

Multi-Site High Availability Service

User Guide

Issue 01
Date 2024-11-20



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2024. 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 Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI 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.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: <https://www.huaweicloud.com/intl/en-us/>

Contents

1 Getting Started with MAS.....	1
2 Modules.....	3
3 Namespace.....	6
3.1 Namespace Management.....	6
3.2 Data Source.....	9
3.3 Data Synchronization.....	11
4 Multi-Active Instances.....	15
4.1 Buying a MAS Instance.....	15
4.1.1 Preparing Resources.....	15
4.1.2 Creating an Instance.....	16
4.2 Name and Description Modification.....	19
4.3 ETCD Certificate Downloading.....	19
4.4 ETCD Password Resetting.....	19
4.5 Security Group Modification.....	20
4.6 Multi-Active Area Monitoring.....	20
4.7 Monitoring Dashboard.....	21
4.8 Billing Mode Change.....	21
4.8.1 From Pay-per-Use to Yearly/Monthly.....	22
4.8.2 From Yearly/Monthly to Pay-per-Use.....	22
4.9 Multi-Active Instance Deletion.....	22
5 Application Management.....	24
6 Monitor Management.....	27
6.1 MySQL/Oracle/PostgreSQL Monitoring.....	27
6.2 Redis Monitoring.....	33
6.3 MongoDB Monitoring.....	38
6.4 Elasticsearch Monitoring.....	43
6.5 API Monitoring.....	47
6.6 General Monitor Operations.....	50
6.6.1 Configuring Monitors.....	50
6.6.2 Obtaining the SDK Access Configuration.....	51
6.6.3 Switching a Monitor.....	52

6.6.4 Modifying a Monitor.....	53
6.6.5 Deleting a Monitor.....	53
6.7 Global Configurations.....	54
6.7.1 Configuring a Secret Key.....	54
6.7.2 Configuring a Notification.....	55
6.7.3 Configuring DC-level Switchover.....	57
7 Credential Management.....	58
8 Event Monitoring.....	62
8.1 Introduction to Event Monitoring.....	62
8.2 Viewing Event Monitoring Graphs.....	62
8.3 Creating an Alarm Rule to Monitor an Event.....	63
8.4 Events Supported by Event Monitoring.....	64
9 Audit Logs.....	66
10 Permissions Management.....	68
10.1 Creating a User and Assigning Permissions.....	68
10.2 MAS Custom Policies.....	69

1 Getting Started with MAS

Multi-Site High Availability Service (MAS) is part of Huawei's consumer solution for high availability of multi-active applications. It provides E2E service failover and disaster recovery (DR) drill capabilities from the traffic input and data to the application layer, for faster service recovery and better continuity.

Prerequisites

1. You have [signed up for a HUAWEI ID and enabled Huawei Cloud services](#).
2. Your account has permissions to use Multi-Site High Availability Service (MAS). For details about how to authorize an account and bind permissions to it, see [10.1 Creating a User and Assigning Permissions](#).

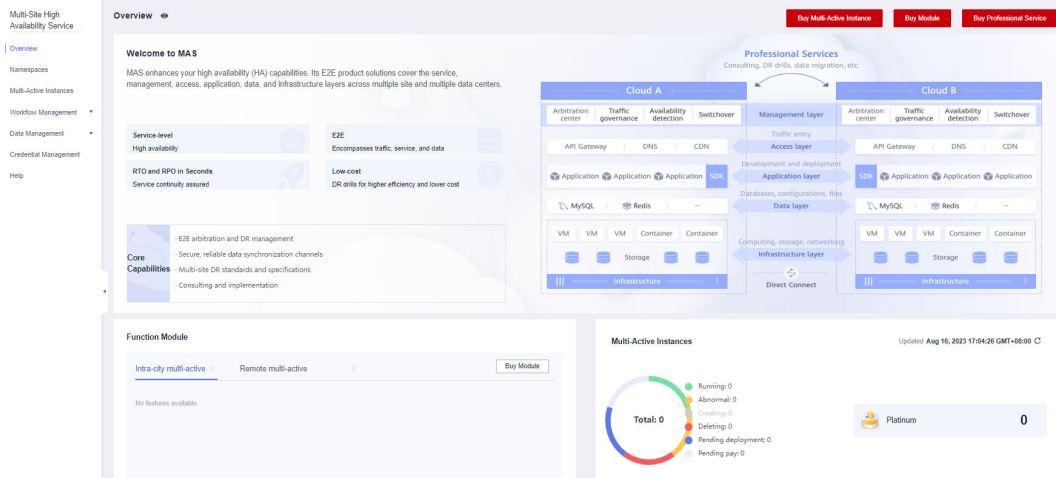
Logging In to the MAS Console

Step 1 Log in to the [Huawei Cloud console](#).

Step 2 Click  and select a region.

Step 3 Click  in the upper left and click **Multi-Site High Availability Service** to enter the MAS console.

Figure 1-1 MAS console



----End

2 Modules

Introduction

This section describes how to manage the edition and features of your instance. The following features are supported:

- MySQL
- Oracle
- PostgreSQL
- Redis
- MongoDB
- Elasticsearch
- openGauss
- API

NOTE

- Enable corresponding features before you create data sources and monitors.
- If a feature is not enabled here, you cannot create or check the corresponding monitor on the instance details page.

Enabling a Module

Step 1 Go to the [Buy Module](#) page.

Step 2 Select an edition and features, and click **OK**.

Figure 2-1 Enabling a module

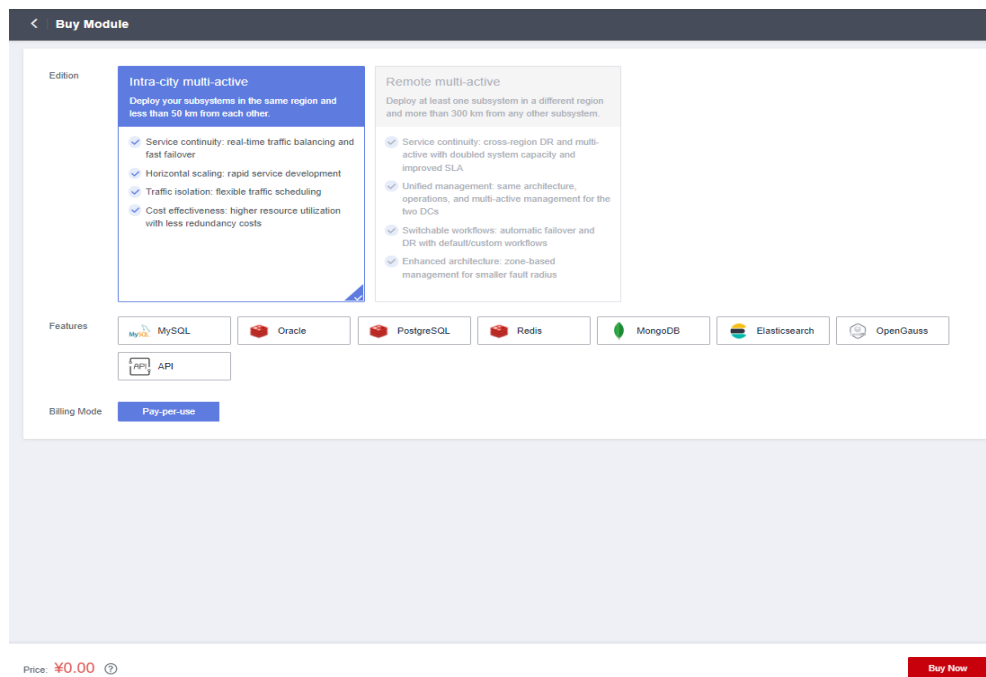


Table 2-1 Module parameters

Parameter	Description
Edition	You can select the Intra-city multi-active or Remote multi-active edition.
Features	Options: <ul style="list-style-type: none"> ● MySQL ● Oracle ● PostgreSQL ● Redis ● MongoDB ● Elasticsearch ● openGauss ● API
Billing Mode	Billing mode of the function module. Pay-per-use is selected by default.

----End

Modifying a Module

Step 1 On the MAS console, click **Overview** and click **Modify** next to a function module.

Step 2 Select or deselect the target features, and click **OK**.

 **NOTE**

If a feature has dependent instances and data sources, you cannot delete it by deselecting it.

----End

Deleting a Module

Step 1 On the MAS console, click **Overview** and click **Delete Module** next to a function module.

Step 2 Click **OK** to delete the module.

 **NOTE**

- The enabled features with the selected edition will also be deleted.
- If a function module has dependent instances and data sources, it cannot be deleted.

----End

3 Namespace

3.1 Namespace Management

3.2 Data Source

3.3 Data Synchronization

3.1 Namespace Management

Introduction

A namespace is a collection of all resources (traffic input, multi-active areas, data synchronization records, and monitoring information) for a MAS instance. You can create a namespace for each system (such as OA and payment systems) to isolate resources.

Creating a Namespace

Step 1 On the MAS console, click **Namespaces** and click **Create Namespace** in the upper right corner.

Step 2 Configure the namespace and click **OK**.

Figure 3-1 Creating a namespace

*Type

Internet

Intra-city multi-active
Deploy your subsystems in the same region and less than 50 km from each other.

Remote multi-active (unification)
Deploy at least one subsystem in a different region and more than 300 km from any other subsystem.

Remote geographic-redundancy
Deploy at least one subsystem in a different region and more than 300 km from any other subsystem.

*Name

Enter a name.

Description

Enter a description.

The screenshot shows a configuration page for a namespace. At the top, there's a dropdown for 'Enterprise Project' set to 'default' and a 'View Enterprise Projects' link. Below that, a checkbox for 'Multi-Active Area' is checked, with a note: 'I understand the following constraint: Select different regions for higher availability, otherwise services will be affected in case of a regional fault.' The main configuration area is divided into three columns: 'Area', 'Primary Multi-Active Area', and 'Standby Multi-Active Area'. Each column has a 'Cloud' section with radio buttons for 'Huawei Cloud' (selected) and 'Third-party data center'. Below this are input fields for 'Area Name', 'Description', and dropdown menus for 'Region' (set to 'CN-North-Ulanqas203'), 'Region Code' (set to 'cn-north-7'), 'Default Credential' (set to 'Current Account Credential'), 'Default Project' (set to 'cn-north-7'), and 'AZ' (set to 'Select an AZ'). At the bottom, there's a 'Features' section with icons for MySQL, Oracle, PostgreSQL, Redis, MongoDB, Elasticsearch, OpenGauss, and API.

Table 3-1 Namespace parameters

Parameter	Description
Type	<p>Select a namespace type.</p> <ul style="list-style-type: none"> • Intra-city multi-active: Deploy your subsystems in the same region and less than 50 km from each other. • Remote multi-active (coming soon): Deploy at least one subsystem in a different region and more than 300 km from any other subsystem. • Remote geographic-redundancy: Deploy at least one subsystem in a different region and more than 300 km from any other subsystem.
Name	Customize a name for the namespace.
Description	Enter a description about the namespace.
Enterprise Project	Select an enterprise project. You can associate a namespace with the enterprise project. This is available only for enterprise accounts.
Multi-Active Area	<p>There are two kinds of clouds for you to deploy your active and standby multi-active areas:</p> <ul style="list-style-type: none"> • Huawei Cloud • Third-party data center
Area Name	Customize the names for the multi-active areas.
Description	Enter the descriptions for the multi-active areas.
Regions	Configure the regions for the multi-active areas.
Region Code	Configure the region codes for the multi-active areas.

Parameter	Description
Default Credential	Configure the credentials for the multi-active areas. The credentials configured here will be displayed when Creating a Data Source . MAS can access different resources based on the credential. The default value Current Account Credential indicates that MAS can access the resources under the current account. For details about credentials, see 7 Credential Management .
Default Project	The Identity and Access Management (IAM) projects to which the resources belong. You can select the default IAM project or enter a project ID. A project is preset in each region by default. IAM users can be granted permissions in a default project to access all resources in the region associated with the project.
AZ	Select the availability zones (AZs) for the multi-active areas. AZs are physically isolated but connected through an internal network.
Features	Select the features to be enabled. If no features are available, see Enabling a Module . NOTE Enable corresponding features before you create data sources and monitors.

