GeminiDB Redis

Issue 02

Date 2023-03-27

HUAWEI

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to "Vul. Response Process". For details about the policy, see the following website:https://www.huawei.com/en/psirt/vul-response-process For enterprise customers who need to obtain vulnerability information, visit:https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

1 Service Overview

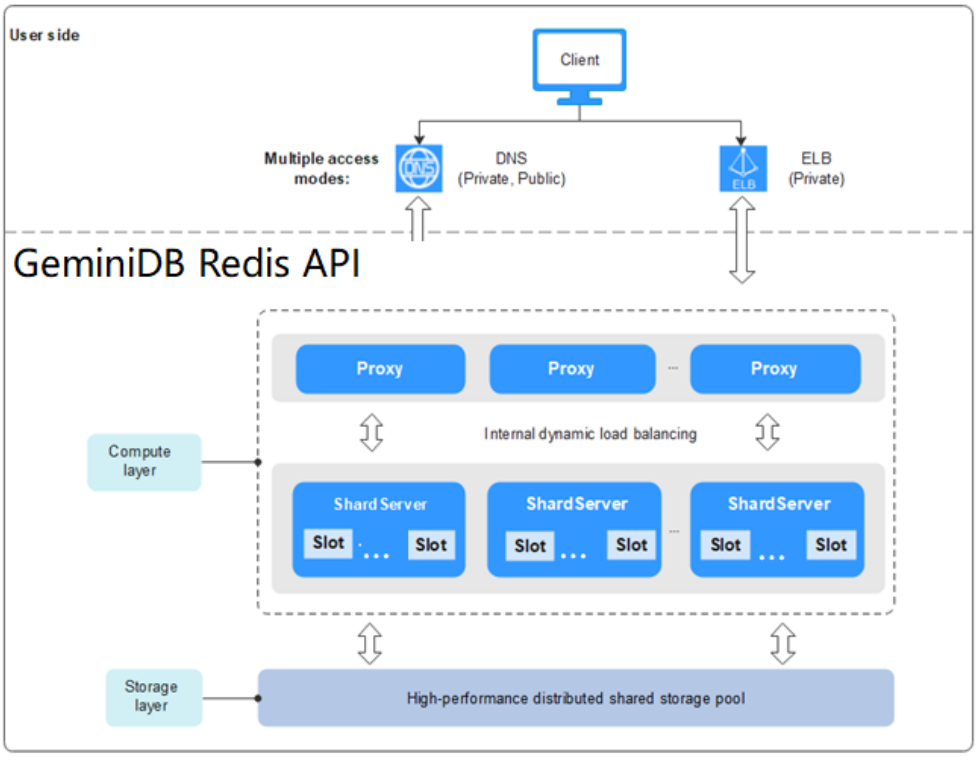
1.1 Advantages over Open-Source Reds

GeminiDB Redis API has great advantages over open-source Redis in terms of product architecture, cost, storage, security, reliability, fault recovery, and O&M. GeminiDB Redis API helps you easily roll out services.

Product Architecture

- GeminiDB Redis API

  Figure 1-1 Product architecture



- Open-source Redis

Figure 1-2 Open-source Redis architecture

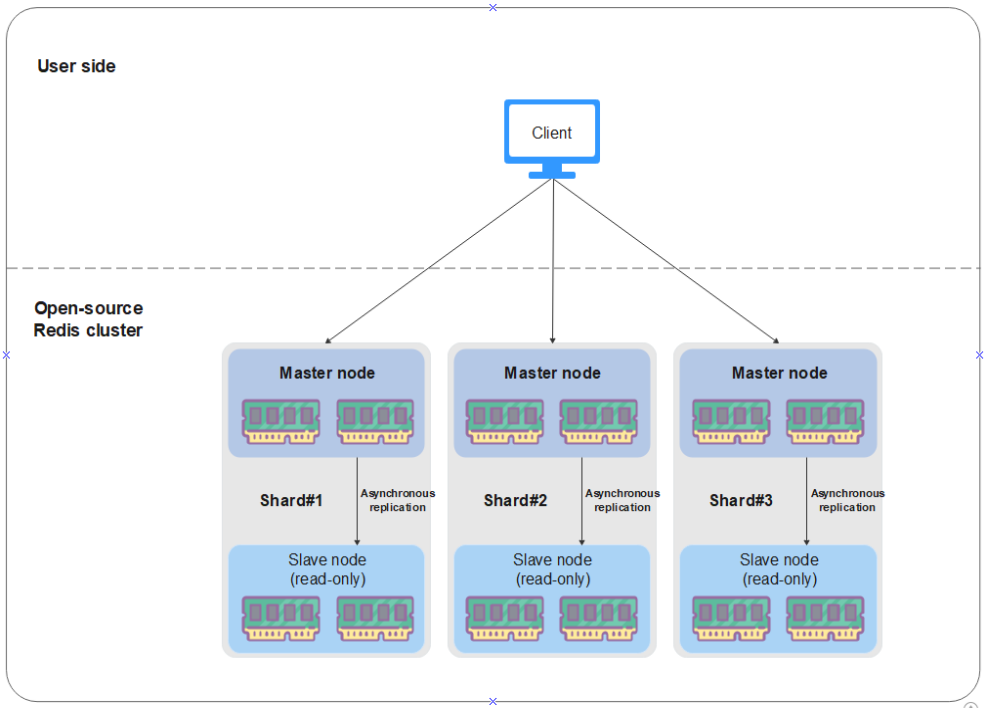


Table 1-1 Architecture comparison

Item	GeminiDB Redis API	Open-source Redis
Architecture	GeminiDB Redis API **features:** • All data is flushed to disks. Three copies of data are stored in the distributed shared storage pool, ensuring zero data loss. • All compute nodes support writes. • Three copies of data can keep your data strongly consistent, and there are no dirty reads even when multiple nodes handle service requests concurrently. • Large-scale clusters can be managed. Once a cluster node becomes faulty, other nodes of the cluster can take over services in seconds. All requests to the cluster are dynamically distributed across all cluster nodes based on your configurations. • Storage and compute resources are decoupled, so they can be scaled flexibly without service interruption.	**Open-source Redis features:** • Open-source Redis data is scattered in memory of independent nodes. If a pair of master and slave nodes become faulty, some data will be lost. • Half of nodes in a Redis cluster are slave nodes, and they are read-only. • Data is replicated asynchronously between master and slave nodes, so you may obtain inconsistent data if you access master and salve nodes at the same time. • The efficiency of the gossip protocol decreases significantly as the scale of the Redis cluster increases. • Scaling the capacity of a Redis instance means increasing its physical nodes. This has a great impact on services.

Service Scenarios

Table 1-2 Service scenario comparison

Item	GeminiDB Redis API	Open-source Redis
Service scenarios	**Has high requirements on:** • Data security • System stability to prevent system breakdown during peak hours • Data consistency **Is suitable if:** • The volume of data involved is small. GeminiDB Redis API helps enterprises lower their costs. • The volume of data involved is large. GeminiDB Redis API can process data more easily than open-source Redis.	**Has low requirements on:** • Low security, which means that core data may be lost or squeezed out of the cache by the LRU (Least Recently Used) page replacement algorithm. • Low stability, which may cause out-of-memory (OOM) issues and breakdowns • Data consistency during multi-point access **Is suitable if:** Only small volume of data is involved and the data is valid within a short period of time.

Other Advantages

Table 1-3 Advantages of GeminiDB Redis API over open-source Redis

Item	GeminiDB Redis API	Open-source Redis
Cost	Cost reduced by 75% to 90% GeminiDB Redis API supports full flush to disks and uses the GaussDB basic component service at low costs.	Extremely high hardware cost All data of open-source Redis is stored in memory, and the fork mechanism results in low disk utilization.
Maximum capacity	**PB-level data volume** Compute and storage resources are decoupled, so they can be scaled flexibly and separately at the same time to meet performance requirements.	**100-GB data volume** As more and more data needs to be stored and processed, hardware costs of a Redis cluster increase sharply, and the Gossip protocol of the cluster becomes inefficient.

Item	GeminiDB Redis API	Open-source Redis
Capacity usage	**100%** GeminiDB Redis API uses a self-developed architecture and is not affected by fork issues. Almost all the persistent storage space you purchased is available.	**<50%** Open-source Redis is affected by the exclusive fork mechanism. The memory required will be doubled theoretically during peak hours when a snapshot is taken, data is replicated between master and slave nodes, or data is rewritten to an AOF file. The memory usage must be less than 50% to ensure data security.
Specifications	1 GB fine-grained and pay-per-use mode	**Discontinuous options such as 32 GB, 48 GB, or 64 GB** Assume that the service data volume is about 30 GB. You can only buy a cloud Redis database of 64 GB storage considering that the efficient memory usage is less than 50%, which is a waste of resources.
Data compression	Logical compression and physical compression are combined, saving more space than open-source Redis. • Logical compression: Values are preliminarily compressed. • Physical compression: Data blocks in storage medium are compressed for the second time. • Service tests show that GeminiDB Redis API uses 15% to 30% less space for storing data of common types like string and hash than open-source Redis.	**Only logical compression is used.**
Latency	The average latency is on par with open-source Redis', but the p9999 latency is higher.	The average latency and the p9999 latency are both low.
Write resistance	**Strong** A multi-thread architecture is used, so multiple nodes support concurrent writes, making it easy to double the throughput.	**Weak** A single-thread architecture is used, so only the master node in a Redis cluster supports writes. There are OOM risks during peak hours.

Item	GeminiDB Redis API	Open-source Redis
Data reliability	**High** Data is flushed to disks in real time by command. Three copies of data are stored at the storage layer to avoid data loss.	**Low** Memory data is flushed to disks in seconds, but asynchronous replication between master and slave nodes is not timely. This may cause data loss.
Data consistency	**Strong** Three-copy storage ensures strong consistency, and dirty reads are prevented during multi-point access	**Weak** Data is replicated asynchronously between master and slave nodes, so you may obtain inconsistent data if you access master and salve nodes at the same time.
Availability	**High** GeminiDB Redis provides superlative fault tolerance (N-1 reliability).	**Medium** • If half of master nodes of a Redis cluster are faulty, the cluster becomes unavailable. • If any pair of master and slave nodes become faulty, the open-source Redis cluster is unavailable.
Fault recovery	Minute-level recovery. The data recovery duration is irrelevant to the data volume. In the shared-everything architecture, data can be taken over immediately by available nodes, requiring little time to load.	The larger the data volume is, the longer the restoration takes. Data is physically distributed on multiple independent nodes. During fault recovery, RDB snapshots are loaded from disks to the memory, which takes a long time.
Load balancing	Supported Fine-grained data sharding and dynamic load balancing between nodes are supported.	Not supported Third-party components are required.

Item	GeminiDB Redis API	Open-source Redis
Scale out	Seamless scale-out • Node scale-out: completed in minutes and service awareness in seconds. • Capacity expansion: completed in seconds without service interruption. • In the shared-everything architecture, underlying data can be accessed by any node. Capacity expansion is fast and does not require data replication and migration.	Time-consuming and great impact on services Data shards are stored in the memory of each node. Data migration means that new nodes are added and data is replicated and migrated, which is time-consuming.
Security	**High** • Huawei-developed architecture eliminates security vulnerabilities of open-source Redis. • The security system consists of VPCs, subnets, security groups, Anti-DDoS, and SSL, which collectively can defend against a wide range of attacks to keep your data secure.	**Low** • The open-source Redis kernel has security vulnerabilities, such as CVE-2021-32761. If the version is not upgraded in a timely manner, your data may be at risk. • Network security depends on reliability of the cloud service you used.
O&M	**One-stop services** GeminiDB Redis database expert teams provide mature migration solutions, real-time monitoring, fault warning, and 24/7 support.	**Depends on quality of the cloud service you used.**

1.2 Application Scenarios

As a key-value database compatible with Redis APIs, GeminiDB Redis extends application scenarios of Redis so that it can better meet diversified service requirements such as persistent and hybrid storage.

E-commerce

- For e-commerce applications, some commodity data is more frequently queried than others. GeminiDB Redis stores frequently queried commodity information in memory as hot data, and cold data in the shared storage pool. This not only meets the quick access requirements of popular commodities, but also avoid excessive in-memory storage costs

- GeminiDB Redis can permanently store massive amounts of historical order data of e-commerce applications. It allows you to access data through the Redis API and provides TB-level storage.
- There may be a large number of concurrent access requests within a short period of time during an e-commerce promotion. GeminiDB Redis works as a front-end cache (large memory required) to help back-end databases handle service peaks. You can easily add compute nodes in seconds to handle the expected peak traffic.

Gaming

- The schema of gaming services is simple. You can select GeminiDB Redis as a persistent database and use simple Redis APIs to quickly develop and launch services. For example, the sorted set structure of Redis can be used to display game rankings in real time.
- In delay-sensitive gaming scenarios, GeminiDB Redis can be used as the front-end cache (large memory required) to accelerate access to applications.

