category}**. The value can be **Occur** or **Clear**. • **Time**: **${time}**. The value is the alarm generation time or alarm clearance time (UTC time).

Step 4 Click **OK**.

----End

8.1.5 Other Related Tasks

You can view, modify, or delete notification rules and message templates.

Prerequisites

- You have obtained the authorization for using SMN.
- You have purchased the professional edition of ESM.
- You have logged in to ESM as an administrator.

Procedure

Step 1 In the upper right corner of the page, click the username and select **Notification**.

Step 2 Perform the tasks described in **Table 8-3**.

Table 8-3 Tasks

Task	Description	Procedure
Viewing notification rules and message templates	View details about notification rules and message templates.	1. Select the **Notification Rule** or **Message Template** tab. 2. View details in the list.
Editing notification rules and message templates	Edit notification rules and message templates. **NOTE** Default templates cannot be edited.	1. Select the **Notification Rule** or **Message Template** tab. 2. Locate the row that contains a rule or template and click **Edit**. 3. Modify the parameters. 4. Click **OK**.
Deleting notification rules and message templates	Delete the notification rules and message templates that are no longer in use. **NOTE** Default templates cannot be deleted.	1. Select the **Notification Rule** or **Message Template** tab. 2. Locate the row that contains a rule or template and click **Delete**. 3. Click **OK**.

----End

8.2 My Service Tickets

On the My Service Tickets page, you can submit service tickets, view service ticket progress, and view service ticket details. This helps you learn about service ticket status and ensure that service tickets are handled in a timely and effective manner, improving user experience.

Prerequisites

You have logged in to ESM as an administrator.

Authorization

Step 1 Click **Customer Service** the upper right corner of the page.

Step 2 In the navigation pane, choose **My Service Tickets**.

Step 3 Perform related tasks by referring to **Table 8-4**.

Table 8-4 Operations about service tickets

Operation	Description	Step
Viewing all service tickets	Allows you to view all service tickets.	On the **My Service Tickets** page, you can: • Click the **All**, **To be confirmed**, **Processing**, or **Assigned** tab page to view service tickets. • Search for a service ticket by ticket number or by entering a keyword. • View service tickets by issue type, like all, consultation, and fault reporting.
Viewing details of a service ticket	Allows you to view details of a service ticket.	1. In the service ticket list, locate a ticket and click its name. 2. In the dialog box, view dialog information and processing details. – Ticket details: View the ticket information on the right of the dialog box. – Closing a ticket: After confirming that the issue is solved, you can close the ticket. – Deleting a ticket: If a ticket is not required, you can delete it.
Creating a service ticket	Allows you to submit a service ticket to resolve an issue.	1. Click **Create a Service Ticket**. 2. In the **Issue Description** area, select a site, service, and issue type, enter an issue description, and click **Next**. 3. In the **Basic Information** area, select a contact method, and enter your mobile number or email address. 4. Click **I have read and agree to the *Ticket Service Agreement*.** and click **Create a Service Ticket**. 5. On the ticket service page, view the ticket submission status and wait for engineers to contact you.

----End

9 Permissions Management

9.1 Creating a User and Granting ESM Permissions

You can use **Identity and Access Management (IAM)** for fine-grained permissions control on ESM. With IAM, you can:

- Create IAM users for employees based on your organizational structure and grant minimum permissions to these users. Each IAM user will have their own security credentials for accessing specific ESM resources.
- Grant users only the permissions required to perform a given task based on their job responsibilities.

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

Prerequisites

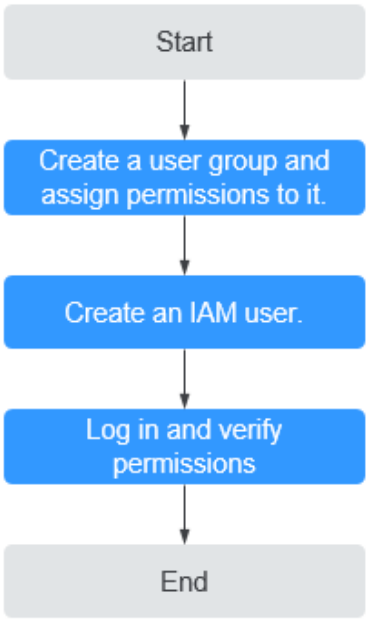
You should be clear about what system policies can be assigned to user groups and choose the right policies based on your requirements. **Table 9-1** describes the system policies.

Table 9-1 ESM system policies

Policy	Description	Type	Suggestion
ESM FullAccess	Administrator permissions on all ESM functions	System policy	Assign this policy to an administrator who registers and deregisters accounts.
ESM ReadOnly Access	Read-only permission on ESM	System policy	Assign this policy to administrators who use dashboards.

Permission Granting Process

Figure 9-1 Process for granting ESM permissions



1. **Create a user group and assign permissions**.

   Create a user group on the IAM console, and attach the **ESM FullAccess** policy to the group.

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

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

3. **Log in** and verify the permission granting.

   Access the ESM console using the created user, and verify that the user has the administrator permissions for ESM in the following way:

   Choose **Organization** from the main menu. On the **Tenants** page, click **Create Tenant**. If a tenant can be created, the **ESM FullAccess** policy has already taken effect.

A Change History

Release Date	Change Description
2025-10-30	This issue is the seventh official release.
2025-04-30	This issue is the sixth official release.
2024-10-30	This issue is the fifth official release. It incorporates the following change. Added: • Agent management in **Managing Agencies**. • **My Service Tickets** in **My Service Tickets**.
2024-07-30	This issue is the fourth official release. Added the following information: • Hardware Monitoring Dashboard in **Operations Dashboards**. • Customized logo and subscription authorization in **Dashboard Management**.
2024-04-30	This issue is the third official release. Added the following information: HCSO Service Capacity Details in **Operations Dashboards**.
2023-11-30	This issue is the second official release. Description about message notification settings in **Configuring Message Notifications**
2023-10-30	This issue is the first official release.