----End

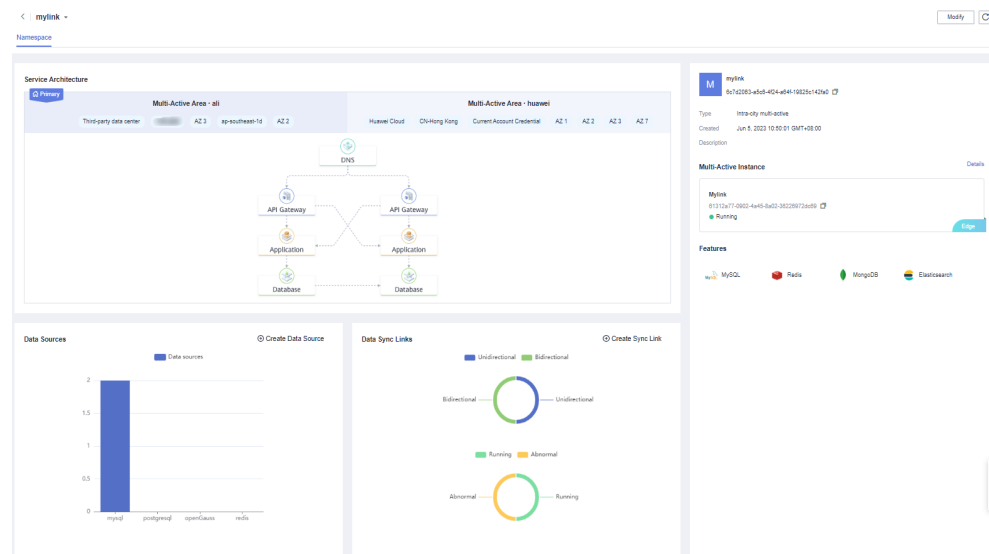
Checking a Namespace

On the namespace details page, the type, instances, enabled features, multi-active areas and their AZs, data sources, and data sync links are shown.

Step 1 On the MAS console, click **Namespaces**. On a namespace card, choose **Operation > Details**.

Alternatively, you can click a namespace's name to check its details.

Step 2 Check namespace information.

Figure 3-2 Namespace

Step 3 (Optional) Click **Create Data Source**. For details, see [Creating a Data Source](#).

Step 4 (Optional) Click **Create Sync Link**. For details, see [Creating a Sync Link](#).

----End

Modifying a Namespace

Step 1 On the MAS console, click **Namespaces**. On a namespace card, choose **Operation** > **Modify**.

Alternatively, you can click **Modify** on the namespace details page.

Step 2 Modify the namespace and click **OK**.

----End

Deleting a Namespace

Step 1 On the MAS console, click **Namespaces**. On a namespace card, choose **Operation** > **Delete**.

Step 2 Click **OK** to delete the namespace.

NOTE

If a namespace has dependent instances and data sources, it cannot be deleted.

----End

3.2 Data Source

Creating a Data Source

Step 1 Log in to the MAS console and choose **Data Management** > **Data Sources**.

- Step 2** Select a target namespace in the upper left corner.
- Step 3** Click **Create Data Source** in the upper right corner.
- Step 4** Configure the data source and click **OK**.

Figure 3-3 Creating a data source

Create Data Source

Basic Info

- * Deployment Mode: huawei
- Standby | Huawei Cloud
- * Data Source Type: MySQL, Redis, Enable More Function Point postgresql openGauss
- * Data Source: mas-data-mysql-GQw8xF
- Description: 0/100

Connection Information

- Mode: Custom, RDS
- * Connection Address: IPv4, . . . / Port
- Database Name: Enter a database name.
- * Username: Enter a database username.
- * Password: Enter a password.
- * Confirm Password: Enter the password again.

Ensure that the database link address is the data source MySQL. Otherwise, the synchronization task cannot be created successfully.

Table 3-2 Data source parameters

Parameter	Description
Deployment Mode	The active/standby area to which the data source belongs
Data Source Type	Options: MySQL , PostgreSQL , Redis , and OpenGauss . If a target data source is unavailable, enable the corresponding feature by modifying the namespace. For details, see Modifying a Namespace .
Data Source	Keep the default name or customize one.
Description	Enter a description for the data source.
Mode	The connection mode
Connection Address	The address and port number for accessing the database. This is required if Mode is set to Custom .

Parameter	Description
Database Name	The name of the database. This is required if Mode is set to Custom .
Credential	The default credential set for the current multi-active area is used. This is displayed if Mode is not set to Custom .
Project	The default project set for the current multi-active area is used. This is displayed if Mode is not set to Custom .
Instances	Select an existing database instance. This is displayed if Mode is not set to Custom .
Username	The username for logging in to the database
Password	The password for logging in to the database
Confirm Password	Enter the password again.

 **NOTE**

If you need to create sync links for MySQL or PostgreSQL data sources, ensure that at least one of your MySQL data sources and one of your PostgreSQL data sources is using RDS, that is, its **Mode** is set to **RDS**.

----End

Deleting a Data Source

- Step 1** Log in to the MAS console, choose **Data Management** > **Data Sources**, and click **Delete** in the row that contains a target data source.
- Step 2** Click **OK** to delete the data source.

----End

3.3 Data Synchronization

This section describes how to create a data sync link for the data source. Currently, only DRS real-time DR tasks can be created. For details, see [DR Overview](#).

Creating a Sync Link

- Step 1** Log in to the MAS console, choose **Data Management** > **Synchronization**, and click **Create Sync Link** in the upper right.
- Step 2** Configure the sync link and click **OK**.

Figure 3-4 Creating a sync link

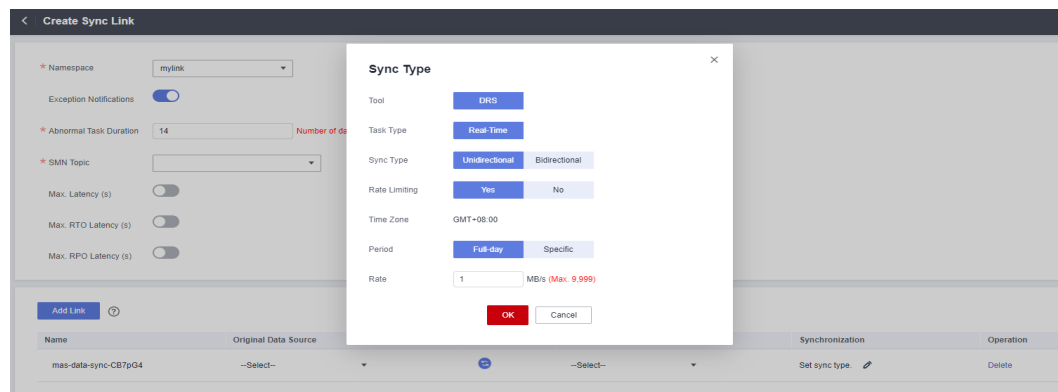


Table 3-3 Sync link parameters

Parameter	Description
Namespace	Select a namespace.
Exception Notifications	By default, this option is disabled. If it is enabled, monitor and database exceptions will be sent to you in a timely manner.
Abnormal Task Duration	Number of days before an abnormal sync task stops automatically. Default value: 14
SMN Topic	This is required if Exception Notifications is enabled. Select a topic from the drop-down box.
Max. Latency (s)	This is disabled by default and is required if Exception Notifications is enabled. During an incremental synchronization, a synchronization delay indicates a time difference (in seconds) of synchronization between the source and destination databases. If the synchronization delay exceeds the threshold you specify, DRS will send alarms to the specified recipients. Value range: 0 to 3600
Max. RTO Latency (s)	This is disabled by default and is required if Exception Notifications is enabled. Recovery Time Objective (RTO) refers to the difference between the time when a transaction on the current DRS instance is transmitted to the DR instance and the time when the transaction is successfully executed. Generally, the transaction is the latest transaction received by DRS. When RTO is 0, all transactions on the DRS instance have been completed on the DR database.

Parameter	Description
Max. RPO Latency (s)	This is disabled by default and is required if Exception Notifications is enabled. Recovery Point Objective (RPO) refers to the difference between the time when a transaction in the current service database is submitted and the time when the transaction is sent to DRS. Generally, the transaction is the latest transaction received by DRS. When RPO is 0, all the data in the service database has been migrated to the DRS instance.
Add Link	Click to add a sync link.
Name	Keep the default name or customize a name for the sync link.
Original Data Source	The source data source
Target Data Source	The target data source
Synchronization	The synchronization settings
Sync Type	The synchronization direction, which can be Unidirectional (default) or Bidirectional .
Rate Limiting	Whether to limit the traffic rate, which can be Yes (rate limited) or No (rate not limited).
Period	Whether the rate will be limited Full-day or during a Specific period of time.
Rate	Traffic rate, in MB/s. Max. 9999
Time Range	This is required if Period is set to Specific .

 **NOTE**

When creating a sync link for a MySQL or PostgreSQL database, ensure that the original data source and target data source are not the same. Additionally, ensure that at least one of your MySQL data sources and one of your PostgreSQL data sources is using RDS.

----End

Deleting a Sync Link

Step 1 Log in to the MAS console, choose **Data Management** > **Synchronization**, and click **Delete** in the row that contains a target link.

Step 2 Click **OK** to delete the link.

----End

Switching Sync Links

Note that:

- Perform sync link switchovers only when the DR task is in progress or abnormal.
- Do not perform switchovers repeatedly or on dual-active DR tasks.

Step 1 Log in to the MAS console and choose **Data Management > Synchronization**.

Step 2 Select the target links, choose **Batch Operations > Data Source Switchover**.

Step 3 Click **OK**.

----End

4 Multi-Active Instances

- [4.1 Buying a MAS Instance](#)
- [4.2 Name and Description Modification](#)
- [4.3 ETCD Certificate Downloading](#)
- [4.4 ETCD Password Resetting](#)
- [4.5 Security Group Modification](#)
- [4.6 Multi-Active Area Monitoring](#)
- [4.7 Monitoring Dashboard](#)
- [4.8 Billing Mode Change](#)
- [4.9 Multi-Active Instance Deletion](#)

4.1 Buying a MAS Instance

4.1.1 Preparing Resources

Introduction

This section describes how to buy, modify, and delete instances on the MAS console.

Preparing Required Resources

Prepare a Virtual Private Cloud (VPC), subnet, and security group before you start. Each MAS instance is deployed in a VPC and bound to a specific subnet and security group. In this way, MAS provides an isolated virtual network environment and security protection policies that can be easily configured and managed by users.

- For details about how to create a VPC and subnet, see [Creating a VPC](#). To create and use a subnet in an existing VPC, see [Creating a Subnet for the VPC](#).

- For details about how to create a security group, see [Creating a Security Group](#). To add rules to a security group, see [Adding a Security Group Rule](#).

4.1.2 Creating an Instance

Introduction

An instance is an independent resource space. All operations are performed in an instance. Resources of different instances are isolated from each other. You can use one or more MAS instances based on service requirements.

Instances' statuses are marked in different colors: green if the instance is normal, yellow if the instance is abnormal, red if the instance is failed to be created or deleted.

Prerequisites

- A VPC is available, and a subnet and security group have been configured. (For details on how to create a VPC, subnet, and security group, see [4.1.1 Preparing Resources](#).)
- You have had enough quota to create MAS instances. Otherwise, increase quota [by referring to My Quotas](#).

Procedure

- Step 1** Go to the [page for buying a MAS instance](#).
- Step 2** Configure the instance and click **Create**. The system will calculate the fee based on the selected product type.