Live streaming

The most-viewed live streaming content usually dominates most traffic of the live streaming applications. GeminiDB Redis can efficiently use memory resources by retaining popular live streaming data in the memory and other data in the shared storage, reducing your business costs.

Online education

Online education applications store a large amount of data such as courses and Qs&As. However, only hot data (including most-viewed courses, latest question libraries, and lectures by famous teachers) is frequently accessed. GeminiDB Redis can save data in memory or shared storage based on data access frequency, achieving a balance between performance and costs.

Persistent storage for other applications

With the rapid development of the Internet, various large-scale applications have increasing requirements for persistent storage. Specifically, a massive amount of data needs to be stored, including historical orders, feature engineering, log records, location coordinates, machine learning, and user profiles. A common feature of these scenarios is large data volume and long validity period. Therefore, a large-capacity and low-cost key-value storage service is required to collect and transfer data. Redis is the most widely used key-value service. Its various data structures and operation APIs have innate advantages in storing such data. However, the native Redis can only be used as a cache and cannot guarantee persistence.

In addition to compatibility with Redis APIs, GeminiDB Redis provides large-capacity, low-cost, and high-reliability data storage capabilities, making it well-suited to persistent storage scenarios.

1.3 Compatible APIs and Versions

This section describes the compatible APIs and versions supported by GeminiDB Redis.

Table 1-4 Compatible APIs and versions

Compatible API	Instance Type	Version
Redis	• Proxy-based general purpose Depending on ELB and proxy to balance load, this type of instance is compatible with single-node and primary/standby instances, Redis Codis, Redis Cluster, and Redis Sentinel. For proxy-based general-purpose instances, recommend you to set your client to StandAlone mode.	5.0 or earlier

1.4 Instance Specifications

Instances of the same type have different memory specifications. You can select instances of different specifications based on application scenarios.

This section describes the instance specifications supported by GeminiDB Redis. The DB instance specifications depend on the selected CPU model.

Table 1-5 GeminiDB Redis instance specifications

Flavor	vCPUs	Min. Persistent Storage Space (GB) per Single-node Instance	Max. Persistent Storage Space (GB) per Single-node Instance	Maximum Connections per Single-node Instance
geminidb.redis.medium.4	1	4	32	10,000
geminidb.redis.large.4	2	8	64	10,000

Flavor	vCPUs	Min. Persistent Storage Space (GB) per Single-node Instance	Max. Persistent Storage Space (GB) per Single-node Instance	Maximum Connections per Single-node Instance
geminidb.redis.xlarge.4	4	16	128	10,000
geminidb.redis.2xlarge.4	8	32	256	10,000
geminidb.redis.4xlarge.4	16	64	512	10,000
geminidb.redis.8xlarge.4	32	128	1024	10,000
geminidb.redis.medium.8	1	8	64	10,000
geminidb.redis.large.8	2	16	128	10,000
geminidb.redis.xlarge.8	4	32	256	10,000
geminidb.redis.2xlarge.8	8	64	512	10,000
geminidb.redis.4xlarge.8	16	128	1024	10,000
geminidb.redis.8xlarge.8	32	256	2048	10,000

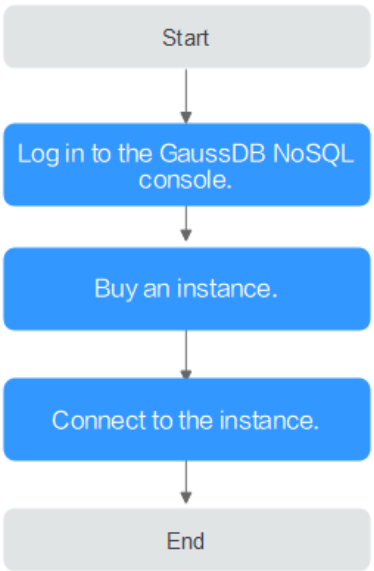
2 Getting Started with GeminiDB Redis API

2.1 Overview

This section describes how to buy an instance and then connect to and manage it.

Process

Figure 2-1 Flowchart



Operation Guide

The process of buying and using an instance involves the following steps:

Step 1: Log in to the GeminiDB Redis API console.

Step 2: **Buy an Instance**.

Step 3: **Connect to an instance**.

2.2 Buying an Instance

This section describes how to buy a GeminiDB instance that is compatible with Redis APIs.

Prerequisites

- You have registered a Huawei Cloud account.

Procedure

Step 1 Log in to the management console.

Step 2 In the service list, choose **Databases** > **GeminiDB**.

Step 3 On the **Instances** page, click **Buy DB Instance**.

Step 4 On the displayed page, specify a billing mode and instance specifications and click **Next**.

Figure 2-2 Billing mode and basic information

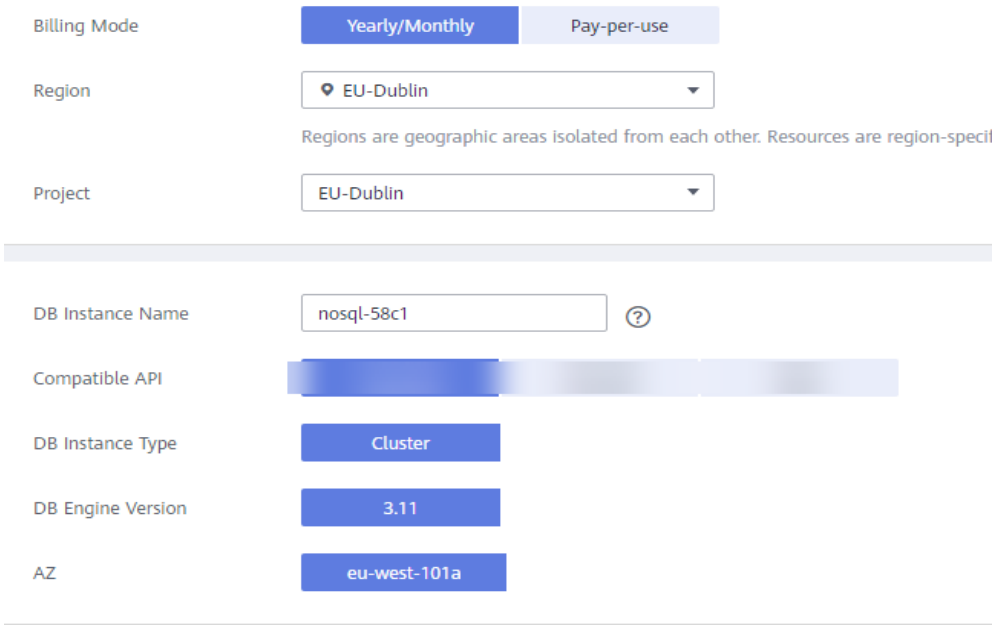


Table 2-1 Billing mode description

Parameter	Description
Billing Mode	Method that the instance is billed in. The value can be **Yearly/Monthly** or **Pay-per-use**. • **Yearly/Monthly** – In this mode, specify **Required Duration** at the bottom of the page. The system bills you based on the service price. – If you do not need such an instance any longer after it expires, change the billing mode to pay-per-use to optimize costs. For details, see **Changing the Billing Mode from Yearly/Monthly to Pay-per-Use**. **NOTE** Yearly/Monthly instances cannot be deleted directly. If such an instance is no longer required, unsubscribe from it. For details, see **Unsubscribing from a Yearly/Monthly Instance**. • **Pay-per-use** – If you select this billing mode, you are billed based on how much time the instance is in use. – If you expect to use an instance for a long period of time, change its billing mode to yearly/monthly to optimize costs. For details, see **Changing the Billing Mode from Pay-per-Use to Yearly/Monthly**.

Table 2-2 Basic information

Parameter	Description
Region	The region where the instance is deployed. **NOTICE** Select the region nearest where you will access the instance from, so latency can be kept to a minimum and response will be faster. Instances deployed in different regions cannot communicate with each other over a private network. After you buy an instance, you cannot change its region.
DB Instance Name	The instance name: • Can be the same as an existing instance name. • Can include 4 to 64 bytes and must start with a letter. It is case-sensitive and allows only letters, digits, hyphens (-), and underscores (_). You can change the name of an instance after it is created. For details, see **Modifying the Name of an Instance**.
Compatible API	Redis

Parameter	Description
DB Instance Type	• **Proxy-based general purpose** Depending on ELB and proxy to balance load, this type of instance is compatible with single-node and primary/standby instances, Redis Codis, Redis Cluster, and Redis Sentinel.
Compatible Version	5.0 or earlier
Data Copies	The default value is **3**. Three copies of the data is created, and each copy always provides the same data as the other two to keep services available.
AZ	Availability zone where the instance is created. An AZ is a part of a region with its own independent power supplies and networks. AZs are physically isolated but can communicate with each other over a private network.

Figure 2-3 Specifications and storage

Table 2-3 Specifications and storage

Parameter	Description
Node Specifications	Provides a standard process to configure instance specifications, including specifying the specifications, node quantity, and storage space.
Nodes	Specify the number of nodes based on service requirements. After an instance is created, you can add nodes.
Storage Space	The storage is an integer and the minimum storage is 32 GB. You can add a minimum of 1 GB at a time.

Table 2-4 Network information

Parameter	Description
VPC	The virtual network where the instance is created. A VPC isolates networks for different services. You can select an existing VPC or create one. For details about how to create a VPC, see "Creating a VPC" in *Virtual Private Cloud User Guide*. If there are no VPCs available, the system automatically allocates a VPC to you. **NOTE** • After a GeminiDB Redis instance is created, its VPC cannot be changed. • If you want to connect to a GeminiDB Redis instance through an ECS over a private network, the instance and the ECS must be in the same VPC. If they are not in the same VPC, you can create a **VPC peering connection** to enable access.
Subnet	A subnet where your instance is created. The subnet provides dedicated and isolated networks, improving network security. **NOTE** Creating an IPv4 subnet or selecting an existing one is recommended. IPv6 subnets are not supported.
Security Group	A security group controls access between GeminiDB Redis instances and other services. Ensure that the security group you select allows your client to access the instance. If there are no security groups available, the system automatically allocates one to you.
SSL	A security protocol. Secure Sockets Layer (SSL) certificates set up encrypted connections between clients and servers, preventing data from being tampered with or stolen during transmission. You can enable SSL to improve data security. After an instance is created, you can connect to it using **SSL**. **NOTE** • This function is in the open beta test (OBT) phase. To use this function, contact customer service. • If SSL is not enabled when you create an instance, you can enable it after the instance is created. For details, see **Configuring an SSL Connection**.

Table 2-5 Database configuration

Parameter	Description
Administrator Password	Password of the administrator account. The password: • Can contain 8 to 32 characters. • Can include uppercase letters, lowercase letters, digits, and any of the following special characters: ~!@#%^*-_=+? • For security reasons, set a strong password. The system will verify the password strength. Keep your password secure. The system cannot retrieve it if it is lost.
Confirm Password	This password must be consistent with the administrator password.
Enterprise Project	This parameter is provided for enterprise users. An enterprise project groups cloud resources, so you can manage resources and members by project. The default project is **default**. Select an enterprise project from the drop-down list. For more information about enterprise projects, see ***Enterprise Management User Guide***.

Table 2-6 Tags

Parameter	Description
Tags	This parameter is optional. Adding tags helps you better identify and manage your GeminiDB Redis instances. Each instance supports up to 20 tags by default. A tag consists of a tag key and a tag value. • Tag key: Mandatory if the instance is going to be tagged Each tag key is unique for each instance. The key can include up to 36 characters, including digits, letters, underscores (_), and hyphens (-). • Tag value: Optional if the instance is going to be tagged The value can contain up to 43 characters, including digits, letters, underscores (_), periods (.), and hyphens (-). After an instance is created, you can click its name to view its tags on the **Tags** page. In addition, you can add, modify, and delete tags of an existing instance. For details, see **Managing Tags**.

Table 2-7 Required duration

Parameter	Description
Required Duration	The length of your subscription if you select **Yearly/Monthly** billing. Subscription lengths range from one month to three years.
Auto-renew	• This option is not selected by default. • If you select this option, the renew cycle is the same as the selected duration.

Step 5 On the displayed page, confirm the instance details.

- For yearly/monthly instances
  - If you need to modify the settings, click **Previous** to modify parameters.
  - If no modification is required, read and agree to the service agreement, click **Pay Now**, and complete the payment.
- Pay-per-use
  - If you need to modify the settings, click **Previous** to modify parameters.
  - If no modification is required, read and agree to the service agreement and click **Submit**.

Step 6 On the **Instances** page, view and manage the created instance.

- After the creation is complete, the instance status changes to **Available**.

  You can click  in the upper right corner of the page to refresh the instance status.
- The default database port of the instance is **8635** and cannot be changed.