Figure 4-1 Buying a MAS instance

The screenshot shows the 'Buy Multi-Active Instance' configuration interface. It includes the following fields and options:

- Namespace:** A dropdown menu with '--Select--' and a help icon.
- Multi-Active Areas:** Two sections, 'Multi-active area 1' and 'Multi-active area 2', each with 'Select a region.' and 'Select an ...' buttons.
- Arbitration Node AZ:** A dropdown menu with 'AZ 3' selected.
- Constraint:** A checkbox 'I understand the following constraint:' with a note: 'The selected AZs must match my service deployment architecture.'
- Billing Mode:** A button labeled 'Pay-per-use'.
- Product Type:** A button labeled 'Platinum'.
- Two-Way Authentication:** Radio buttons for 'Yes' (selected) and 'No'.
- Instance Name:** A text input field with a red border and placeholder 'Enter an instance name.'
- Description:** A text area with placeholder 'Enter a description.' and a character count '0/100'.
- Network:** A dropdown menu with 'vpc-mylink' and a 'Create VPC' link.
- IPv4 CIDR Block:** Input fields for '192', '168', '0', '0' and a slash '24'. Below are recommended blocks: '10.0.0.0/24 (choose)', '172.16.0.0/24 (choose)', and '192.168.0.0/24 (choose)'. A warning message states: 'This CIDR block cannot overlap that of your VPC or any peering connection CIDR blocks.'
- Security Group:** A dropdown menu with 'default' and a 'Security Group' link.
- ETCD Password:** A password input field with a toggle for visibility.
- Confirm Password:** A password input field with a toggle for visibility.
- Price:** '¥0.00' with a help icon.
- Create:** A red button at the bottom right.

Table 4-1 Instance parameters

Parameter	Description
Namespace	Select a namespace. NOTE Namespaces with any of the following types are supported: <ul style="list-style-type: none"> Intra-city multi-active: Both the active and standby areas are in the current region. This is recommended for instances that are used for intra-city multi-active. Remote geographic-redundancy: The standby area is in the current region. This is recommended for instances that are used to execute workflows.
Multi-Active Areas	The AZs of the areas had been set during namespace creation.
Arbitration Node AZ	Select an AZ to which the ETCD arbitration node belongs based on your service deployment architecture. This is required when an intra-city multi-active namespace is selected.

Parameter	Description
Billing Mode	There are two options: <ul style="list-style-type: none">• Pay-per-use: This postpaid mode bills you by instance usage. You can enable or delete your instance at any time.• Yearly/Monthly: This prepaid mode bills you based on the subscription duration and is ideal when the resource use duration is predictable.
Product Type	Platinum is supported.
Two-way Authentication	ETCD authentication. This is enabled by default and is required when an intra-city multi-active namespace is selected. CAUTION Disabling two-way authentication can be risky.
Instance Name	Customize a name for the instance.
Description	Enter a description for the instance.
Enterprise Project	Select an enterprise project.
Network	Select a VPC and subnet to be associated with the instance. The VPC and subnet must be created in advance.
IPv4 CIDR Block	This CIDR block cannot overlap that of your VPC or any peering connection CIDR blocks. Recommended: 10.0.0.0/24, 172.16.0.0/24, 192.168.0.0/24
Security Group	Select a security group to be associated with the instance. The security group must be created in advance. CAUTION Enable the port of the monitored resource for the security group.
ETCD Password	Enter an ETCD password. This is required when an intra-city multi-active namespace is selected.
Confirm Password	Enter the ETCD password again. This is required when an intra-city multi-active namespace is selected.
Required duration	This is required when Billing Mode is set to Yearly/Monthly .
Auto Renew	This is required when Billing Mode is set to Yearly/Monthly . Renew the subscription on the management console. For details, see Renew Rules .

Step 3 Wait for the system to create an instance with pay-per-use billing.

Pay for the order and wait for the system to create an instance with yearly/monthly billing.

Step 4 This will take 5 to 15 minutes to complete. After the instance is created, the instance status is **Available** on the **Multi-Active Instances** page.

If the instance status is **Failed**, delete it, create another one, or contact the technical support.

----End

4.2 Name and Description Modification

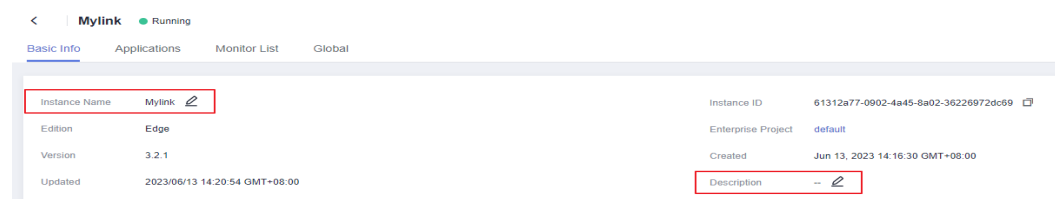
This section describes how to modify the name and description of an instance on the instance details page.

Procedure

Step 1 Log in to the MAS console. On the **Multi-Active Instances** page, click an instance to go to its console.

Step 2 On the **Basic Info** page, click  next to **Instance Name** and **Description**.

Figure 4-2 Modifying the instance name and description



Step 3 Click  to complete the modification.

----End

4.3 ETCD Certificate Downloading

ETCD supports two-way client certificate authentication.

Procedure

Step 1 Log in to the MAS console. On the **Multi-Active Instances** page, click an instance to go to its console.

Step 2 On the **Basic Info** page, go to the **Connections** area and click **Download**.

----End

4.4 ETCD Password Resetting

This section describes how to reset the ETCD password for a platinum instance.



Procedure

- Step 1** Log in to the MAS console. On the **Multi-Active Instances** page, click an instance to go to its console.
 - Step 2** On the **Basic Info** page, go to the **Connections** area, click **Details** next to the ETCD certificate.
 - Step 3** Reset the password by entering it twice, and click **OK**.
- End

4.5 Security Group Modification

This section describes how to modify the security group for a platinum instance. Ensure that the port of the monitored resource for the security group is enabled.

Procedure

- Step 1** Log in to the MAS console. On the **Multi-Active Instances** page, click an instance to go to its console.
 - Step 2** On the **Basic Info** page, go to the **Networking** area and click  next to the security group.
 - Step 3** Select a new security group and click .
 - Step 4** Wait for a period of time for the security group to change.
- End

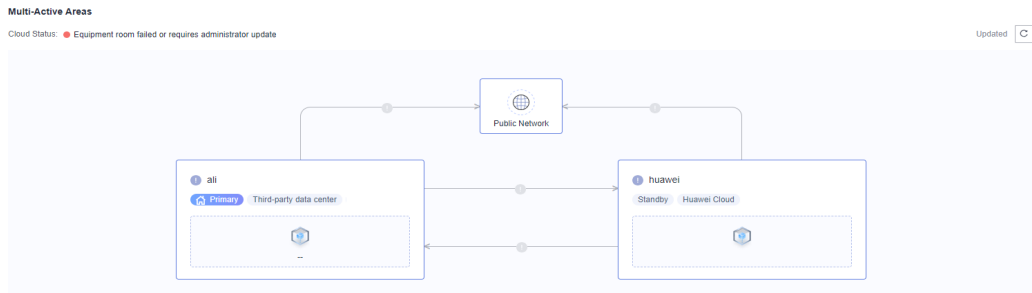
4.6 Multi-Active Area Monitoring

This section describes how to monitor the connection statuses between the multi-active areas, from the multi-active area to the public network, and within a multi-active area.

Checking Multi-Active Area Statuses

- Step 1** Log in to the MAS console. On the **Multi-Active Instances** page, click an instance to go to its console.
- Step 2** On the **Basic Info** page, check the multi-active area statuses.

Figure 4-3 Checking multi-active areas



----End

4.7 Monitoring Dashboard

You can check the quantity, status, and statistics of monitors and applications under the instance.

Checking the Monitoring Dashboard

- Step 1** Log in to the MAS console. On the **Multi-Active Instances** page, click an instance to go to its console.
- Step 2** On the **Basic Info** page, check the monitoring dashboard.
- Step 3** Click a pie chart to go to the **Monitor List** page to check monitor details.

Figure 4-4 Monitoring dashboard



NOTE

The **Abnormal** legend in charts indicates the exceptions, including invoking exception, monitoring initialization failure, monitoring exception, monitoring not generated, or monitoring configuration error. For details, see [Table 6-1](#).

----End

4.8 Billing Mode Change

4.8.1 From Pay-per-Use to Yearly/Monthly

Scenario

Instance billing mode can be changed from the pay-per-use mode to yearly/monthly mode.

 **NOTE**

- This is unavailable for frozen instances.
- This will not affect services.

Procedure

- Step 1** Log in to the MAS console and go to the **Multi-Active Instances** page.
- Step 2** In the **Operation** column of an instance, click **More**, and change the billing mode.
- Step 3** Click **OK** in the dialog box.
- Step 4** Confirm the subscription details, specify the usage duration, and pay for the order.
----End

4.8.2 From Yearly/Monthly to Pay-per-Use

Scenario

Instance billing mode can be changed from the yearly/monthly mode to pay-per-use mode.

 **NOTE**

- This is unavailable for frozen instances.
- This will not affect services.

Procedure

- Step 1** Log in to the MAS console and go to the **Multi-Active Instances** page.
- Step 2** In the **Operation** column of an instance, click **More**, and change the billing mode.
- Step 3** Click **OK** in the dialog box.
- Step 4** Confirm the subscription details and complete the process.
----End

4.9 Multi-Active Instance Deletion

Scenario


You can delete unnecessary instances to release resources.

You may need to force delete instances that are not in the **Running** status.

Deleting a Running Instance

- Step 1** Log in to the MAS console and go to the **Multi-Active Instances** page.
 - Step 2** In the **Operation** column of an instance or on an instance card, choose **More > Delete**.
 - Step 3** Click **OK** to delete the instance.
- End

Forcibly Deleting an Instance

- Step 1** Log in to the MAS console and go to the **Multi-Active Instances** page.
 - Step 2** In the **Operation** column of an instance or on an instance card, choose **More > Force Delete**.
-  **NOTE**
- Only instances that are not in the running state can be deleted by force.
- Step 3** Click **OK** to delete the instance.
- End

5 Application Management

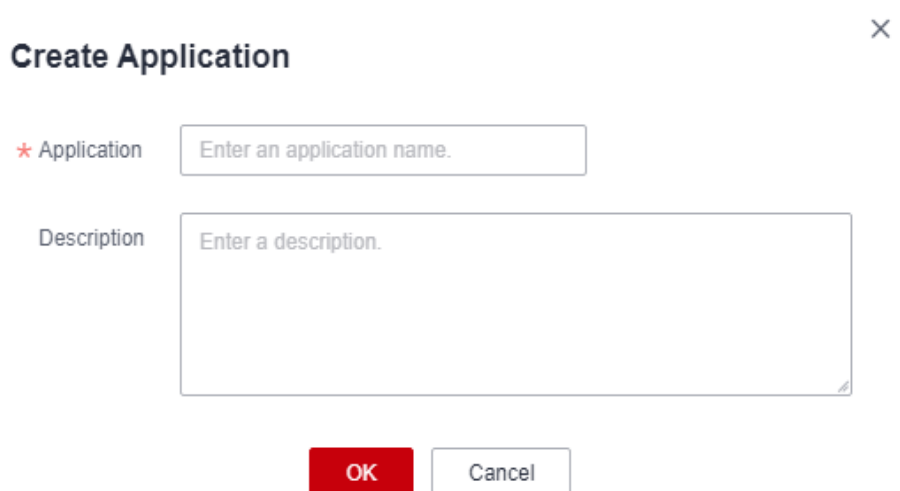
Introduction

MAS uses applications to isolate resources of different users in the same instance. Resources (such as MySQL and Redis monitors) created in an instance must be associated with an application. By default, IAM users can only view and manage their own applications and resources. You can use your account to view and manage all applications and resources created by IAM users under your account.

Creating an Application

- Step 1** Log in to the MAS console. On the **Multi-Active Instances** page, click an instance to go to its console.
- Step 2** Click the **Applications** tab, and click **Create**.
- Step 3** Enter the application information, then click **OK**.

Figure 5-1 Creating an application



Create Application ×

* Application

Description

OK Cancel

Table 5-1 Application parameters

Parameter	Description
Application	Customize the application name.
Description	(Optional) Enter a description about the application.

----End

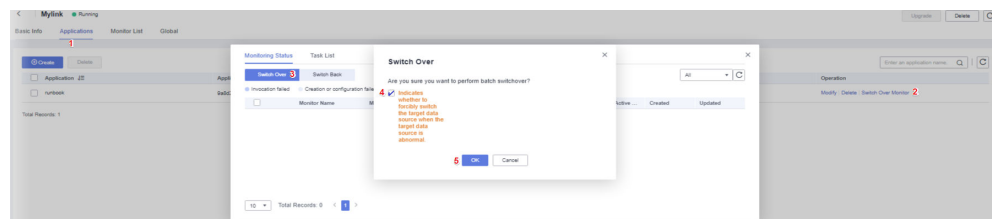
Switching Monitors

Create monitors for the application by referring to [6 Monitor Management](#). Then, you can switch over and switch back monitors under the application.