----End

2.3 Connect to the Instance

2.3.1 Connection Methods

GeminiDB Redis is compatible with the Redis API and allows traffic from applications using different types of SDKs. It can also be accessed using a web-based console or over private and public networks.

Table 2-8 Connection methods

Method	Scenario	Description
Console	You can connect to a GeminiDB Redis instance using a web-based console client.	-

Method	Scenario	Description
Private network	You can connect to a GeminiDB Redis instance using **a private IP address**, **private domain name**, or **load balancer address**. This method is suitable when your application is deployed on an ECS that is in the same region and VPC as your DB instance.	• Use the load balancer address or private domain name to ensure high reliability and eliminate SPOFs. • High security and performance
Public network	You can connect to a GeminiDB Redis instance using a **public domain name** or an **EIP**. This method is suitable when an instance cannot be accessed over a private network. You can connect to the instance from an ECS using a public domain name or an EIP.	• For faster transmission and improved security, migrate your applications to an ECS that is in the same subnet as your instance and use a private IP address to access the instance. • Use a public domain name to ensure high reliability and eliminate SPOFs.

2.3.2 Brute Force Attack Defense

- Brute-force attack defense mechanism

  GeminiDB Redis enables brute force attack defense by default, to automatically lock out an IP address after 5 failed authentication attempts.
- Automatic unlocking

  After an IP address is locked for 5s, the IP address is automatically unlocked and can be authenticated again.
- Manual unlocking

  If you want to manually unlock an IP address or disable brute-force defense, contact customer service for authorization.

CAUTION

To improve security, you can submit a service ticket and ask technical engineers to help adjust authentication times and locking duration.

Make sure to fully evaluate risks and exercise caution when you disable or modify the security policy. After you adjust the security policy, risks and accidents incurred will not be accounted in the SLA and shall be borne by yourself.

2.3.3 Connecting to a GeminiDB Redis Instance Over Private Networks

2.3.3.1 Connecting to an Instance Using a Load Balancer Address (Recommended)

This section describes how to connect to a GeminiDB Redis instance using a load balancer address on a Linux ECS. Load balancing can improve data reliability and eliminate single point of failures (SPOFs).

Precautions

- The instances must be in the same VPC and subnet as the ECS.
- The ECS must be in a security group that has access to the instances.

  Scenario 1: If the instance is associated with the default security group, you do not need to configure security group rules.

  Scenario 2: If the instance is not associated with the default security group, check whether the security group rules allow the ECS to connect to the instance.

  - If yes, the ECS can connect to the instance.
  - If no, add an inbound rule to the security group.

    For details about how to configure a security group, see **Configuring Security Group Rules**.

Prerequisites

- An ECS has been created. The following uses a Linux ECS as an example. For details, see **Purchasing an ECS** in *Getting Started with Elastic Cloud Server*.
- Download the **Redis client installation package**.

Procedure

Step 1 Log in to the ECS. For details, see **Logging In to an ECS** in *Getting Started with Elastic Cloud Server*.

Step 2 Obtain the Redis client.

Method 1

Run the following command to download the Redis client.

wget http://download.redis.io/releases/redis-5.0.7.tar.gz

Method 2

Download the Redis client from the address provided in **Prerequisites** and upload the Redis client installation package to the ECS.

Step 3 Decompress the client tool package.

tar -xzf redis-5.0.7.tar.gz

Step 4 Connect to the DB instance in the **src** directory.

cd redis-5.0.7

make

cd src

./redis-cli -h <*DB_HOST*> **-p** <*DB_PORT*> **-a** <*DB_PWD*>

Example:

./redis-cli -h 192.xx.xx.xx -p 8635 -a <*DB_PWD*>

Table 2-9 Parameter description

Parameter	Description
<DB_HOST>	Load balancer IP address of the instance to be connected. After the load balancer IP address is created, click the instance name to go to the **Basic Information** page and obtain the load balancer IP address in the **Network Information** area.
<DB_PORT>	Access port corresponding to the load balancer IP address of the instance. Click the name of the instance to go to the **Basic Information** page. In the **Network Information** area, you can find the access port in field **Load Balancer IP Address**.
<DB_PWD>	Specifies the administrator password set when you buy a GeminiDB Redis instance.

Step 5 Check the results. If the following information is displayed, the connection is successful.

```
IP:port>
```

----End

2.3.3.2 Connecting to an Instance Using a Private Domain Name

This section describes how to connect to a GeminiDB Redis instance using a private domain name on a Linux ECS.

Precautions

- The instances must be in the same VPC and subnet as the ECS.
- The ECS must be in a security group that has access to the instances.

  Scenario 1: If the instance is associated with the default security group, you do not need to configure security group rules.

  Scenario 2: If the instance is not associated with the default security group, check whether the security group rules allow the ECS to connect to the instance.

  - If yes, the ECS can connect to the instance.
  - If no, add an inbound rule to the security group.

    For details about how to configure a security group, see **Configuring Security Group Rules**.

Prerequisites

- An ECS has been created. The following uses a Linux ECS as an example. For details, see **Purchasing an ECS** in *Getting Started with Elastic Cloud Server*.
- Download the **Redis client installation package**.

Procedure

Step 1 Configure the private domain name for the GeminiDB Redis instance. For details, see **Configuring a Private Domain Name**.

Step 2 Log in to the ECS. For details, see **Logging In to an ECS** in *Getting Started with Elastic Cloud Server*.

Step 3 Obtain the Redis client.

Method 1

Run the following command to download the Redis client.

wget http://download.redis.io/releases/redis-5.0.7.tar.gz

Method 2

Download the Redis client from the address provided in **Prerequisites** and upload the Redis client installation package to the ECS.

Step 4 Decompress the client tool package.

tar -xzf redis-5.0.7.tar.gz

Step 5 Connect to the DB instance in the **src** directory.

cd redis-5.0.7

make

cd src

./redis-cli -h <*DB_Domain_Name*> **-p** <*DB_PORT*> **-a** <*DB_PWD*>

Example:

./redis-cli -h redis.com -p 8635 -a *<DB_PWD>*

Table 2-10 Parameter description

Parameter	Description
<DB_Domain_Name>	The private domain name of the DB instance to be connected. The private domain name is the one created in **Step 1**.

Parameter	Description
<DB_PORT>	Port for accessing the target instance. Configure this parameter based on service requirements. To obtain the instance port number, perform the following steps: Click the target instance to go to the **Basic Information** page. In the **Network Information** area, you can find the database port.
<DB_PWD>	Specifies the administrator password set when you buy a GeminiDB Redis instance.

Step 6 Check the results. If the following information is displayed, the connection is successful.

```
Domain_Name:port>
```

----End

2.3.3.3 Connecting to an Instance Using a Private IP Address

You can use the private IP address to connect to the GeminiDB Redis instance.

This section uses the Linux OS as an example to describe how to connect to a GeminiDB Redis instance using the Redis-cli client.

Precautions

- The instances must be in the same VPC and subnet as the ECS.
- The ECS must be in a security group that has access to the instances. For details, see **Configuring Security Group Rules**.

Prerequisites

An ECS has been created. The following uses a Linux ECS as an example. For details, see **Purchasing an ECS** in *Getting Started with Elastic Cloud Server*.

Procedure

Step 1 Log in to the ECS. For details, see **Logging In to an ECS** in *Getting Started with Elastic Cloud Server*.

Step 2 Obtain the Redis client.

Method 1

Run the following command to download the Redis client.

wget http://download.redis.io/releases/redis-5.0.7.tar.gz

Method 2

Download the **Redis client** installation package and upload it to the ECS.

Step 3 Decompress the client tool package.

tar -xzf redis-5.0.7.tar.gz

Step 4 Connect to the DB instance in the **src** directory.

cd redis-5.0.7

make

cd src

./redis-cli -h <*DB_HOST*> **-p** <*DB_PORT*> **-a** <*DB_PWD*>

Example:

./redis-cli -h 192.xx.xx.xx -p 8635 -a <*DB_PWD*>

Table 2-11 Parameter description

Parameter	Description
<DB_HOST>	The private IP address of the instance to be connected. To obtain this IP address, go to the **Instance Management** page and click the target DB instance name. The IP address can be found in the **Private IP Address** field under **Node Information** on the **Basic Information** page. If the instance you purchased has multiple nodes, select the private IP address of any node.
<DB_PORT>	Port for accessing the target instance. Configure this parameter based on service requirements. To obtain the instance port number, perform the following steps: Click the target instance to go to the **Basic Information** page. In the **Network Information** area, you can find the database port.
<DB_PWD>	Specifies the administrator password set when you buy a GeminiDB Redis instance.

Step 5 Check the results. If the following information is displayed, the connection is successful.

```
IP:port>
```

----End

2.3.4 Connecting to a GeminiDB Redis Instance Over Public Networks

2.3.4.1 Connecting to an Instance Using a Public Domain Name (Recommended)

A public domain name is a domain name used to access websites or web applications on the Internet.

You can use Domain Name Service (DNS) to translate common domain names (for example, www.example.com) into IP addresses (for example, 1.2.3.4) required for network connection. In this way, you can access GeminiDB Redis instances using the resolved IP addresses.

This section uses the Linux OS as an example to describe how to use the public network domain name configured by the DNS service to connect to a GeminiDB Redis instance.

Prerequisites

- An ECS has been created. The following uses a Linux ECS as an example. For details, see **Purchasing an ECS** in *Getting Started with Elastic Cloud Server*.
- You have registered a domain name and an EIP.
- You have bound an EIP to a node of the purchased instance and configure security group rules for the node. For details, see **Binding and Unbinding an EIP** and **Configuring Security Group Rules**.

  NOTE

  A GeminiDB Redis instance can have multiple nodes. Select any node and bind an EIP to it.
- Download the **Redis client installation package**.

Procedure

Step 1 Configure the private domain name for the GeminiDB Redis instance. For details, see **Configuring a Public Domain Name**.

Step 2 Log in to the ECS. For details, see **Logging In to an ECS** in *Getting Started with Elastic Cloud Server*.

Step 3 Obtain the Redis client.

Method 1

Run the following command to download the Redis client.

wget http://download.redis.io/releases/redis-5.0.7.tar.gz

Method 2

Download the Redis client from the address provided in **Prerequisites** and upload the Redis client installation package to the ECS.

Step 4 Decompress the client tool package.

tar -xzf redis-5.0.7.tar.gz

Step 5 Open the **src** directory and connect to the DB instance.

cd redis-5.0.7

make

cd src

./redis-cli -h <*DB_Domain_Name*> **-p** <*DB_PORT*> **-a** <*DB_PWD*>

Example:

./redis-cli -h redis.com -p 8635 -a *<DB_PWD>*

Table 2-12 Parameter description

Parameter	Description
<DB_Domain_Name>	The public domain name of the instance to be connected. The public domain name is the one created in **Step 1**.
<DB_PORT>	Port for accessing the target instance. Configure this parameter based on service requirements. To obtain the instance port number, perform the following steps: Click the target instance to go to the **Basic Information** page. In the **Network Information** area, you can find the database port.
<DB_PWD>	Specifies the administrator password set when you buy a GeminiDB Redis instance.

Step 6 Check the results. If the following information is displayed, the connection is successful.

```
Domain_Name:port>
```

----End

2.3.4.2 Connecting to an Instance Using an EIP

You can connect to a GeminiDB Redis instance from an ECS or a local device over a public network.

This section uses the Linux OS as an example to describe how to connect to a GeminiDB Redis instance using the Redis-cli client. You can connect to a DB instance through an unencrypted connection or an encrypted connection (SSL). The SSL connection encrypts data and is more secure.

If you need to access GeminiDB Redis instances over a public network, use a **public domain name** to ensure instance reliability.

Precautions

- The SSL connection is in the open beta test (OBT) phase. To use this mode, contact customer service.
- After the SSL connection is enabled, download the SSL certificate for your applications to access to the GeminiDB Redis instance.
- If the SSL connection is used, ensure that the Redis client, for example, Redis-cli 6.x, supports SSL.

- To connect to a DB instance through an unencrypted connection, the SSL connection must be disabled. For details about how to disable SSL, see **Configuring an SSL Connection**.
- You need to estimate the bandwidth required by services and purchase an EIP with sufficient bandwidth resources. **Client access exceptions caused by poor public network performance will not be included in the SLA.**

Prerequisites

1. An ECS has been created. The following uses a Linux ECS as an example. For details, see **Purchasing an ECS** in *Getting Started with Elastic Cloud Server*.
2. Bind an EIP to the instance node and configure security group rules. For details, see **Binding and Unbinding an EIP** and **Configuring Security Group Rules**.

   NOTE

   A GeminiDB Redis instance has multiple nodes. Select any node and bind an EIP to it.

SSL (Recommended)

Step 1 Obtain the Redis client.

Method 1

Run the following command to download the Redis client.

wget https://download.redis.io/releases/redis-6.2.6.tar.gz

Method 2

Download the **Redis client** installation package and upload it to the ECS.

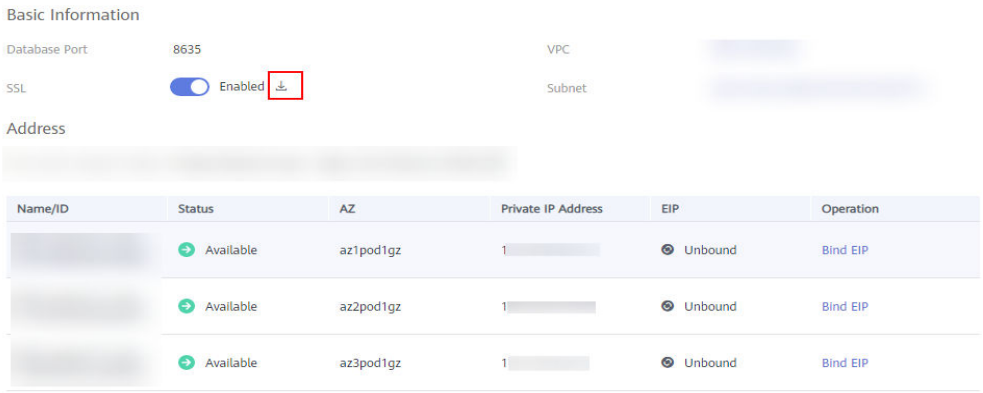
Step 2 Obtain the SSL certificate.

Method 1: Click the target instance name. On the **Basic Information** page, in the **DB Information** area, click the download button in the **SSL** field to obtain the SSL certificate.

Figure 2-4 Obtaining the SSL certificate

Method 2: Click the target instance. On the **Basic Information** page, choose **Connections**. In the **Basic Information** area, click the download button in the **SSL** field to download the SSL certificate.

Figure 2-5 Obtaining the SSL certificate



Step 3 Upload the SSL certificate to the ECS.

Step 4 Check the OpenSSL version supported by the ECS OS.

openssl version

NOTE

- The SSL function provided by GeminiDB Redis API supports only TLS 1.3 or later.
- The OpenSSL version in the ECS OS must be 1.1.1 or later so that redis-cli can support TLS 1.3 or later.

- If the OS version is earlier than 1.1.1, perform the following steps to install OpenSSL:

  wget https://www.openssl.org/source/openssl-1.1.1m.tar.gz

  tar -zxvf openssl-1.1.1m.tar.gz

  cd openssl-1.1.1m/

  ./config --prefix=/usr/local/openssl-1.1.1m_install_dir

  make

  make install

  After OpenSSL is installed, go to **Step 5**.
- If the OS is 1.1.1 or later, go to **Step 5**.

Step 5 Decompress the client tool package.

tar -xzf redis-6.2.6.tar.gz

Step 6 Connect to the DB instance in the **src** directory.

- If the required OpenSSL version has been installed by performing **Step 4** and the version is earlier than 1.1.1, you can connect to the DB instance using the following method:

  cd redis-6.2.6

  make BUILD_TLS=yes OPENSSL_PREFIX=/usr/local/openssl-1.1.1m_install_dir

  cd src

  LD_PRELOAD=/usr/local/openssl-1.1.1m_install_dir/lib/libssl.so.1.1:/usr/local/openssl-1.1.1m_install_dir/lib/libcrypto.so.1.1 ./redis-cli -h *<DB_HOST>* **-p** *<DB_PORT>* **-a** *<DB_PWD>* **--tls --cacert** *<CACERT_PATH>*

Example:

LD_PRELOAD=/usr/local/openssl-1.1.1m_install_dir/lib/libssl.so.1.1:/usr/local/openssl-1.1.1m_install_dir/lib/libcrypto.so.1.1 ./redis-cli -h 192.168.0.208 -p 8635 -a *<DB_PWD>* **--tls --cacert ./cacert.crt**

- If the OpenSSL version in the ECS OS is 1.1.1 or later, you can connect to the DB instance using the following method:

  cd redis-6.2.6

  make BUILD_TLS=yes

  cd src

  ./redis-cli -h *<DB_HOST>* **-p** *<DB_PORT>* **-a** *<DB_PWD>* **--tls --cacert** *<CACERT_PATH>*

  Example:

  ./redis-cli -h 192.168.0.208 -p 8635 -a *<DB_PWD>* **--tls --cacert ./cacert.crt**

Table 2-13 Parameter description

Parameter	Description
<DB_HOST>	Specifies the EIP bound to the instance to be connected. To obtain the EIP, go to the **Instance Management** page and click the target instance name. The EIP can be found in the **EIP** column in the **Node Information** area on the **Basic Information** page. If the instance you bought has multiple nodes, you can bind the EIP to any node to connect to the instance. If a message is displayed indicating that no EIP has been bound to the instance, bind an EIP to the instance by referring to **Binding and Unbinding an EIP**.
<DB_PORT>	Port for accessing the target instance. Configure this parameter based on service requirements. To obtain the instance port number, perform the following steps: Click the target instance to go to the **Basic Information** page. In the **Network Information** area, you can find the database port.
<DB_PWD>	Specifies the administrator password set when you buy a GeminiDB Redis instance.
<CACERT_PATH>	The path of the SSL certificate.

Step 7 Check the results. If the following information is displayed, the connection is successful.

```
IP:port>
```

----End

Non-SSL Connection

Step 1 Log in to the ECS. For details, see **Logging In to an ECS** in *Getting Started with Elastic Cloud Server*.

Step 2 Obtain the Redis client.

Method 1

Run the following command to download the Redis client.

wget http://download.redis.io/releases/redis-5.0.7.tar.gz

Method 2

Download the **Redis client** installation package and upload it to the ECS.

Step 3 Decompress the client tool package.

tar -xzf redis-5.0.7.tar.gz

Step 4 Connect to the DB instance in the **src** directory.

cd redis-5.0.7

make

cd src

./redis-cli -h <*DB_HOST*> **-p** <*DB_PORT*> **-a** <*DB_PWD*>

Example:

./redis-cli -h 192.168.0.208 -p 8635 -a <*DB_PWD*>

Table 2-14 Parameter description

Parameter	Description
<DB_HOST>	Specifies the EIP of the instance to be connected. To obtain the EIP, go to the **Instance Management** page and click the target instance name. The EIP can be found in the **EIP** column in the **Node Information** area on the **Basic Information** page. If the instance you bought has multiple nodes, you can bind the EIP to any node to connect to the instance. If a message is displayed indicating that no EIP has been bound to the instance, bind an EIP to the instance by referring to **Binding and Unbinding an EIP**.
<DB_PORT>	Port for accessing the target instance. Configure this parameter based on service requirements. To obtain the instance port number, perform the following steps: Click the target instance to go to the **Basic Information** page. In the **Network Information** area, you can find the database port.

Parameter	Description
<DB_PWD>	Specifies the administrator password set when you buy a GeminiDB Redis instance.

Step 5 Check the results. If the following information is displayed, the connection is successful.

```
IP:port>
```

----End

3 Working with GeminiDB Redis API

3.1 IAM Permissions Management

3.1.1 Creating a User and Assigning Permissions

This section describes how to use **IAM** to control fine-grained permissions for your GeminiDB resources. With IAM, you can:

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

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

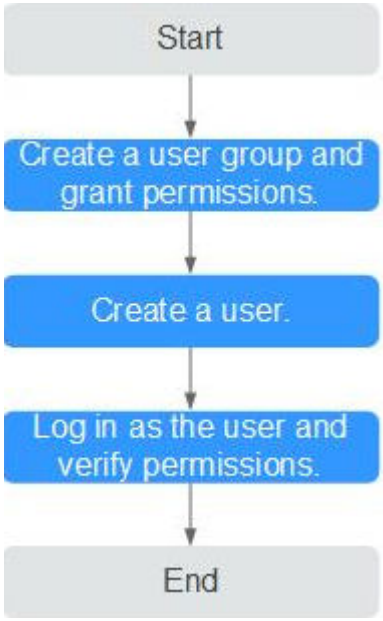
The following describes the procedure for granting permissions (see **Figure 3-1**).

Prerequisites

Learn about the permissions supported by GeminiDB and choose policies or roles based on your requirements. For details about the permissions, see . For system policies of other services, see **Permissions Policies**.

Process Flow

Figure 3-1 Process of granting GeminiDB permissions



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

   Create a user group on the IAM console and attach the **GaussDB NoSQL FullAccess** policy to the group.

   NOTE

   To use some interconnected services, you also need to configure permissions of such services.

   For example, you need to configure the **DAS FullAccess** permission so that you can log in to your DB instance on the DAS console.

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

   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 management console using the created user, and verify the user's permissions:

   Choose **Service List** > **GeminiDB** and click **Buy DB Instance**. If you can buy an instance, the required permission policy has taken effect.

3.1.2 Creating a Custom Policy

Custom policies can be created to supplement the system-defined policies of GeminiDB. For the actions supported for custom policies, see .

You can create custom policies in either of the following ways:

- 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.

For details, see **Creating a Custom Policy**. The following describes examples of common GeminiDB custom policies.

Example Custom Policy

- Example 1: Allowing users to create GeminiDB instances

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "nosql:instance:create"
         ]
      }
   ]
}
```

- Example 2: Refusing users to delete GeminiDB instances

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

  The following method can be used if you need to assign permissions of the **GaussDB NoSQLFullAccess** policy to a user but you want to prevent the user from deleting GeminiDB 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 GeminiDB instances except deleting GeminiDB instances. The following is an example of the deny policy:

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

- Example 3: Defining permissions for multiple services in a policy

  A custom policy can contain the actions of multiple services that are of the global or project-level type. The following is an example policy containing actions of multiple services:

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "nosql:instance:create",
                "nosql:instance:rename",
                "nosql:instance:delete",
                "vpc:publicIps:list",
                "vpc:publicIps:update"
            ],
            "Effect": "Allow"
        }
```



```
        ]
}
```

3.2 Billing Management

3.2.1 Renewing Instances

This section describes how to renew your yearly/monthly GeminiDB Redis instances.

Precautions

- Pay-per-use instances cannot be renewed.

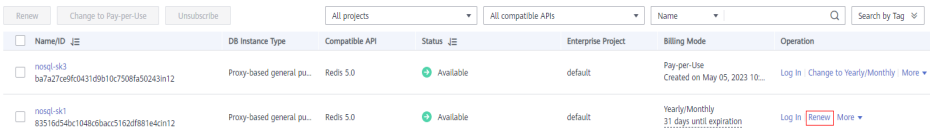
Renewing a Yearly/Monthly Instance

Step 1 Log in to the management console.

Step 2 In the service list, choose **Databases** > **GeminiDB**.

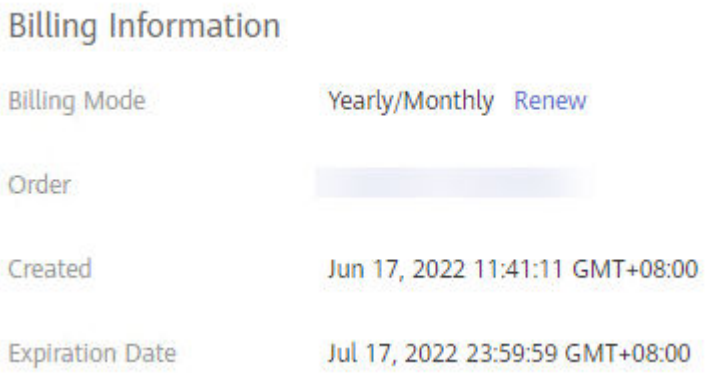
Step 3 On the **Instances** page, locate the instance that you want to renew and click **Renew** in the **Operation** column.

Figure 3-2 Renewing an instance



Alternatively, click the instance name to go to the **Basic Information** page. In the **Billing Information** area, click **Renew** next to the **Billing Mode** field.

Figure 3-3 Renewing an instance



Step 4 On the displayed page, renew the instance.

----End

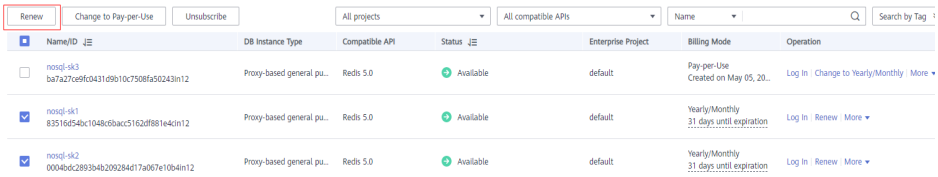
Renewing Multiple Instances in Batches

Step 1 Log in to the management console.

Step 2 In the service list, choose **Databases** > **GeminiDB**.

Step 3 On the **Instances** page, select the instance that you want to renew and click **Renew** above the instance list.

Figure 3-4 Batch renewing instances



Step 4 In the displayed dialog box, click **Yes**.