- Step 1** Log in to the MAS console. On the **Multi-Active Instances** page, click an instance to go to its console.
- Step 2** On the **Applications** tab page, click **Switch Over Monitor** in the row of a target application.
- Step 3** On the **Monitoring Status** tab page in the dialog box, click **Switch Over**.
- Step 4** Click **OK**.

If the target data center is abnormal but you have to switch over the monitor, select the checkbox to confirm the switchover, and click **OK**.

Figure 5-2 Switching over monitors



- Step 5** On the **Applications** tab page, click **Switch Over Monitor** in the row of the application. On the **Monitoring Status** tab page in the dialog box, click **Switch Back**.

----End

Modifying an Application

- Step 1** Log in to the MAS console. On the **Multi-Active Instances** page, click an instance to go to its console.
- Step 2** Go to the **Applications** tab page.
- Step 3** Click **Modify** in the row of a target application.
- Step 4** Enter the application information, then click **OK**.

----End

Deleting an Application

- Step 1** Log in to the MAS console. On the **Multi-Active Instances** page, click an instance to go to its console.
 - Step 2** Go to the **Applications** tab page.
 - Step 3** Click **Delete** in the row of a target application.
 - Step 4** Click **OK**.
- End

Deleting Multiple Applications

- Step 1** Log in to the MAS console. On the **Multi-Active Instances** page, click an instance to go to its console.
 - Step 2** Go to the **Applications** tab page and select the target applications.
 - Step 3** Click **Delete** in the upper left corner.
 - Step 4** Click **OK**.
- End

6 Monitor Management

[6.1 MySQL/Oracle/PostgreSQL Monitoring](#)

[6.2 Redis Monitoring](#)

[6.3 MongoDB Monitoring](#)

[6.4 Elasticsearch Monitoring](#)

[6.5 API Monitoring](#)

[6.6 General Monitor Operations](#)

[6.7 Global Configurations](#)

6.1 MySQL/Oracle/PostgreSQL Monitoring

Introduction

A MySQL/Oracle/PostgreSQL monitor detects your database status, and automatically triggers traffic switching when the database is abnormal.

This section describes these three monitors because they share the same operations.

Table 6-1 Monitoring status description

Monitoring Status	Description
Green	<p>The monitoring is normal.</p> <p>NOTE MAS cannot perform availability detection on the subhealth statuses of MySQL monitors, such as full connection and full disk usage.</p> <p>If the MySQL instance is active, the connection is normal, and the query command can be executed properly, the MySQL database and the monitor are normal.</p>

Monitoring Status	Description
Red	The monitoring is abnormal. Traffic switchover is automatically triggered (if enabled) when the status changes from normal to failed.
Yellow	The monitor initialization failed. The MAS process cannot detect the service database. In this case, confirm the configurations or contact O&M personnel.
Light gray	Monitor creation or configuration failed.
Dark gray	Invocation failed. The ETCD connection status is abnormal.

Creating a Monitor

- Step 1** Log in to the MAS console. On the **Multi-Active Instances** page, click an instance whose namespace type is **Intra-city multi-active**.
- Step 2** Click the **Monitor List** tab and click **Create Monitor**.
- Step 3** Configure the basic information, then click **Next: Data Centers**.

Figure 6-1 Basic information configurations

The screenshot shows the 'Basic' configuration step in the MAS console. At the top, there are five numbered tabs: 1 Basic, 2 Data Centers, 3 Databases, 4 Advanced, and 5 Confirm. The 'Basic' tab is active. The configuration items are as follows:

- Monitor:** A dropdown menu set to 'MySQL Monitoring'. To its right is a link: 'Enable More Function Point Oracle PostgreSQL API'.
- Application:** A dropdown menu set to '--Select--' with a refresh icon.
- Monitor Name:** A text input field containing 'mysql-qlyw1q5jo4'.
- Exception Notification:** A toggle switch set to 'Off'.
- Monitoring:** Radio buttons for 'Yes' (selected) and 'No'.
- Automatic Switchover:** Radio buttons for 'Yes' (selected) and 'No'.
- Username:** A text input field with the placeholder 'Enter a username.'
- Password:** A text input field with the placeholder 'Enter a password.' and a visibility icon.
- Confirm Password:** A text input field with the placeholder 'Enter the password again.' and a visibility icon.
- Associate with DRS:** A toggle switch set to 'Off'.

Table 6-2 Basic information parameters

Parameter	Description
Monitor	Select a monitor type. <ul style="list-style-type: none">• MySQL• Oracle• PostgreSQL Monitor NOTE Ensure that you have enabled the corresponding features in functions module settings, and have selected these features when creating the namespace for your instance. Otherwise, you will not see these options.
Application	Select the application.
Monitor Name	Customize the monitor name.
Exception Notification	By default, this option is disabled. If it is enabled, <ul style="list-style-type: none">• Monitor and database exceptions will be sent to you in a timely manner with the Huawei Cloud SMN service. Configure a secret key first.• Cloud Eye is enabled by default. Ensure that the alarm rules for MAS have been created on the Cloud Eye console. For details, see 8.3 Creating an Alarm Rule to Monitor an Event.
Subject	If Exception Notification is enabled, select a subject from the drop-down list or click Add to create a new one.
Monitoring	The default value is Yes . If No , database exceptions will not be monitored.
Automatic Switchover	The default value is Yes . If No , automatic switchover of the databases will not be triggered.
Username	Enter the username for logging in to the database.
Password	Enter the password for logging in to the database.
Confirm Password	Enter the password again.
Associate with DRS	By default, this option is disabled. If it is enabled, the Data Replication Service (DRS) real-time DR tasks will be associated. Configure a secret key before enabling this option.
Multi-Active Area	Select the multi-active area where the instance's namespace belongs to. NOTE This option is displayed only when Associate with DRS is enabled.

Parameter	Description
DRS Task	If Associate with DRS is enabled, select a real-time DR task from the drop-down list or click Add to create a new one.

Step 4 Configure the data centers, then click **Next: Databases**.

Figure 6-2 Data center configurations

The screenshot shows the 'Create Monitor' interface with the 'Data Centers' step selected. It features two sections, 'Data Center 1' and 'Data Center 2'. Each section contains three required fields: 'Cloud' (a dropdown menu), 'Region' (a dropdown menu), and 'IPv4 Address' (a text input with a 'Port' button next to it). Below each set of fields is a button labeled 'Add Read Database'. A progress bar at the top shows five steps: 1 Basic, 2 Data Centers (active), 3 Databases, 4 Advanced, and 5 Confirm.

Table 6-3 Data center parameters

Parameter	Description
Cloud	The environment where the monitored database is deployed
Region	The region where the monitored database is located
IPv4 Address	The IP address and port number for accessing the database
Add Read Database	Click to add the read database address.

Step 5 Configure the databases, then click **Next: Advanced**.

Figure 6-3 Database configurations

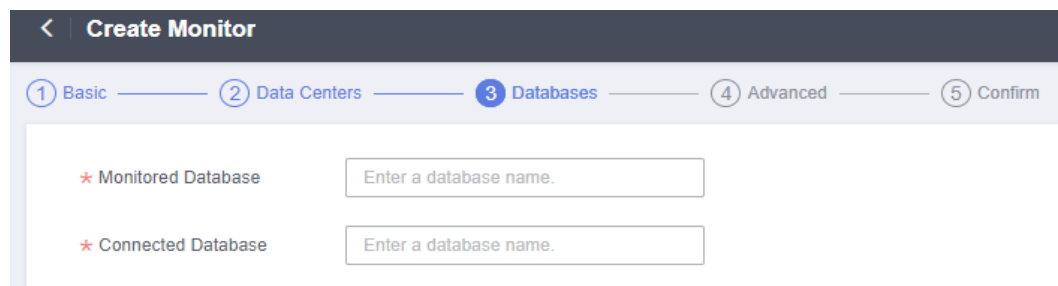


Table 6-4 Database parameters

Parameter	Description
Monitored Database	Enter the monitored database name.
Connected Database	Enter the connected database name.

Step 6 Configure the advanced settings, then click **Next: Confirm**.

Figure 6-4 Advanced configurations

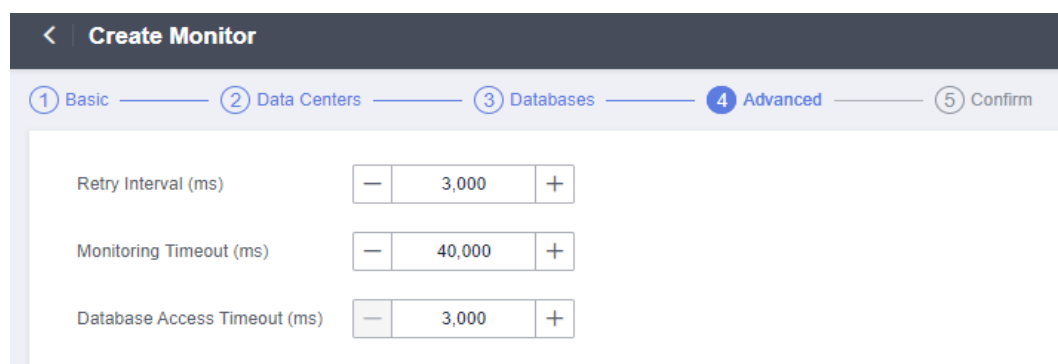


Table 6-5 Advanced settings

Parameter	Description
Retry Interval (ms)	The interval of reconnection attempts, in milliseconds. Default value (recommended): 3000 Value range: 1 to 300,000
Monitoring Timeout (ms)	The timeout duration before a monitor becomes abnormal, in milliseconds. Default value (recommended): 40,000; Value range: 1 to 600,000 NOTE Ensure that the time you specify here is longer than the time required for data center 1 to synchronize data to data center 2. Otherwise, the data in data center 2 may be incomplete.

Parameter	Description
Database Access Timeout (ms)	The database access timeout duration, over which the database access is considered failed, in milliseconds. Default value (recommended): 3000 Value range: 3000 to 100,000

Step 7 Confirm settings and click **Create**.

 **NOTE**

If the created monitor is not normal, that is, its indicator is not green, its configurations or databases may be abnormal. In this case, rectify the fault.

----End

Configuring the Connection Pool

Step 1 Log in to the MAS console. On the **Multi-Active Instances** page, click an instance to go to its console.

Step 2 Click the **Monitor List** tab and choose **More > Configure Connection Pool** in the row that contains the target monitor.

Step 3 Set the configurations and click **OK**.

Table 6-6 Connection pool parameters

Parameter	Description
Database Name	Enter the name of the connected database.
Routing Algorithm	Options: Single read/write and Single write, local read
Data Source	Customize a name for the data source.
Database Address	Connection address of the database
Schema	Name of the schema to be connected
Load Balancing Algorithm	Options: Random and Polling
Add Data Source	Configure the secondary/standby data source.

----End

Configuring the Database Read/Write

To disable the database to write, interconnect the application with the DB-SDK of the Java 1.2.6-RELEASE or later version.

Step 1 Log in to the MAS console. On the **Multi-Active Instances** page, click an instance to go to its console.

Step 2 Go to the **Monitor List** tab page.


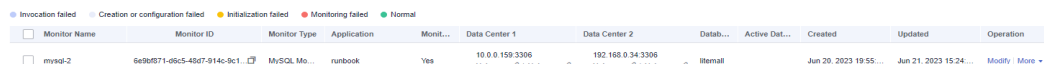
Step 3 Click  in the row of a data center.

Figure 6-5 Configuring the database read/write



Monitor Name	Monitor ID	Monitor Type	Application	Monit...	Data Center 1	Data Center 2	Datab...	Active Dat...	Created	Updated	Operation
mysql-2	6e2b071-d9c5-43d7-914c-9c1...	MySQL Mo...	runbook	Yes	10.0.0.159:3306 Unknown	192.168.0.34:3306 Unknown	Itemall		Jun 20, 2023 19:55...	Jun 21, 2023 15:24...	Modify More

Step 4 Select a new status and click **OK**.