----End

3.2.2 Changing the Billing Mode from Pay-per-Use to Yearly/Monthly

This section describes how to change the billing mode of a GeminiDB Redis instance from pay-per-use to yearly/monthly. If you want to use a pay-per-use instance for a long time, change its billing mode to yearly/monthly to reduce costs.

Precautions

- Only when the status of a pay-per-use instance is **Available**, its billing mode can be changed to yearly/monthly.
- The function of batch changing the billing mode of pay-per-use instances to yearly/monthly is in the open beta test (OBT) phase. To use this function, contact customer service.

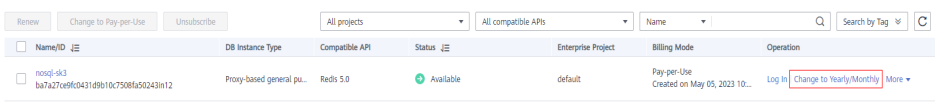
Changing the Billing Mode of a Single Instance

Step 1 Log in to the management console.

Step 2 In the service list, choose **Databases** > **GeminiDB**.

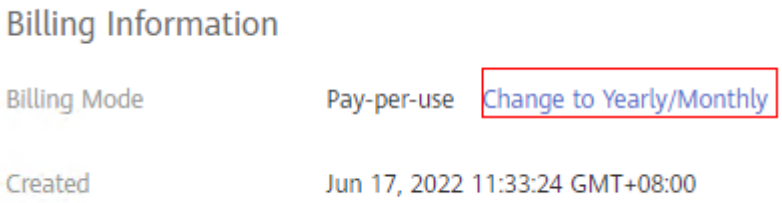
Step 3 On the **Instances** page, locate the instance whose billing mode you want to change and click **Change to Yearly/Monthly** in the **Operation** column.

Figure 3-5 Changing from pay-per-use to yearly/monthly



Alternatively, click the instance name to go to the **Basic Information** page. In the **Billing Information** area, click **Change to Yearly/Monthly** in the **Billing Mode** field.

Figure 3-6 Changing from pay-per-use to yearly/monthly



Step 4 On the displayed page, specify a renewal duration in month. The minimum duration is one month.

Confirm the settings and click **Pay Now**.

Step 5 Select a payment method and click **Pay**.

Step 6 View the results on the **Instances** page.

In the upper right corner of the instance list, click to refresh the list. The instance status will become **Available** after the change is successful. The billing mode changes to **Yearly/Monthly**.

----End

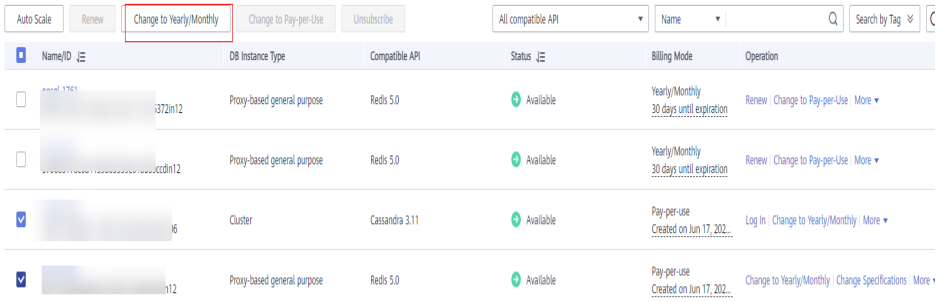
Changing the Billing Mode of Multiple Instance in Batches

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

Step 2 In the service list, choose **Databases** > **GeminiDB**.

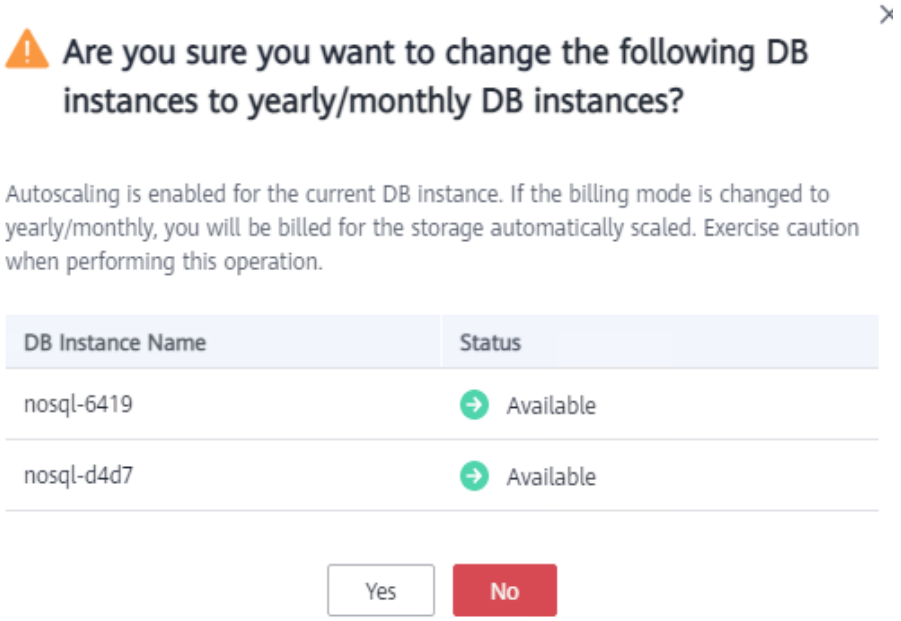
Step 3 On the **Instances** page, select the instances whose billing mode you want to change and click **Change to Yearly/Monthly** above the instance list.

Figure 3-7 Changing the billing mode of multiple instances



Step 4 In the displayed dialog box, click **Yes**.

Figure 3-8 Confirming the instance information



Step 5 On the displayed page, specify a renewal duration in month. The minimum duration is one month.

Confirm the settings and click **Pay Now**.

Step 6 Select a payment method and click **Pay**.

Step 7 View the results on the **Instances** page.

In the upper right corner of the instance list, click to refresh the list. The instance status will become **Available** after the change is successful. The billing mode changes to **Yearly/Monthly**.

----End

3.2.3 Changing the Billing Mode from Yearly/Monthly to Pay-per-Use

You can change the billing mode of a GeminiDB Redis instance from yearly/monthly to pay-per-use.

Precautions

- The billing mode of a yearly/monthly instance can only be changed to pay-per-use when the instance is in the **Available** status.

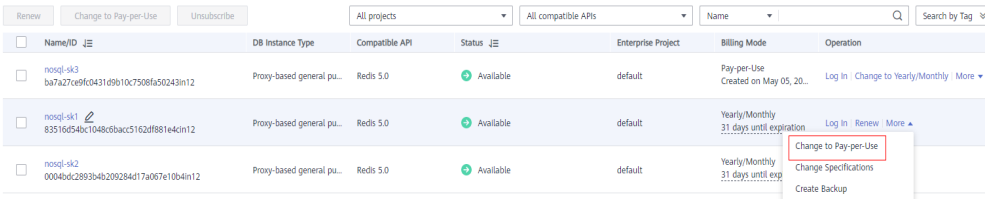
Changing the Billing Mode of a Single Instance to Pay-per-Use

Step 1 Log in to the management console.

Step 2 In the service list, choose **Databases** > **GeminiDB**.

Step 3 On the **Instances** page, locate the instance whose billing mode you want to change and click **More** > **Change to Pay-per-Use** in the **Operation** column.

Figure 3-9 Changing from yearly/monthly to pay-per-use



Step 4 On the displayed page, confirm the instance information and click **Change to Pay-per-Use**. The billing mode will change to pay-per-use after the instance expires.

NOTICE

Auto renewal will be disabled after the billing mode of your instances change to pay-per-use. Exercise caution when performing this operation.

Step 5 After you submit the change, a message is displayed in the **Billing Mode** column of the target DB instance, indicating that the billing mode will be changed to pay-per-use after the DB instance expires.

Step 6 To cancel the change, choose **Billing** > **Renewal** to enter the Billing Center. On the **Renewals** page, locate the target DB instance and click **More** > **Cancel Change to Pay-per-Use**.

Step 7 In the displayed dialog box, click **Yes**.

----End

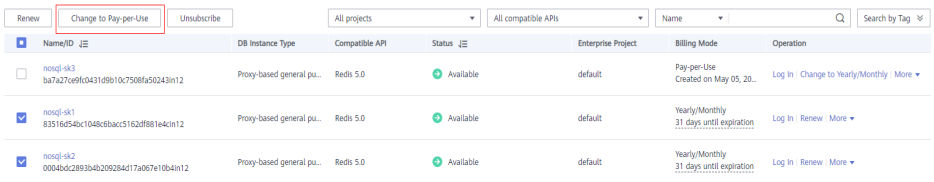
Changing the Billing Mode of Multiple Instances to Pay-per-use

Step 1 Log in to the management console.

Step 2 In the service list, choose **Databases** > **GeminiDB**.

Step 3 On the **Instances** page, select the instances whose billing mode you want to change and click **Change to Pay-per-Use** above the instance list.

Figure 3-10 Changing the billing mode of multiple instances to pay-per-use



Step 4 In the displayed dialog box, click **Yes**.

Step 5 On the displayed page, confirm the instance information and click **Change to Pay-per-Use**. The billing mode will change to pay-per-use after the DB instance expires.

NOTICE

Auto renewal will be disabled after the billing mode of your instances change to pay-per-use. Exercise caution when performing this operation.

Step 6 After you submit the change, a message is displayed in the **Billing Mode** column of the target DB instance, indicating that the billing mode will be changed to pay-per-use after the DB instance expires.

Step 7 To cancel the change, choose **Billing** > **Renewal** to enter the Billing Center. On the **Renewals** page, locate the target DB instance and click **More** > **Cancel Change to Pay-per-Use**.

Step 8 In the displayed dialog box, click **Yes**.

----End

3.2.4 Unsubscribing from a Yearly/Monthly Instance

If you do not need a yearly/monthly instance any longer, unsubscribe from it.

Precautions

- Unsubscribed operations cannot be undone. Exercise caution when performing this operation. To retain data, create a manual backup before unsubscription. For details, see **Creating a Manual Backup**.
- After an unsubscription request is submitted, resources and data will be deleted and cannot be retrieved. Ensure that the manual backup is complete before submitting the unsubscription request.

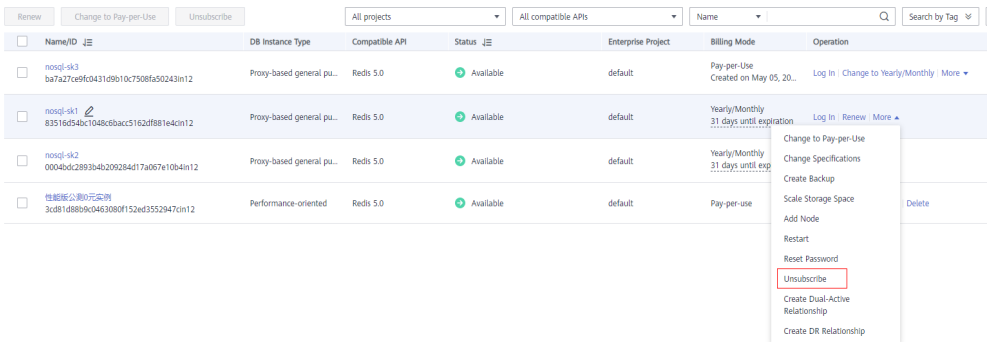
Unsubscribing from a Single Yearly/Monthly Instance

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

Step 2 In the service list, choose **Databases** > **GeminiDB**.

Step 3 On the **Instances** page, locate the instance you want to unsubscribe and choose **More** > **Unsubscribe** in the **Operation** column.

Figure 3-11 Unsubscribing from a yearly/monthly instance



Step 4 In the displayed dialog box, click **Yes**.

Step 5 On the displayed page, confirm the order to be unsubscribed and select a reason. Then, click **Confirm**.

For details about unsubscribing from resources, see **Unsubscription Rules**.

Step 6 In the displayed dialog box, click **Yes**.

NOTICE

1. After an unsubscription request is submitted, resources and data will be deleted and cannot be retrieved.
2. If you want to retain data, complete a manual backup before submitting the unsubscription request.

Step 7 View the unsubscription result. After the instance order is successfully unsubscribed, the instance is no longer displayed in the instance list on the **Instances** page.

----End

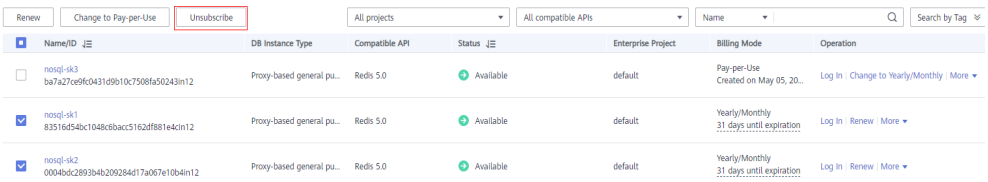
Unsubscribing from Multiple Yearly/Monthly Instances

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

Step 2 In the service list, choose **Databases** > **GeminiDB**.