Table 6-7 Database read/write parameters

Parameter	Description
Readable	Whether the database is readable. <ul style="list-style-type: none"> • Readable: The database status is normal and can be read. • Unreadable: The database status is abnormal and cannot be read. In this case, you need to change the database status.
Writable	Whether the database is writable. <ul style="list-style-type: none"> • Writable: You can write data to the database. • Unwritable: You cannot write data to the database.

NOTE

If DC 1 (active) is abnormal, MAS automatically sets DC 2 to active and sets DC 1 to **Unreadable**. If you need to set DC 1 to active after it recovers, you will need to click **Switch Back** and set DC 1 to **Readable**.

----End

6.2 Redis Monitoring

Introduction

A Redis monitor detects your database status, and automatically triggers traffic switching when the database is abnormal.

Table 6-8 Monitoring status description

Monitoring Status	Description
Green	The monitoring is normal.
Red	The monitoring is abnormal. Traffic switchover is automatically triggered (if enabled) when the status changes from normal to failed.
Yellow	The monitor initialization failed. The MAS process cannot detect the service database. In this case, confirm the configurations or contact O&M personnel.
Light gray	Monitor creation or configuration failed.
Dark gray	Invocation failed. The ETCD connection status is abnormal.

Creating a Redis Monitor

- Step 1** Log in to the MAS console. On the **Multi-Active Instances** page, click an instance whose namespace type is **Intra-city multi-active**.
- Step 2** Click the **Monitor List** tab and click **Create Monitor**.
- Step 3** Configure the basic information, then click **Next: Data Centers**.

Figure 6-6 Basic information configurations

The screenshot shows the 'Create Monitor' configuration interface. At the top, there is a navigation bar with a back arrow and the title 'Create Monitor'. Below the navigation bar is a progress indicator with four steps: 1 Basic (highlighted in blue), 2 Data Centers, 3 Advanced, and 4 Confirm. The main configuration area contains several fields, each with a red asterisk indicating it is required:

- Monitor:** A dropdown menu with 'Redis Monitoring' selected.
- Application:** A dropdown menu with 'runbook' selected.
- Monitor Name:** A text input field containing 'redis-r7w3okud51a'.
- Exception Notification:** A toggle switch currently set to 'Off'.
- Monitoring:** Radio buttons for 'Yes' (selected) and 'No'.
- Automatic Switchover:** Radio buttons for 'Yes' (selected) and 'No'.
- Routing Algorithm:** A dropdown menu with '-Select-' selected.
- Mode:** Radio buttons for 'Normal' (selected), 'Sentinel', and 'Cluster'.

Table 6-9 Basic information parameters

Parameter	Description
Monitor	Select Redis Monitoring .
Application	Select the application.
Monitor Name	Customize the monitor name.
Exception Notification	By default, this option is disabled. If it is enabled, monitor and database exceptions will be sent to you in a timely manner. To enable this option, configure a secret key first.
Subject	If Exception Notification is enabled, select a subject from the drop-down list or click Add to create a new one.
Monitoring	The default value is Yes . If No , database exceptions will not be monitored.
Automatic Switchover	The default value is Yes . If No , automatic switchover of the databases will not be triggered.
Routing Algorithm	Select Single read/write , Local read , asynchronous dual write , or Single read, asynchronous dual write as required.
Mode	Select Normal (default), Sentinel , or Cluster based on Redis deployment.

Step 4 Configure the data centers, then click **Next: Advanced**.

Figure 6-7 Data center configurations

Create Monitor

① Basic — ② Data Centers — ③ Advanced — ④ Confirm

Data Center 1

* Cloud

* Region

AZs

* Connection Address :

* Password

* Confirm Password

Data Center 2

* Cloud

* Region

AZs

* Connection Address :

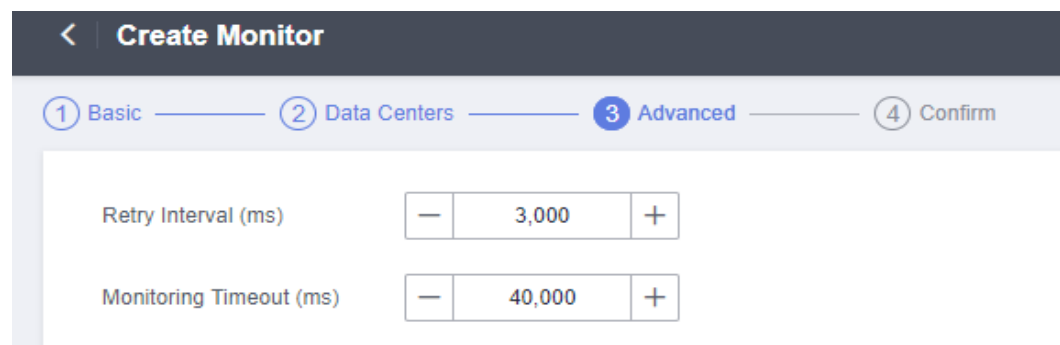
* Password

* Confirm Password

Table 6-10 Data center parameters

Parameter	Description
Cloud	Select the environment where the Redis databases are deployed. You can select a third-party data center for cross-cloud monitoring.
Region	Select the region where the Redis databases are deployed.
AZs	Set this parameter for data centers 1 and 2 based on the AZs where the Redis databases are deployed.
Connection Address	Enter the connection address and port of the monitored Redis database.
Password	Enter the password of the monitored Redis database.
Confirm Password	Enter the password again.

Step 5 Configure the advanced settings, then click **Next: Confirm**.

Figure 6-8 Advanced configurations**Table 6-11** Advanced settings

Parameter	Description
Retry Interval (ms)	The interval of reconnection attempts, in milliseconds. Default value (recommended): 3000 Value range: 1 to 300,000
Monitoring Timeout (ms)	The timeout duration before a monitor becomes abnormal, in milliseconds. Default value (recommended): 40,000; Value range: 1 to 600,000 NOTE Ensure that the time you specify here is longer than the time required for data center 1 to synchronize data to data center 2. Otherwise, the data in data center 2 may be incomplete.

Step 6 Confirm settings and click **Create**.

 **NOTE**

If the created monitor is not normal, that is, its indicator is not green, its configurations or databases may be abnormal. In this case, rectify the fault.

----End

6.3 MongoDB Monitoring

Introduction

A MongoDB monitor detects your database status, and automatically triggers traffic switching when the database is abnormal.

Table 6-12 Monitoring status description

Monitoring Status	Description
Green	The monitoring is normal.
Red	The monitoring is abnormal. Traffic switchover is automatically triggered (if enabled) when the status changes from normal to failed.
Yellow	The monitor initialization failed. The initial detection fails when the monitor starts. In this case, confirm the configurations or contact O&M personnel.
Light gray	Monitor creation or configuration failed
Dark gray	Invocation failed. The ETCD connection status is abnormal.

Creating a MongoDB Monitor

- Step 1** Log in to the MAS console. On the **Multi-Active Instances** page, click an instance to go to its console.
- Step 2** Click the **Monitor List** tab, and click **Create Monitor**.
- Step 3** Configure the basic information, then click **Next: Data Centers**.

Figure 6-9 Basic information configurations

Table 6-13 Basic information parameters

Parameter	Description
Monitor	Select MongoDB Monitoring .
Application	Select the application.
Monitor Name	Customize the monitor name.
Exception Notification	By default, this option is disabled. If it is enabled, <ul style="list-style-type: none"> monitor and database exceptions will be sent to you in a timely manner with the Huawei Cloud SMN service. Configure a secret key first. Cloud Eye is enabled by default. Ensure that the alarm rules for MAS have been created on the Cloud Eye console. For details, see 8.3 Creating an Alarm Rule to Monitor an Event.
Subject	If Exception Notification is enabled, select a subject from the drop-down list or click Add to create a new one.
Monitoring	The default value is Yes . If No , database exceptions will not be monitored.
Automatic Switchover	The default value is Yes . If No , automatic switchover of the databases will not be triggered.
Username	Enter the username for logging in to the database.
Password	Enter the password for logging in to the database.

Step 4 Configure the data centers, then click **Next: Databases**.

Figure 6-10 Data center configurations

The screenshot shows the 'Create Monitor' interface with a progress bar at the top indicating five steps: 1 Basic, 2 Data Centers (current), 3 Databases, 4 Advanced, and 5 Confirm. Below the progress bar, there are two sections for configuring data centers. Each section, labeled 'Data Center 1' and 'Data Center 2', contains the following fields:

- Cloud:** A dropdown menu with 'Huawei Cloud' selected.
- Region:** A dropdown menu with 'CN-Hong Kong' selected.
- Connection Address:** A text input field for an IP address (format: . . .) followed by a colon and a 'Port' input field.
- Add Connection Address:** A button with a plus icon and a circular arrow.

Table 6-14 Data center parameters

Parameter	Description
Cloud	The environment where the monitored MongoDB database is deployed
Region	The region where the monitored database is located
Connection Address	The IP address and port number for accessing the MongoDB database

Step 5 Configure the databases, then click **Next: Advanced**.

Figure 6-11 Database configurations



Table 6-15 Database parameters

Parameter	Description
Monitored Database	Enter the monitored database name.
Connected Database	Enter the connected database name. CAUTION The names of the Monitored Database and Connected Database should be the same, and the specified database must exist in the monitored data source.

Step 6 Configure the advanced settings, then click **Next: Confirm**.

Figure 6-12 Advanced configurations

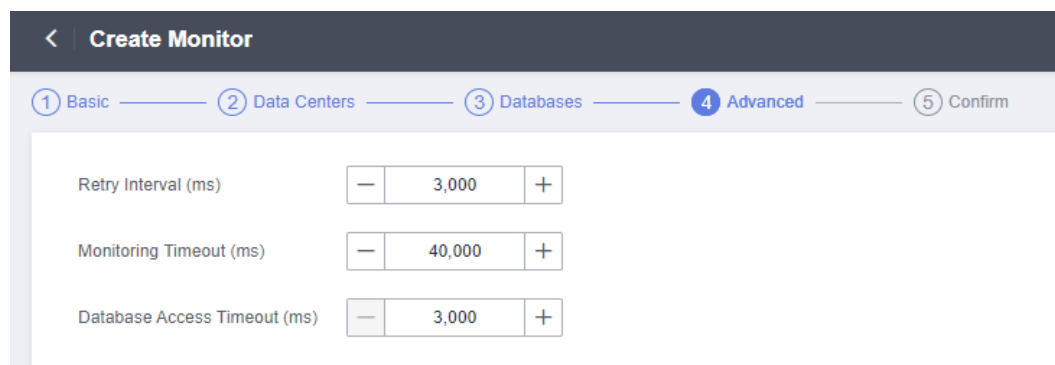


Table 6-16 Advanced settings

Parameter	Description
Retry Interval (ms)	The interval of reconnection attempts, in milliseconds. Default value (recommended): 3000 Value range: 1 to 300,000

Parameter	Description
Monitoring Timeout (ms)	The timeout duration before a monitor becomes abnormal, in milliseconds. Default value (recommended): 40,000; Value range: 1 to 600,000 NOTE Ensure that the time you specify here is longer than the time required for data center 1 to synchronize data to data center 2. Otherwise, the data in data center 2 may be incomplete.
Database Access Timeout (ms)	The database access timeout duration, over which the database access is considered failed, in milliseconds. Default value (recommended): 3000 Value range: 3000 to 100,000

Step 7 Confirm settings and click **Create**.

NOTE

If the created monitor is not normal, that is, its indicator is not green, its configurations or databases may be abnormal. In this case, rectify the fault.

----End

Connection pool parameters

- Step 1** Log in to the MAS console. On the **Multi-Active Instances** page, click an instance to go to its console.
- Step 2** Click the **Monitor List** tab and choose **More > Configure Connection Pool** in the row that contains the target monitor.
- Step 3** Set the configurations and click **OK**.

Figure 6-13 Connection pool configurations

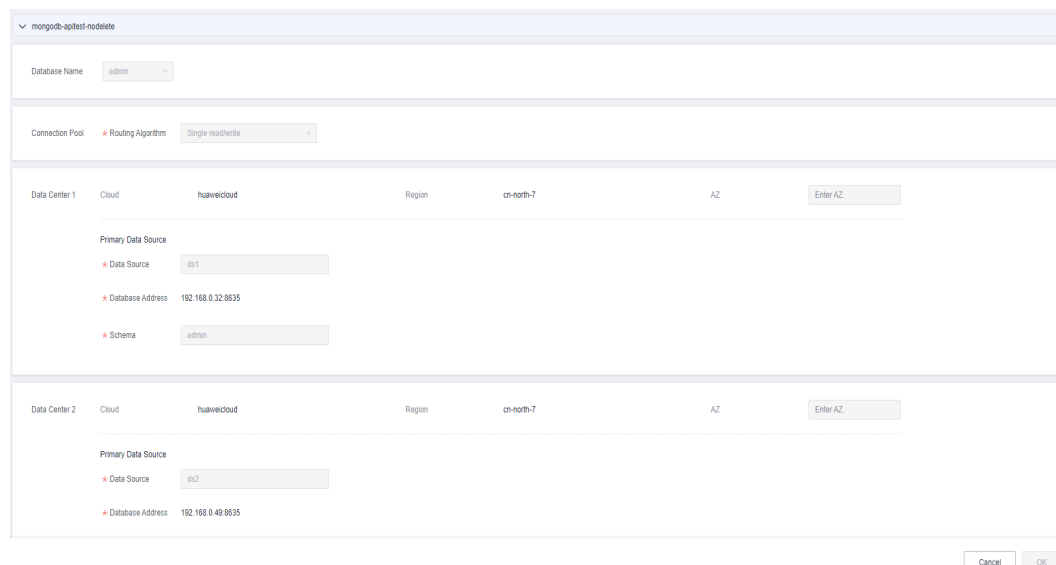


Table 6-17 Connection pool parameters

Parameter	Description
Database Name	Enter the name of the connected MongoDB database.
Routing Algorithm	Options: Single read/write and Single write, local read
AZs	Set this parameter for data centers 1 and 2 based on the AZs where the MongoDB databases are deployed.
Data Source	Customize a name for the data source.
Database Address	Connection address of the MongoDB database
Schema	Name of the schema to be connected

----End

6.4 Elasticsearch Monitoring

Introduction

An Elasticsearch monitor detects your database status, and automatically triggers traffic switching when the database is abnormal.

Table 6-18 Monitoring status description

Monitoring Status	Description
Green	The monitoring is normal.
Red	The monitoring is abnormal. Traffic switchover is automatically triggered (if enabled) when the status changes from normal to failed.
Yellow	The monitor initialization failed. The initial detection fails when the monitor starts. In this case, confirm the configurations or contact O&M personnel.
Light gray	Monitor creation or configuration failed
Dark gray	Invocation failed. The ETCD connection status is abnormal.

Creating an Elasticsearch Monitor

Step 1 Log in to the MAS console. On the **Multi-Active Instances** page, click an instance to go to its console.

Step 2 Click the **Monitor List** tab, and click **Create Monitor**.

Step 3 Configure the basic information, then click **Next: Data Centers**.

Figure 6-14 Basic information configurations

The screenshot shows the 'Create Monitor' configuration interface. At the top, there is a navigation bar with a back arrow and the title 'Create Monitor'. Below the navigation bar is a progress indicator with four steps: 1 Basic (selected), 2 Data Centers, 3 Advanced, and 4 Confirm. The main configuration area contains several fields, each with a red asterisk indicating it is required:

- Monitor:** A dropdown menu set to 'Elasticsearch Monitoring'. To its right is a link: 'Enable More Function Point Oracle PostgreSQL API'.
- Application:** A dropdown menu set to 'runbook'. To its right is a plus icon: '+ C'.
- Monitor Name:** A text input field containing 'elasticsearch-54on9sknvm'.
- Exception Notification:** A toggle switch set to 'Off'.
- Monitoring:** Radio buttons for 'Yes' (selected) and 'No'.
- Automatic Switchover:** Radio buttons for 'Yes' (selected) and 'No'.
- Routing Algorithm:** A dropdown menu set to '--Select--'.

Table 6-19 Basic information parameters

Parameter	Description
Monitor	Select Elasticsearch Monitoring .
Application	Select the application.
Monitor Name	Customize the monitor name.
Exception Notification	By default, this option is disabled. If it is enabled, <ul style="list-style-type: none">monitor and database exceptions will be sent to you in a timely manner with the Huawei Cloud SMN service. Configure a secret key first.Cloud Eye is enabled by default. Ensure that the alarm rules for MAS have been created on the Cloud Eye console. For details, see 8.3 Creating an Alarm Rule to Monitor an Event.
Subject	If Exception Notification is enabled, select a subject from the drop-down list or click Add to create a new one.
Monitoring	The default value is Yes . If No , database exceptions will not be monitored.
Automatic Switchover	The default value is Yes . If No , automatic switchover of the databases will not be triggered.

Parameter	Description
Routing Algorithm	Option: Single read/write

Step 4 Configure the data centers, then click **Next: Advanced**.

Figure 6-15 Data center configurations

The screenshot shows the 'Create Monitor' configuration interface. It has four steps: 1 Basic, 2 Data Centers (active), 3 Advanced, and 4 Confirm. Two data center configurations are visible:

- Data Center 1:**
 - Cloud: Huawei Cloud
 - Region: CN-Hong Kong
 - AZs: Enter AZs.
 - Connection Address: [IP Address] : Port
 - Add Connection Address: [Add]
 - Username: Enter a username.
 - Protocol: HTTPS HTTP
 - Password: Enter a password.
 - Confirm Password: Enter the password again.
- Data Center 2:** (Identical configuration to Data Center 1)

Table 6-20 Data center parameters

Parameter	Description
Cloud	The environment where the monitored Elasticsearch database is deployed
Region	The region where the monitored Elasticsearch database is deployed
AZs	Set this parameter for data centers 1 and 2 based on the AZs where the Elasticsearch databases are deployed.

Parameter	Description
Connection Address	The IP address and port number for accessing the Elasticsearch database
Add Connection Address	You can add more connection addresses.
Username	Enter the username for logging in to the Elasticsearch database. CAUTION To prevent risks, it is recommended to use a username that is different from your service username and has been granted only the read permissions.
Protocol	Options: HTTPS and HTTP
Password	Enter the password of the monitored Elasticsearch database.
Confirm Password	Enter the password again.

⚠ CAUTION

MAS supports Elasticsearch 7.10.2 and later. Ensure that the password is correct, otherwise, the data source will be locked for 15 minutes.

Step 5 Configure the advanced settings, then click **Next: Confirm**.

Figure 6-16 Advanced configurations

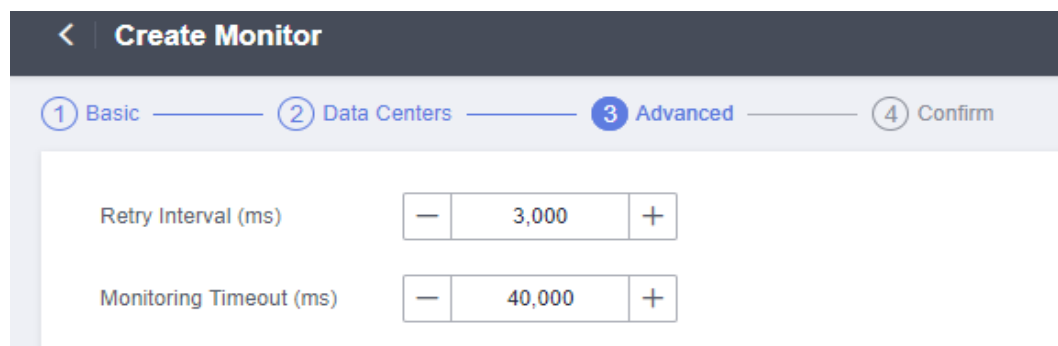


Table 6-21 Advanced settings

Parameter	Description
Retry Interval (ms)	The interval of reconnection attempts, in milliseconds. Default value (recommended): 3000 Value range: 1 to 300,000

Parameter	Description
Monitoring Timeout (ms)	The timeout duration before a monitor becomes abnormal, in milliseconds. Default value (recommended): 40,000; Value range: 1 to 600,000 NOTE Ensure that the time you specify here is longer than the time required for data center 1 to synchronize data to data center 2. Otherwise, the data in data center 2 may be incomplete.

Step 6 Confirm settings and click **Create**.

 **NOTE**

If the created monitor is not normal, that is, its indicator is not green, its configurations or databases may be abnormal. In this case, rectify the fault.

----End

6.5 API Monitoring

Introduction

API monitors monitor the API gateway of your service, and control the resolution result of the DNS entry based on the availability of API gateway.

Table 6-22 Monitoring status description

Monitoring Status	Description
Green	The monitoring is normal.
Red	The monitoring is abnormal. Traffic switchover is automatically triggered when the status changes from normal to failed.
Yellow	The monitor initialization failed. The MAS process cannot detect the service API. In this case, confirm the configurations or contact O&M personnel.
Light gray	Monitor creation or configuration failed.
Dark gray	Invocation failed. The ETCD connection status is abnormal.

Creating an API Monitor

Step 1 Log in to the MAS console. On the **Multi-Active Instances** page, click an instance whose namespace type is **Intra-city multi-active**.

Step 2 Click the **Monitor List** tab and click **Create Monitor**.

Step 3 Configure the basic information, then click **Next: Data Centers**.

Figure 6-17 Basic information configurations

Table 6-23 Basic information parameters

Parameter	Description
Monitor	Select API Monitoring .
Application	Select the application.
Monitor Name	Customize the monitor name.
Exception Notification	By default, this option is disabled. If it is enabled, <ul style="list-style-type: none"> Monitor and API exceptions will be sent to you in a timely manner with the Huawei Cloud SMN service. Configure a secret key first. Cloud Eye is enabled by default. Ensure that the alarm rules for MAS have been created on the Cloud Eye console. For details, see 8.3 Creating an Alarm Rule to Monitor an Event.
Subject	If Exception Notification is enabled, select a subject from the drop-down list or click Add to create a new one.
Monitoring	The default value is Yes . If you select No , the API gateway status will not be monitored.

Step 4 Configure the data centers, then click **Next: Advanced**.

Figure 6-18 Data center configurations

Table 6-24 Data center parameters

Parameter	Description
Cloud	Select the environment where the monitored API gateway is deployed.
Region	Select the regions of the API gateways.
Connection Address	Select HTTP or HTTPS , and enter the connection address of the API gateway.
Request path	Health check path of the API gateway.
Request Methods	Select GET , POST , DELETE , PATCH , or PUT .
Status Code	Set this parameter based on the actual requirements of the monitored API gateway, for example, 200.
Request Header	Set this parameter based on the actual requirements of the monitored API gateway. Encrypt the request header if it contains sensitive information.

Step 5 Configure the advanced settings, then click **Next: Confirm**.

Figure 6-19 Advanced configurations

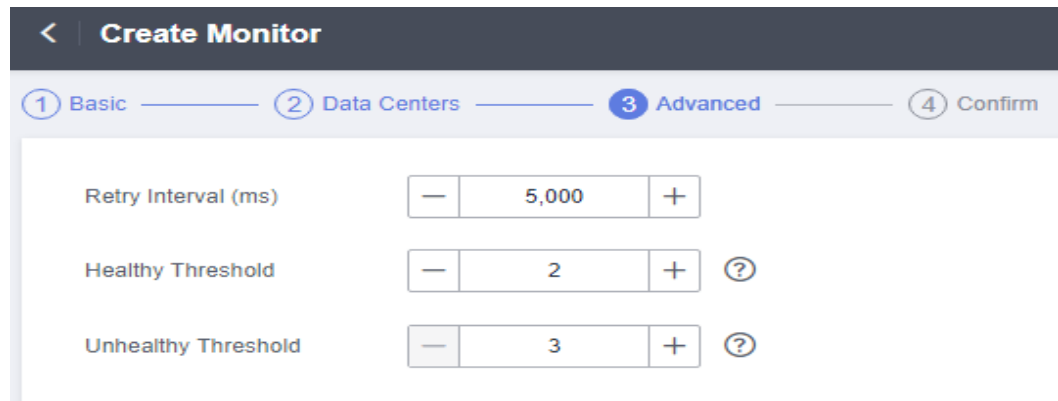


Table 6-25 Advanced settings

Parameter	Description
Retry Interval (ms)	The interval of reconnection attempts, in milliseconds. Default value (recommended): 5000 Value range: 1 to 300,000
Healthy Threshold	If the number of successful consecutive API connections reaches or exceeds the threshold, the API connection is normal. NOTE Default value (recommended): 2; Value range: 1 to 5
Unhealthy Threshold	If the number of consecutive API connection failures reaches or exceeds the threshold, the API connection is abnormal. NOTE Default value (recommended): 3; Value range: 3 to 10

Step 6 Confirm settings and click **Create**.