Step 3 Choose **Instances** in the navigation pane on the left, select the instances you want to unsubscribe from and click **Unsubscribe** above the instance list.

Figure 3-12 Unsubscribing from multiple yearly/monthly instances



Step 4 In the displayed dialog box, click **Yes**.

Step 5 On the displayed page, confirm the order to be unsubscribed and select a reason. Then, click **Confirm**.

For details about unsubscribing from resources, see **Unsubscription Rules**.

Step 6 In the displayed dialog box, click **Yes**.

NOTICE

1. After an unsubscription request is submitted, resources and data will be deleted and cannot be retrieved.
2. If you want to retain data, complete a manual backup before submitting the unsubscription request.

Step 7 View the unsubscription result. After the instance order is successfully unsubscribed, the instance is no longer displayed in the instance list on the **Instances** page.

----End

3.3 Instance Statuses

The status of a DB instance indicates the health of the instance. You can view the DB instance statuses on the management console.

Table 3-1 DB instance statuses

Status	Description
Available	The instance is available.
Abnormal	The instance is abnormal.
Creating	The instance is being created.
Creation failed	The instance failed to be created.
Restarting	The instance is being restarted.
Resetting password	The administrator password is being reset.
Adding node	Nodes are being added to an instance.
Deleting node	Nodes are being deleted from an instance.
Scaling up	The storage space of an instance is being scaled up.
Changing instance class	The vCPUs and memory of an instance are being changed.
Changing to yearly/monthly	The billing mode is being changed from pay-per-use to yearly/monthly.
Changing to pay-per-use	The billing mode is being changed from yearly/monthly to pay-per-use.
Uploading backup	The backup file is being uploaded.
Backing up	A database backup is being created.
Checking restoration	The backup of the instance is being restored to a new instance.
Configuring SSL	SSL is being enabled or disabled.
Checking changes	The yearly/monthly instance is pending check when its billing mode is changed.

3.4 Instance Lifecycle Management

3.4.1 Restarting an Instance

Scenarios

You may need to restart an instance for routine maintenance.

Precautions

- Only instances in states **Available**, **Abnormal**, or **Checking restoration** can be restarted.
- After you restart an instance, all nodes in the instance are also restarted.
- Restarting an instance will interrupt services. Wait until off-peak hours and ensure that your application can re-connect.
- If you enable operation protection, two-factor authentication is required for sensitive operations to secure your account and cloud products. For details about how to enable operation protection, see ***Identity and Access Management User Guide***.

Procedure

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

Step 2 In the service list, choose **Databases** > **GeminiDB**.

Step 3 On the **Instances** page, locate the instance you want to restart and in the **Operation** column choose **Restart** or **More** > **Restart**.

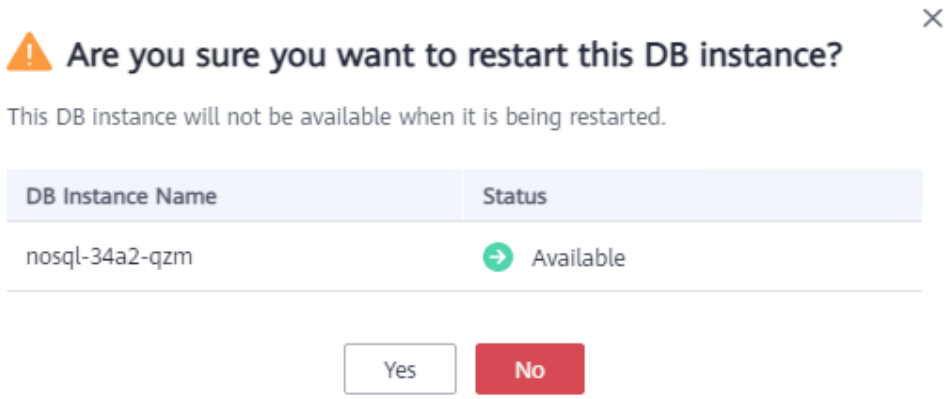
Alternatively, locate the instance you want to restart and click its name. On the displayed **Basic Information** page, click **Restart** in the upper right corner of the page.

Step 4 If you have enabled operation protection, click **Start Verification** in the **Restart DB Instance** dialog box. On the displayed page, click **Send Code**, enter the verification code, and click **Verify**. The page is closed automatically.

Step 5 In the displayed dialog box, click **Yes**.

For GeminiDB Redis instances, you can restart several nodes at the same time or in sequence based on service requirements.

Figure 3-13 Restarting the GeminiDB Redis instance



----End

3.4.2 Exporting Instance Information

Scenarios

You can export information about all or selected instances to view and analyze instance information.

Precautions

To enable this function, contact customer service.

Exporting All Instance Information

Step 1 Log in to the management console.

Step 2 In the service list, choose **Databases** > **GeminiDB**.

Step 3 On the **Instances** page, click in the upper right corner of the page. By default, information about all DB instances are exported. In the displayed dialog box, you can select the items to be exported and click **Export**.

Step 4 After the export task is complete, an XLS file is generated locally.

----End

Exporting Information About Selected Instances

Step 1 On the **Instances** page, select the instances that you want to export or search for required instances by project, compatible API, name, ID, or tag and click in the upper right corner of the page. In the displayed dialog box, select the items to be exported and click **Export**.

Step 2 After the export task is complete, an XLS file is generated locally.

----End

3.4.3 Deleting a Pay-per-Use Instance

Scenarios

You can choose to delete a pay-per-use instance on the **Instances** page based on service requirements. To delete a yearly/monthly instance, unsubscribe from it. For details, see **Unsubscribing from a Yearly/Monthly Instance**.

Precautions

- Instances that an operation is being performed on cannot be deleted. They can be deleted only after the operations are complete.
- If a instance is deleted, its automated backups will also be deleted and you will no longer be billed for them. Manual backups, however, will be retained and generate additional costs.
- After an instance is deleted, all its data and automated backups are automatically deleted as well and cannot be recovered. Back up the instance before you delete it. For details, see **Creating a Manual Backup**.
- After you delete an instance, all of its nodes are deleted.
- A deleted instance will be retained in the recycle bin for a period of time after being released, so you can rebuild the instance and restore data from it.

Procedure

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

Step 2 In the service list, choose **Databases** > **GeminiDB**.

Step 3 On the **Instances** page, locate the instance that you want to delete and in the **Operation** column choose **Delete** or **More** > **Delete**.

Step 4 If you have enabled operation protection, click **Start Verification** in the **Delete DB Instance** dialog box. On the displayed page, click **Send Code**, enter the verification code, and click **Verify**. The page is closed automatically.

NOTE

If you enable operation protection, two-factor authentication is required for sensitive operations to secure your account and cloud products. For details about how to enable operation protection, see ***Identity and Access Management User Guide***.

Step 5 In the displayed dialog box, click **Yes**.

Deleted instances are not displayed in the instance list any longer.

----End

3.4.4 Recycling an Instance

Unsubscribed yearly/monthly instances and deleted pay-per-use instances are moved to the recycle bin and can be restored.

Precautions

- The recycling bin is enabled by default and cannot be disabled. Instances in the recycle bin are retained for 7 days by default, and this will not incur any charges.
- You can put up to 100 instances into the recycle bin. If the maximum number of instances is reached, you cannot put instances into the recycle bin any more.
- If you delete an instance of full storage, the deleted instance will not be moved to the recycle bin.

Modifying the Recycling Policy

NOTICE

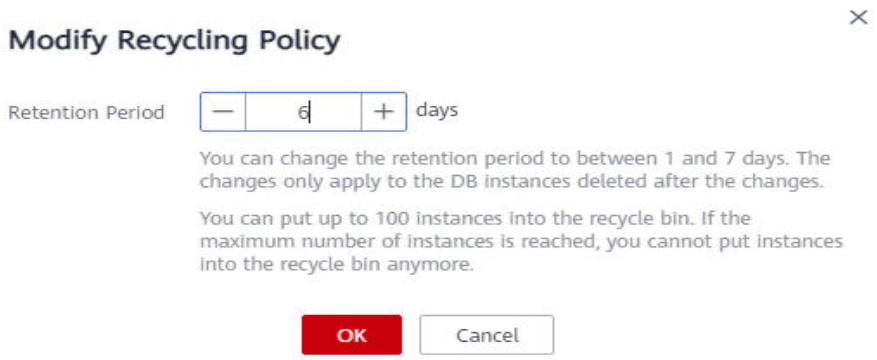
You can modify the retention period, and the new retention period only takes effect for the instances that are deleted after the modification.

Step 1 Log in to the management console.

Step 2 In the service list, choose **Databases** > **GeminiDB**.

Step 3 On the **Recycling Bin** page, click **Modify Recycling Policy**. In the displayed dialog box, set the retention period from 1 day to 7 days. Then, click **OK**.

Figure 3-14 Modifying the recycling policy



----End

Rebuilding an Instance

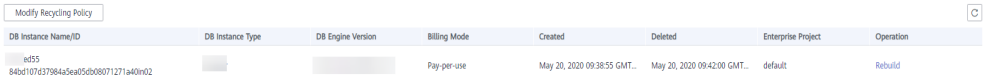
You can rebuild DB instances from the recycle bin within the retention period to restore data.

Step 1 Log in to the management console.

Step 2 In the service list, choose **Databases** > **GeminiDB**.

Step 3 On the **Recycling Bin** page, locate the instance that you want to rebuild and click **Rebuild** in the **Operation** column.

Figure 3-15 Rebuilding an instance



Step 4 On the displayed page, set required parameters and submit the rebuilding task.

----End

3.5 Instance Changes

3.5.1 Modifying the Name of an Instance

Scenarios

This section describes how to modify the name of a GeminiDB Redis instance.

Method 1

Step 1 Log in to the management console.

Step 2 In the service list, choose **Databases** > **GeminiDB**.

Step 3 On the **Instances** page, locate the instance whose name you want to modify and click to the right of the instance.

- To submit the change, click **OK**.
- To cancel the change, click **Cancel**.

NOTE

The instance name:

- Can be the same as an existing instance name.
- Can include 4 to 64 bytes and must start with a letter. It is case-sensitive and allows only letters, digits, hyphens (-), and underscores (_).

Step 4 View the results on the **Instances** page.

----End

Method 2

Step 1 Log in to the management console.

Step 2 In the service list, choose **Databases** > **GeminiDB**.

Step 3 On the **Instances** page, click the instance whose name you want to modify and click its name.

Step 4 In the **Instance Information** area on the **Basic Information** page, click in the **DB Instance Name** field.

- To submit the change, click  .
- To cancel the change, click  .

Step 5 View the results on the **Instances** page.

----End

3.5.2 Changing the Administrator Password of a GeminiDB Redis Instance

Scenarios

For security reasons, regularly change your administrator password.

Precautions

- You can reset the administrator password only when the **instance status** is **Available**, **Backing up**, or **Scaling up**.
- If you enable operation protection, two-factor authentication is required for sensitive operations to secure your account and cloud products. For details about how to enable operation protection, see ***Identity and Access Management User Guide***.

Method 1

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

Step 2 In the service list, choose **Databases** > **GeminiDB**.

Step 3 On the **Instances** page, locate the instance whose administrator password you want to reset and choose **More** > **Reset Password** in the **Operation** column.

Step 4 Enter and confirm the new administrator password and click **OK**.

The password must be 8 to 32 characters in length and contain any two of uppercase letters, lowercase letters, digits, and the following special characters: ~!@#%^*-_=+?$()&

Step 5 If you have enabled operation protection, click **Start Verification** in the displayed dialog box. On the displayed page, click **Send Code**, enter the verification code, and click **Verify**. The page is closed automatically.

----End

Method 2

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

Step 2 In the service list, choose **Databases** > **GeminiDB**.

Step 3 On the **Instances** page, locate the instance whose administrator password you want to reset and click its name. The **Basic Information** page is displayed.

Step 4 In the **DB Information** area, click **Reset Password** in the **Administrator** field.

Step 5 Enter and confirm the new administrator password and click **OK**.

The password must be 8 to 32 characters in length and contain any two of uppercase letters, lowercase letters, digits, and the following special characters: ~!@#%^*-_=+?$()&

Step 6 If you have enabled operation protection, click **Start Verification** in the displayed dialog box. On the displayed page, click **Send Code**, enter the verification code, and click **Verify**. The page is closed automatically.

----End

3.5.3 Scaling Up Storage Space

Scenarios

This section describes how to scale up storage space of an instance to suit your service requirements.