NOTE

If the created monitor is not normal, that is, its indicator is not green, its configurations or APIs may be abnormal. In this case, rectify the fault.

----End

6.6 General Monitor Operations

6.6.1 Configuring Monitors

This section describes how to configure parameters for all monitors under an instance.

Note that these configurations will not change the **Advanced** settings configured in monitor creation.

Procedure

- Step 1** Log in to the MAS console. On the **Multi-Active Instances** page, click an instance to go to its console.
- Step 2** Click the **Monitor List** tab and click **Configure Monitoring**.
- Step 3** Configure the parameters and click **OK**. You are advised to retain the default settings.

Table 6-26 Monitoring configurations

Parameter	Description
Monitor Type	The type of the monitor to be configured. Only monitors created under the instance are displayed.
Monitoring Timeout (ms)	The timeout duration before a monitor becomes abnormal, in milliseconds. Value range: 4000 to 400,000
Retry Interval (ms)	Retry Interval (ms) Value range: 2000 to 30,000
Database Access Timeout (ms)	This is required only for MySQL, Oracle, PostgreSQL, and MongoDB monitors. The database access timeout duration, over which the database access is considered failed. Value range: 3000 to 100,000
Healthy Threshold	How many workers are required to confirm the database health. For example, 1 indicates that as long as one worker in the monitoring cluster detects the database, the detection is considered successful. If the detection fails, the leader will handle the fault. Enter 1 or 2. NOTE For API monitors, only Healthy Threshold needs to be configured.

----End

6.6.2 Obtaining the SDK Access Configuration

This section describes how to obtain the SDK access configuration. For details about how to reference the SDK, see *MAS Developer Guide*.

Procedure

- Step 1** Log in to the MAS console. On the **Multi-Active Instances** page, click an instance to go to its console.
- Step 2** Click the **Monitor List** tab, choose **More > SDK Access Configuration** in the row that contains the target monitor.

NOTE

The SDK access configuration is not applicable to API monitors.

Step 3 In the dialog box that is displayed, click next to **Copy parameters**.

----End

6.6.3 Switching a Monitor

This section describes how to switch monitors. It is not recommended to switch from data center 1 to 2 if there are no exceptions.

Procedure

Step 1 Log in to the MAS console. On the **Multi-Active Instances** page, click an instance to go to its console.

Step 2 Go to the **Applications** tab page, click **Switch Over Monitor**, and click **Switch Over** on the **Monitoring Status** page.

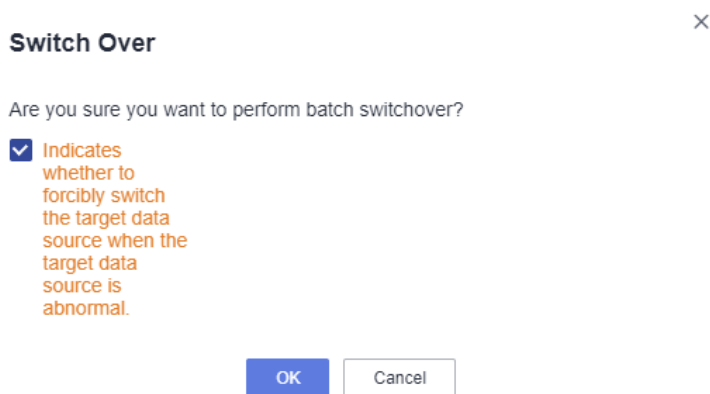
NOTE

You cannot perform switchovers on API monitors.

Step 3 Click **OK**.

If the target data center is abnormal but you have to switch over the monitor, select the checkbox to confirm the switchover, and click **OK**.

Figure 6-20 Switching a monitor by force

**NOTE**

- When the service database is abnormal, the automatic switchover will be triggered and take 10 seconds to complete. During this period, services may be interrupted.
- After data center 1 recovers, click **Switch Back** in the row that contains the target monitor.
- If DC 1 (active) is abnormal, MAS automatically sets DC 2 to active. However, MAS will not perform automatic switchover if DC 2 is active and becomes abnormal.

----End

6.6.4 Modifying a Monitor

This section describes how to modify the monitored database information. Note that you cannot modify the monitor type, application name, and monitor name using this method.

Procedure

- Step 1** Log in to the MAS console. On the **Multi-Active Instances** page, click an instance to go to its console.
- Step 2** Go to the **Monitor List** tab page.
- Step 3** Click **Modify** in the row that contains the target monitor.
- Step 4** Modify the monitor information and click **OK**.

----End

6.6.5 Deleting a Monitor

This section describes how to delete monitors.

Deleting a Monitor

- Step 1** Log in to the MAS console. On the **Multi-Active Instances** page, click an instance to go to its console.
- Step 2** Go to the **Monitor List** tab page.
- Step 3** Choose **More > Delete** in the row containing a monitor.
- Step 4** Click **OK** to delete the monitor.

NOTE

For an API monitor, click **Delete** directly.

----End

Deleting Monitors

- Step 1** Log in to the MAS console. On the **Multi-Active Instances** page, click an instance to go to its console.
- Step 2** Go to the **Monitor List** tab page.
- Step 3** Select the monitors to be deleted.
- Step 4** Click **Delete**.
- Step 5** Click **OK**.

----End

6.7 Global Configurations

The following sections describe how to configure secret keys, notifications, and DC-level switchovers.

6.7.1 Configuring a Secret Key

Adding a Secret Key

- Step 1** Log in to the MAS console. On the **Multi-Active Instances** page, click an instance whose namespace type is **Intra-city multi-active**.
- Step 2** Click the **Global** tab.
- Step 3** On the **Secret Keys** page, click **Add Secret Key**.
- Step 4** Configure information and click **OK**.

Figure 6-21 Secret key configurations

Table 6-27 Secret key parameters

Parameter	Description
Cloud	Select the environment where the SMN service is deployed.
AK	Access key ID.
SK	Secret access key.

 NOTE

Refer to [Access Keys](#) to obtain an AK/SK.

----End

Modifying a Secret Key

Step 1 Log in to the MAS console. On the **Multi-Active Instances** page, click an instance to go to its console.

Step 2 Click the **Global** tab.

Step 3 On the **Secret Keys** page, click **Modify** in the row that contains the target secret key.

Step 4 Modify the secret key information, and click **OK**.

----End

Deleting a Secret Key

Step 1 Log in to the MAS console. On the **Multi-Active Instances** page, click an instance to go to its console.

Step 2 Click the **Global** tab.

Step 3 On the **Secret Keys** page, click **Delete** in the row that contains the target secret key.

Step 4 Click **OK** to delete the secret key.

----End

6.7.2 Configuring a Notification

Creating a Notification

Step 1 Log in to the MAS console. On the **Multi-Active Instances** page, click an instance whose namespace type is **Intra-city multi-active**.

Step 2 Click the **Global** tab.

Step 3 On the **Notifications** page, click **Create Notification**.

Step 4 Enter the notification information, then click **OK**.

Figure 6-22 Notification configurations

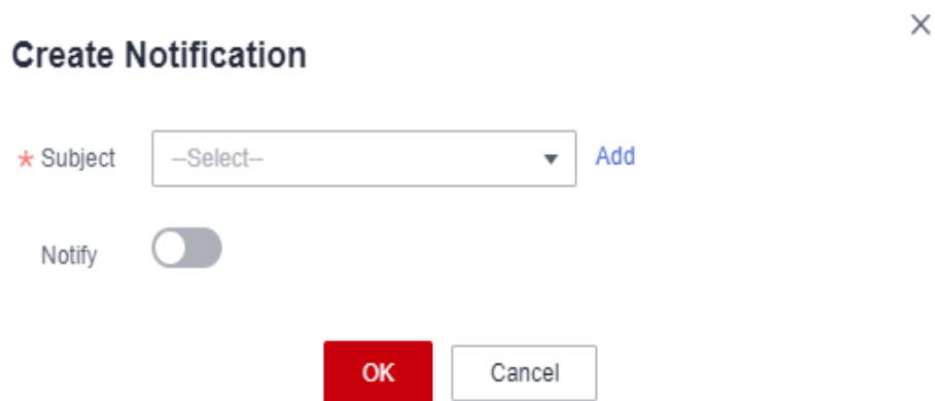


Table 6-28 Notification parameters

Parameter	Description
Subject	Select a notification subject or click Add to create one.
Notify	Specify whether to enable notification.

NOTE

For details about how to create an SMN subject, see [Publishing a JSON Message](#).

----End

Creating an SMN Subject

- Step 1** Log in to the MAS console. On the **Multi-Active Instances** page, click an instance to go to its console.
- Step 2** Click the **Global** tab.
- Step 3** On the **Notifications** page, click **Create Notification**.
- Step 4** Click **Add** to create a subject.

For details about how to create an SMN subject, see [Publishing a JSON Message](#).

----End

Modifying a Notification

- Step 1** Log in to the MAS console. On the **Multi-Active Instances** page, click an instance to go to its console.
- Step 2** Click the **Global** tab.
- Step 3** On the **Notifications** page, click **Modify** in the row that contains the target notification.

Step 4 Modify the notification information, and click **OK**.

----End

Deleting a Notification

Step 1 Log in to the MAS console. On the **Multi-Active Instances** page, click an instance to go to its console.

Step 2 Click the **Global** tab.

Step 3 On the **Notifications** page, click **Delete** in the row that contains the target notification.

Step 4 Click **OK** to delete the notification.

----End

6.7.3 Configuring DC-level Switchover

This section describes how to configure the automatic switchover setting. If this function is enabled, switchovers between data centers will be automatically triggered if MAS is abnormal, for example, when split-brain occurs or the active data center is faulty.

Configuring DC-level Switchover

Step 1 Log in to the MAS console. On the **Multi-Active Instances** page, click an instance to go to its console.

Step 2 Click the **Global** tab.

Step 3 On the **DC Switchover** page, toggle the switch as required.

- **Disabled:** If the data sources are normal but split-brain occurs or an active DC is faulty, monitors under the instance will not switch over automatically. This prevents unnecessary switchovers.
- **Enabled:** If split-brain occurs, an active DC is faulty, or a data source is abnormal, monitors under the instance will switch over automatically.

NOTE

- Split-brain refers to the situation where more than one master brain exists in an HA cluster due to network problems. When split-brain occurs in a cluster, data between clusters may be inconsistent, affecting arbitration of monitoring results.
- When split-brain occurs or an active DC is faulty, all monitors under the MAS instance will switch over. When a data source is faulty, only the corresponding monitor will switch over.
- Automatic switchover can also be enabled during monitor creation.

Step 4 Click **OK**.

----End

7 Credential Management

Introduction

MAS can manage, query, and access Huawei Cloud resources across accounts with an IAM agency or AK/SK.

Creating a Credential

- Step 1** Log in to the MAS console, go to the the **Credential Management** page, and click **Create Credential**.
- Step 2** Configure the credential.

Figure 7-1 Creating a credential

Table 7-1 Credential parameters

Parameter	Description
Name	Customize a credential name.
Cloud	Select Huawei Cloud .
Credential Type	Options: <ul style="list-style-type: none"> • IAM agency • IAM AK/SK
Delegating Account	This is required if Credential Type is set to IAM agency .

Parameter	Description
Delegate Name	This is required if Credential Type is set to IAM agency . If no agency is available, create an agency by referring to Creating an Agency (by a Delegating Party) .
AK	This is required if Credential Type is set to IAM AK/SK . For details, see Access Keys .
SK	This is required if Credential Type is set to IAM AK/SK .
Enterprise Project	Select an enterprise project.
Description	Enter the description information.

Step 3 Click **Validate Credential**. If the validation fails, check the configurations.

Step 4 Click **OK**.

----End

Deleting a Credential

Step 1 Log in to the MAS console and go to the **Credential Management** page.

Step 2 Click **Delete** in the row that contains a target credential.