Precautions

- Storage space can only be scaled up.
- When the disk usage of a GeminiDB Redis instance exceeds 95%, the instance enters the read-only mode. You can only read or delete data from the instance, but cannot write new data into it. To keep services accessible, scale up storage space when the disk usage exceeds 80%.
- **Storage scaling does not interrupt your services. After storage scaling is complete, you do not need to restart your instance.**

Method 1

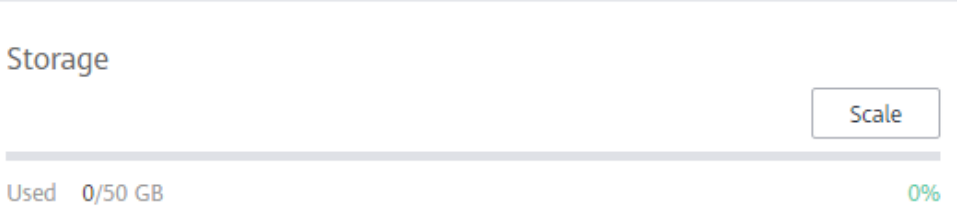
Step 1 Log in to the management console.

Step 2 In the service list, choose **Databases** > **GeminiDB**.

Step 3 On the **Instances** page, locate the instance whose storage space you want to scale up and click its name.

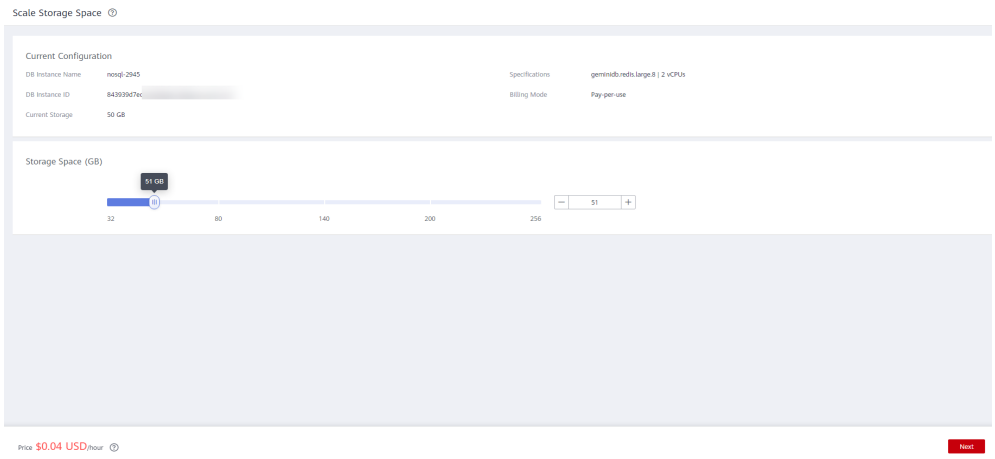
Step 4 In the **Storage Space** area on the **Basic Information** page, click **Scale**.

Figure 3-16 Scaling storage



Step 5 On the displayed page, specify the new storage capacity and click **Next**.

Figure 3-17 Scaling storage



Select at least 1 GB each time you scale up the storage, and the storage size must be an integer.

Step 6 On the displayed page, confirm the storage space.

- For yearly/monthly instances
  - If you need to modify your settings, click **Previous**.
  - If you do not need to modify your settings, click **Submit** and complete the payment.
- For pay-per-use instances
  - If you need to modify your settings, click **Previous**.
  - If you do not need to modify your settings, click **Submit**.

Step 7 Check the scaling result.

- When the scaling task is ongoing, the instance status is **Scaling up**.
- After the scaling task is complete, the instance status becomes **Available**.
- In the **Storage Space** area on the **Basic Information** page, view the new storage space.

----End

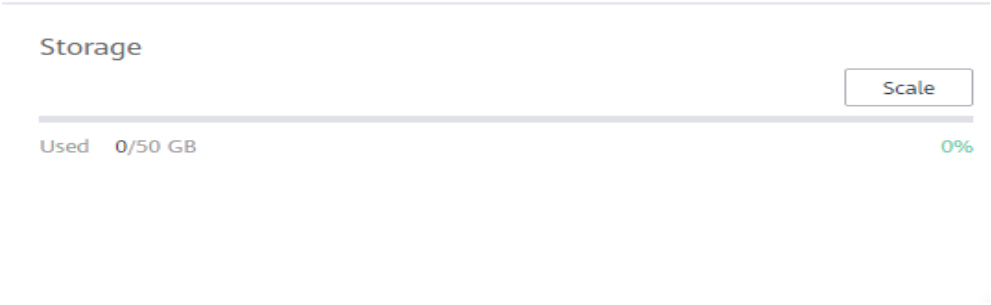
Method 2

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

Step 2 In the service list, choose **Databases** > **GeminiDB**.

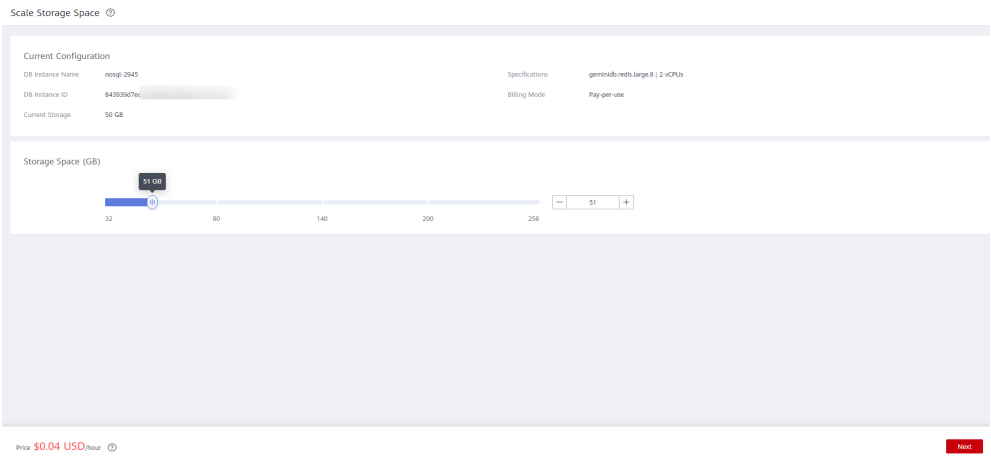
Step 3 On the **Instances** page, locate the instance whose storage space you want to scale and choose **More** > **Scale Storage Space** in the **Operation** column.

Figure 3-18 Scaling storage



Step 4 On the displayed page, specify the new storage capacity and click **Next**.

Figure 3-19 Scaling storage



Select at least 1 GB each time you scale up the storage, and the storage size must be an integer.

Step 5 On the displayed page, confirm the storage space.

- For yearly/monthly instances
  - If you need to modify your settings, click **Previous**.
  - If you do not need to modify your settings, click **Submit** and complete the payment.
- For pay-per-use instances
  - If you need to modify your settings, click **Previous**.
  - If you do not need to modify your settings, click **Submit**.

Step 6 Check the scaling result.

- When the scaling task is ongoing, the instance status is **Scaling up**.
- After the scaling task is complete, the instance status becomes **Available**.
- In the **Storage Space** area on the **Basic Information** page, view the new storage space.

----End

3.5.4 Changing the CPU and Memory Specifications of an Instance

Scenarios

You can change the vCPU and memory specifications of your instance to meet your service requirements.

Precautions

- Instances can be scaled up or down by changing their specifications.
- If one instance has multiple nodes, the change will be performed on the nodes one by one. It takes about 5 to 10 minutes for each node, and the total time required depends on the number of the nodes.
- For a node whose specifications are being changed, its computing tasks are handed over to other nodes. Change specifications of nodes during off-peak hours to prevent the instance from overload.

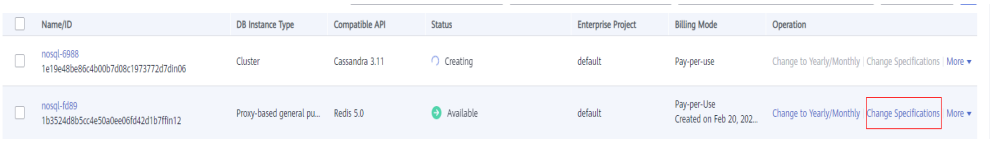
Procedure

Step 1 Log in to the management console.

Step 2 In the service list, choose **Databases** > **GeminiDB**.

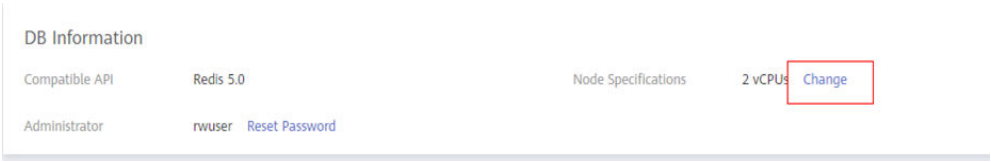
Step 3 On the **Instances** page, locate the instance whose specifications you want to change and click **More** > **Change Specifications** in the **Operation** column.

Figure 3-20 Changing specifications



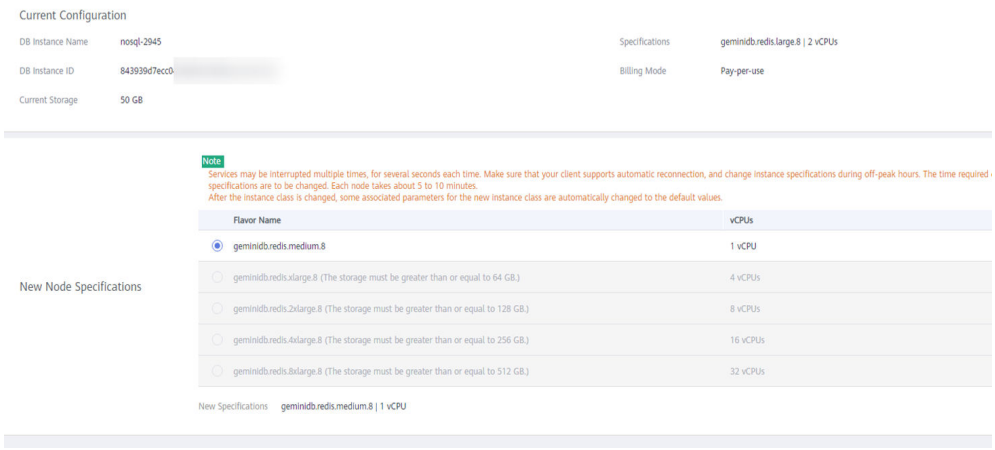
In the **DB Information** area on the **Basic Information** page, click **Change** next to the **Specifications** field.

Figure 3-21 Changing the specifications



Step 4 On the displayed page, select the required specifications and click **Next**.

Figure 3-22 Changing specifications



Step 5 On the displayed page, confirm the specifications.

- If you need to modify your settings, click **Previous**.
- If you do not need to modify your settings, click **Submit** .

Step 6 View the results.

Go to the **Basic Information** page and in the **DB Information** area you can see the new instance specifications.

----End

3.5.5 Adding Nodes

Scenarios

This section describes how to add nodes to an instance to suit your service requirements. You can also delete a node as required. For details, see **Deleting Nodes**.

Precautions

- Adding nodes will trigger fast load balancing, which may cause a request timeout for a few seconds. Enable automatic retry for services.
- You can add nodes only when the instance status is **Available** or **Checking restoration**.
- An instance cannot be deleted when one or more nodes are being added.
- If the storage is insufficient, adding nodes is not supported. Expand the storage first. For details about the storage supported by instances of different specifications, see **Instance Specifications**.

Method 1

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

Step 2 In the service list, choose **Databases** > **GeminiDB**.

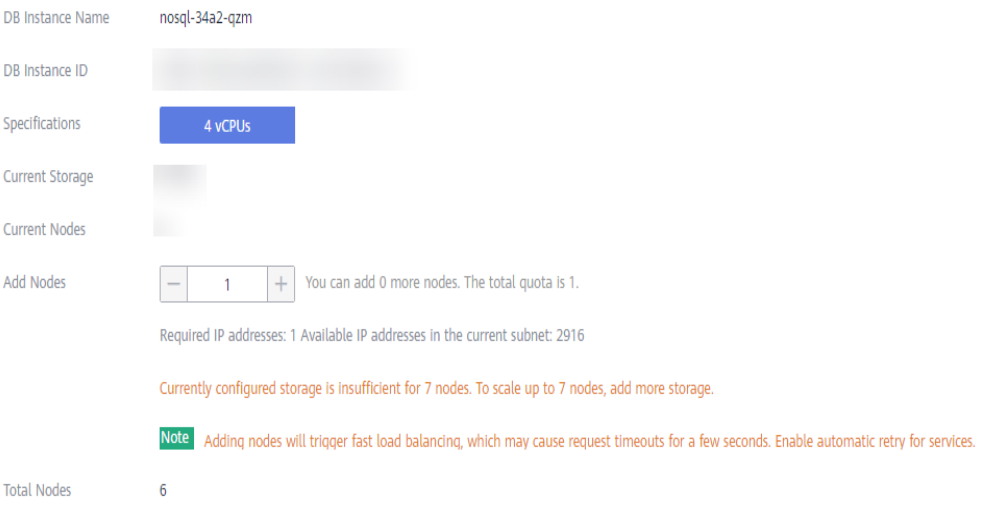
Step 3 On the **Instances** page, locate the instance you want to add nodes for and click its name.