Step 3 Click **OK** to delete the credential.

----End

Application Scenarios

Others can create an agency to delegate their resource management permissions to you. In this way, you can create a credential on MAS based on the agency, and use the credential to query and invoke resources under other accounts.

The following uses Account A (you) and Account B (another user) as an example:

1. Account B creates an agency, then grants permissions of IAM and RDS to Account A. For account security, it is recommended to grant only the permissions required (minimum permissions) to agencies. For details, see [Creating an Agency \(by a Delegating Party\)](#).

– The minimum permissions required by IAM:

```
{
  "Version": "1.1",
  "Statement": [{
    "Action": [
      "iam:projects:listProjects"
    ],
    "Effect": "Allow"
  }]
}
```


- The minimum permissions required by RDS:

```
{
  "Version": "1.1",
  "Statement": [{
    "Action": [
      "rds:instance:list"
    ],
    "Effect": "Allow"
  }]
}
```

2. Account A creates a credential by referring to [Creating a Credential](#), sets **Credential Type** to **IAM agency**, and configures the **Delegating Account** and **Delegate Name** as set in [1](#).
3. Account A [creates a namespace](#). The **Default Credential** of the primary multi-active area is **Current Account Credential** and the **Default Credential** of the secondary multi-active area is the credential created in [2](#).
4. Account A then does as follows to obtain Account B's RDS resources: perform the steps described in [Creating a Data Source](#), set **Deployment Mode** to the secondary multi-active area created in [3](#), set **Mode** to **RDS**, and confirm that the **Credential** is the one created in [2](#).
5. IAM users under Account A can be granted permissions to operate resources under Account B. For details, see [10 Permissions Management](#).

```
{
  "Version": "1.1",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "iam:tokens:assume"
    ]
  }]
}
```

8 Event Monitoring

- [8.1 Introduction to Event Monitoring](#)
- [8.2 Viewing Event Monitoring Graphs](#)
- [8.3 Creating an Alarm Rule to Monitor an Event](#)
- [8.4 Events Supported by Event Monitoring](#)

8.1 Introduction to Event Monitoring

Introduction

Cloud Eye provides you insights in cloud service running and metrics, and allows you to create alarm rules for the monitoring metrics.

After you enable MAS, Cloud Eye automatically associates with MAS monitoring metrics to help you understand the running status of MAS.

Enabling Cloud Eye

Cloud Eye is enabled by default.

For details about how to view MAS monitoring metrics, see [Querying Cloud Service Monitoring Metrics](#).

You can create an alarm rule to send an alarm notification when the monitoring data meets the specified conditions. For details, see [Creating an Alarm Rule](#).

8.2 Viewing Event Monitoring Graphs

Scenario

This section describes how to view the event monitoring data.

Procedure

1. Log in to the management console.
2. Choose **Service List > Cloud Eye**.
3. In the navigation pane on the left, click **Event Monitoring**.
4. On the displayed page, all system and custom events of the last 24 hours are displayed by default.
5. Locate the target event and click **View Graph** in the **Operation** column to view its graph.

8.3 Creating an Alarm Rule to Monitor an Event

Scenario

This section describes how to create an alarm rule to monitor an MAS event.

Procedure

1. Log in to the management console.
2. Choose **Service List > Cloud Eye**.
3. In the navigation pane on the left, click **Event Monitoring**.
4. On the event list page, click **Create Alarm Rule** in the upper right corner.
5. Configure the alarm rule name, alarm policy, and alarm notification as prompted.
 - **Alarm Type:** Select **Metric** or **Event**.
 - **Event Type:** Select **System event**.
 - **Event Source:** Select **Multi-Site High Availability Service**.

Figure 8-1 Creating an alarm rule

The screenshot displays the 'Create Alarm Rule' configuration interface. At the top, there is a dark header with a back arrow and the title 'Create Alarm Rule'. Below the header, the form is organized into several sections. The first section contains a text input field for 'Name' with the value 'alarm-guup' and a larger text area for 'Description' which is currently empty. The second section contains four configuration items, each with a red asterisk indicating a required field: 'Alarm Type' is set to 'Event' (highlighted in blue); 'Event Type' has two radio buttons, with 'System event' selected; 'Event Source' is a dropdown menu showing 'Multi-Site High Availability Service'; and 'Monitoring Scope' is set to 'All resources' (highlighted in blue). A small question mark icon is visible next to the Event Source dropdown.

For details about other parameters, see [Creating an Alarm Rule to Monitor an Event](#). After the alarm rule is created, when the event monitoring metric triggers the specified alarm policy, Cloud Eye will immediately notify you of cloud resource exceptions through SMN to avoid losses.

8.4 Events Supported by Event Monitoring

Table 8-1 MAS events

Source	Name	Severity	Description	Solution	Impact
MAS	Abnormal database	Critical	Abnormal relational database is detected by the MAS MySQL/Oracle/PostgreSQL monitor.	On the MAS console, click Multi-Active Instances , choose an instance, and check event MySQL/Oracle/PostgreSQL details and rectify the faults.	Data in the relational database may be lost.
MAS	Database recovered	Major	The relational database is recovered, detected by the MySQL/Oracle/PostgreSQL monitor.	None	None
MAS	Abnormal Redis database	Critical	Abnormal Redis database is detected by the MAS Redis monitor.	On the MAS console, click Multi-Active Instances , choose an instance, and view Redis event details and rectify the faults.	Data in the Redis database may be lost.
MAS	Redis database recovered	Major	The Redis database is recovered.	None	None

Source	Name	Severity	Description	Solution	Impact
MAS	Abnormal MongoDB database	Critical	Abnormal MongoDB database is detected by the MAS MongoDB monitor.	On the MAS console, click Multi-Active Instances , choose an instance, and view MongoDB event details and rectify the faults.	Data in the MongoDB database may be lost.
MAS	MongoDB database recovered	Major	The MongoDB database is recovered.	None	None
MAS	Abnormal Elasticsearch	Critical	Abnormal Elasticsearch database is detected by the MAS Elasticsearch monitor.	On the MAS console, click Multi-Active Instances , choose an instance, and view Elasticsearch event details and rectify the faults.	The Elasticsearch instance may be unavailable.
MAS	Elasticsearch instance recovered	Major	The Elasticsearch database is recovered.	None	None
MAS	Abnormal API	Critical	Abnormal API or unexpected response code is detected by the MAS API monitor.	On the MAS console, click Multi-Active Instances , choose an instance, and view API event details and rectify the faults.	API data in the database may be lost.
MAS	API recovered	Major	The API is recovered.	None	None
MAS	Area status changed	Major	Area status changes are detected by MAS.	On the MAS console, click Multi-Active Instances , choose an instance, and view multi-active area event details and rectify the faults.	Network of the multi-active areas may change.

9 Audit Logs

Introduction

You can use Cloud Trace Service (CTS) to record key operation events related to MAS. The events can be used in various scenarios such as security analysis, compliance audit, resource tracing, and problem locating.

After you enable CTS, the system starts to record MAS operations. CTS stores operation records from the last seven days.

Enabling CTS

For details about how to enable CTS, see [Enabling CTS](#).

After CTS is enabled, if you want to view MAS operation events, see [Querying Real-Time Traces](#).

MAS Operations Supported by CTS

Table 9-1 MAS operations that can be supported by CTS.

Operation	Resource Type	Trace Name
Creating a Namespace	namespace	createNamespace
Modifying a Namespace	namespace	updateNameSpace
Deleting a Namespace	namespace	deleteNameSpace
Creating a Data Source	dataSource	createDataSource
Editing a Data Source	dataSource	updateDataSource
Deleting a Data Source	dataSource	deleteDataSource
Creating a Sync Link	dataSync	createDataSyncTask
Deleting a Sync Link	dataSync	deleteDataSyncTask
Create Instance	instance	createInstance

Operation	Resource Type	Trace Name
Deploying an Instance	instance	deployInstance
Deleting an Instance	instance	deleteInstance
Upgrading an Instance	instance	internalUpgradeInstance
Creating an Application	application	createApplication
Updating an Application	application	updateApplication
Deleting an Application	application	deleteApplication
Deleting Monitors	application	batchSwitchMonitor
Creating a Monitor	monitor	createMonitor
Updating a Monitor	monitor	updateMonitor
Deleting a Monitor	monitor	deleteMonitor
Configuring Global Settings	monitor	setMonitorGlobalConfig
Switching Over Monitors	monitor	switchMonitor
Creating a Connection Pool	monitor	createDBConnectionPool
Updating a Connection Pool	monitor	updateDBConnectionPool
Resetting Equipment Room Monitoring	dcmonitor	resetDcMonitor
Creating a Notification	globalConf	setNotify
Adding a Secret	secret	setSecret

10 Permissions Management

[10.1 Creating a User and Assigning Permissions](#)

[10.2 MAS Custom Policies](#)

10.1 Creating a User and Assigning Permissions

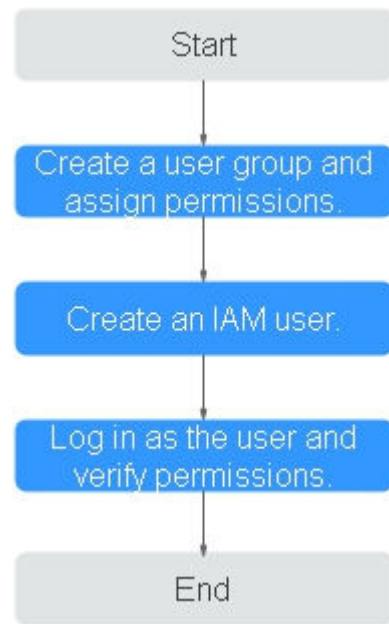
You can use [IAM](#) for fine-grained permissions control on MAS resources. With IAM, you can:

- Create IAM users for employees based on the organizational structure of your enterprise. Each IAM user has their own security credentials for accessing MAS resources.
- Grant only the permissions required for users to perform a specific task.
- Entrust an account of Huawei Cloud or cloud service to perform efficient O&M on your MAS resources.

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

This section describes the procedure for assigning permissions (see [Figure 10-1](#)).

Figure 10-1 Process for assigning MAS permissions



1. Create a user group and assign permissions to it.
Create a user group on the IAM console, and grant the **MAS ReadOnlyAccess** permission to MAS.
2. Create an IAM user.
Create a user on the IAM console and add the user to the group created in 1.
3. Log in and verify permissions.
Log in to the MAS console as the created user, and verify that the user has the granted read permissions.
 - Choose **Service List > Multi-Site High Availability Service**. Then click **Buy Multi-Active Instance** on the MAS console. If a message appears indicating that you have insufficient permissions to perform the operation, the **MAS ReadOnlyAccess** policy has already taken effect.
 - Choose any other service in **Service List**. If a message appears indicating that you have insufficient permissions to access the service, the **MAS ReadOnlyAccess** policy has already taken effect.

Prerequisites

Before assigning permissions to user groups, learn [MAS system policies](#).

For the permissions of other services, see [System Permissions](#).

10.2 MAS Custom Policies

Custom policies can be created to supplement the system-defined policies of MAS. You can create custom policies using one of the following methods:

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.

- JSON: Edit JSON policies from scratch or based on an existing policy.

The following section contains examples of common MAS custom policies.

NOTE

For details about how to use the visual editor, see [Creating a Custom Policy](#).

Example of Custom Policies

- Example 1: Authorizing users to create, modify, and check instances

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "mas:instance:create",
        "mas:instance:modify",
        "mas:instance:list",
        "mas:instance:get"
      ]
    }
  ]
}
```

- Example 2: Authorizing users to use all components and monitors in MAS

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "mas:monitor:*",
        "mas:component:*"
      ]
    }
  ]
}
```

- Example 3: Denying MAS instances deletion

A policy with only "Deny" permissions must be used in conjunction with other policies to take effect. If the permissions assigned to a user contain both "Allow" and "Deny", the "Deny" permissions take precedence over the "Allow" permissions.

The following method can be used if you need to assign permissions of the **MAS FullAccess** policy to a user but you want to prevent the user from deleting instances. Create a custom policy for denying instance deletion, and attach both policies to the group to which the user belongs. Then, the user can perform all operations on MAS except deleting instances. The following is an example of a deny policy:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "mas:instance:delete"
      ]
    }
  ]
}
```