Step 4 In the **Node Information** area on the **Basic Information** page, click **Add Node**.

Figure 3-23 Adding nodes

Step 5 Specify **Add Nodes** and click **Next**.

Figure 3-24 Add Node



New nodes are of the same specifications as existing nodes. Once a new node is added, its specifications cannot be changed.

Step 6 On the displayed page, confirm the node configuration details.

- For yearly/monthly instances
  - If you need to modify your settings, click **Previous**.
  - If you do not need to modify your settings, click **Submit** and complete the payment.
- For pay-per-use instances
  - If you need to modify the settings, click **Previous**.
  - If you do not need to modify the settings, click **Submit**.

Step 7 View the results.

- The status of the DB instance in the instance list is **Adding node**.
- After the nodes are added, the DB instance status becomes **Available**.
- Click the instance name. In the **Node Information** area on the **Basic Information** page, view the information about the new nodes.

----End

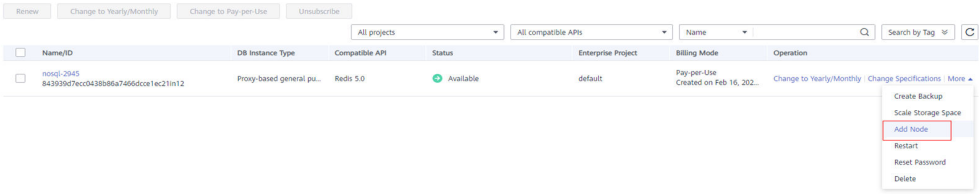
Method 2

Step 1 Log in to the management console.

Step 2 In the service list, choose **Databases** > **GeminiDB**.

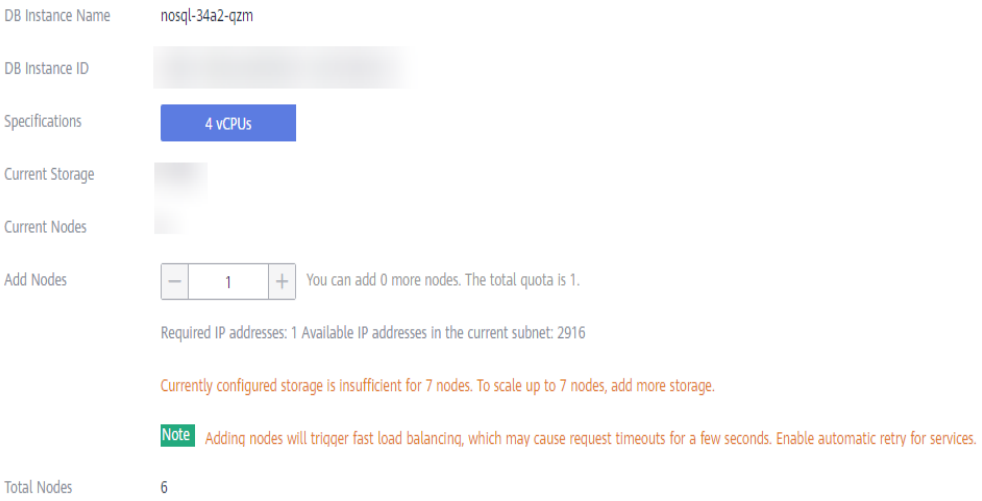
Step 3 On the **Instances** page, locate the instance which you want to add nodes for, click its name, and choose **More** > **Add Node** in the **Operation** column.

Figure 3-25 Adding nodes



Step 4 Specify **Add Nodes** and click **Next**.

Figure 3-26 Add Node



New nodes are of the same specifications as existing nodes. Once a new node is added, its specifications cannot be changed.

Step 5 On the displayed page, confirm the node configuration details.

- For yearly/monthly instances
  - If you need to modify your settings, click **Previous**.
  - If you do not need to modify your settings, click **Submit** and complete the payment.
- For pay-per-use instances
  - If you need to modify the settings, click **Previous**.
  - If you do not need to modify the settings, click **Submit**.

Step 6 View the results.

- The status of the DB instance in the instance list is **Adding node**.
- After the nodes are added, the DB instance status becomes **Available**.
- Click the instance name. In the **Node Information** area on the **Basic Information** page, view the information about the new nodes.

----End

3.5.6 Deleting Nodes

Scenarios

You can add or delete nodes for a pay-per-use or yearly/monthly instance to release resources.

Precautions

- Deleted nodes cannot be recovered. Exercise caution when performing this operation.
- If you enable operation protection, two-factor authentication is required for sensitive operations to secure your account and cloud products. For details about how to enable operation protection, see ***Identity and Access Management User Guide***.

Procedure

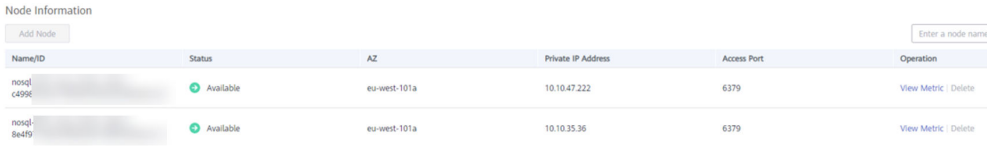
Step 1 **Log in to the management console**.

Step 2 In the service list, choose **Databases** > **GeminiDB**.

Step 3 On the **Instances** page, locate the instance that you want to delete nodes from and click its name.

Step 4 On the **Basic Information** page, at the **Node Information** area, locate the node that you want to delete and click **Delete**.

Figure 3-27 Node information



Step 5 If you have enabled operation protection, click **Start Verification** in the **Delete Node** dialog box. On the displayed page, click **Send Code**, enter the verification code, and click **Verify**. The page is closed automatically.

Step 6 In the displayed dialog box, click **Yes**.

- When the node is being deleted, the instance status is **Deleting node**.
- After the node is deleted, the instance status becomes **Available**.

----End

3.5.7 Managing Tags

Scenarios

Tag Management Service (TMS) enables you to use tags on the management console to manage resources. TMS works with other cloud services to manage global tags, and other cloud services manage their own tags.

Adding tags to GeminiDB Redis instances helps you better identify and manage them. A DB instance can be tagged during or after it is created.

After a DB instance is tagged, you can search for the tag key or value to quickly query the instance details.

Precautions

- You are advised to set predefined tags on the TMS console.
- A tag consists of a key and value. You can add only one value for each key. For details about the naming rules of tag keys and tag values, see **Table 3-2**.
- Each instance can have up to 20 tags by default.
- The tag name must comply with the naming rules described in **Table 3-2**.

Table 3-2 Naming rules

Parameter	Requirement	Example Value
Tag key	• Cannot be left blank. • Must be unique for each instance. • Contains a maximum of 36 characters. • Can only consist of digits, letters, underscores (_), and hyphens (-).	Organization
Tag value	• Can be left blank. • Contains a maximum of 43 characters. • Can only consist of digits, letters, underscores (_), periods (.), and hyphens (-).	nosql_01

Adding a Tag

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

Step 2 In the service list, choose **Databases** > **GeminiDB**.

Step 3 On the **Instances** page, click the instance that you want to add tags to and click its name.

Step 4 In the navigation pane on the left, choose **Tags**.

Step 5 On the **Tags** page, click **Add Tag**. In the displayed dialog box, enter a tag key and value, and click **OK**.

Step 6 View and manage the tag on the **Tags** page.

----End

Editing a Tag

Step 1 Log in to the management console.

Step 2 In the service list, choose **Databases** > **GeminiDB**.

Step 3 On the **Instances** page, locate the instance whose tags you want to edit and click its name.

Step 4 In the navigation pane on the left, choose **Tags**.

Step 5 On the **Tags** page, locate the tag to be edited and click **Edit** in the **Operation** column. In the displayed dialog box, change the tag value and click **OK**.

Only the tag value can be edited.

Step 6 View and manage the tag on the **Tags** page.

----End

Deleting a Tag

Step 1 Log in to the management console.

Step 2 In the service list, choose **Databases** > **GeminiDB**.

Step 3 On the **Instances** page, locate the instance whose tags you want to delete and click its name.

Step 4 In the navigation pane on the left, choose **Tags**.

Step 5 On the **Tags** page, locate the tag to be deleted and click **Delete** in the **Operation** column. In the displayed dialog box, click **Yes**.

Step 6 View that the tag is no longer displayed on the **Tags** page.

----End

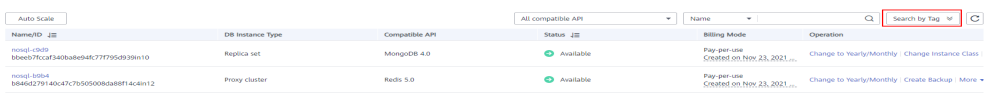
Searching an Instance by Tag

Step 1 Log in to the management console.

Step 2 In the service list, choose **Databases** > **GeminiDB**.

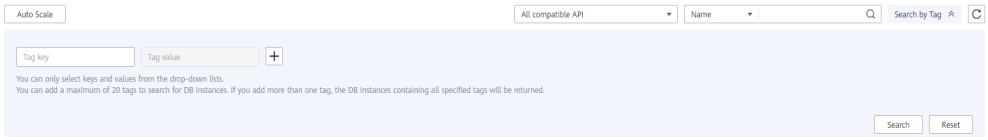
Step 3 On the **Instances** page, click **Search by Tag** in the upper right corner of the instance list.

Figure 3-28 Search by Tag



Step 4 Enter a tag key or value and click **Search** to query the instance associated with the tag.

Figure 3-29 Searching by tag key



----End

3.5.8 Updating the OS of an Instance

To improve database performance and security, the OS of a GeminiDB Redis instance needs to be updated in a timely manner.

Every time you upgrade the kernel version of your instance, GeminiDB Redis determines whether to update the OS and selects the right cold patch to upgrade the OS if necessary.

Updating the OS does not change the DB instance version or other information.

In addition, GeminiDB Redis installs hot patches as required to fix major OS vulnerabilities within the maintenance window you specified.

3.6 Audit

3.6.1 Key Operations Supported by CTS

With CTS, you can record GeminiDB Redis key operations for later query, audit, and backtracking.

Table 3-3 GeminiDB Redis key operations

Operation	Resource Type	Trace Name
Creating an instance	instance	NoSQLCreateInstance
Deleting an instance	instance	NoSQLDeleteInstance
Adding nodes	instance	NoSQLEnlargeInstance
Deleting nodes	instance	NoSQLReduceInstance
Restarting an instance	instance	NoSQLRestartInstance
Restoring data to a new instance	instance	NoSQLRestoreNewInstance
Scaling up storage space of an instance	instance	NoSQLExtendInstanceVolume

Operation	Resource Type	Trace Name
Resetting the password of an instance	instance	NoSQLResetPassword
Modifying the name of an instance	instance	NoSQLRenameInstance
Binding an EIP	instance	NoSQLResizeInstance
Unbinding an EIP	instance	NoSQLBindEIP
Changing specifications	instance	NoSQLUnBindEIP
Freezing an instance	instance	NoSQLFreezeInstance
Unfreezing an instance	instance	NoSQLUnfreezeInstance
Creating a backup	backup	NoSQLCreateBackup
Deleting a backup	backup	NoSQLDeleteBackup
Setting a backup policy	backup	NoSQLSetBackupPolicy
Adding an instance tag	tag	NoSQLAddTags
Modifying an instance tag	tag	NoSQLModifyInstanceTag
Deleting an instance tag	tag	NoSQLDeleteInstanceTag
Creating a parameter template	parameterGroup	NoSQLCreateConfigurations
Modifying a parameter template	parameterGroup	NoSQLUpdateConfigurations
Modifying instance parameters	parameterGroup	NoSQLUpdateInstanceConfigurations
Replicating a parameter template	parameterGroup	NoSQLCopyConfigurations
Resetting a parameter template	parameterGroup	NoSQLResetConfigurations
Applying a parameter template	parameterGroup	NoSQLApplyConfigurations
Deleting a parameter template	parameterGroup	NoSQLDeleteConfigurations
Deleting the node that fails to be added	instance	NoSQLDeleteEnlargeFailNode
Enabling SSL	instance	NoSQLSwitchSSL
Changing the security group of an instance	instance	NoSQLModifySecurityGroup

Operation	Resource Type	Trace Name
Creating a dual-active relationship	instance	NoSQLBuildBiactiveInstance
Modifying the recycling policy	instance	NoSQLModifyRecyclePolicy

3.6.2 Querying Traces

Scenarios

After CTS is enabled, CTS starts recording operations on cloud resources. The CTS console stores the last 7 days of operation records for later query, audit, and backtracking.

This section describes how to query the last 7 days of operation records on the CTS console.

Procedure

Step 1 Log in to the management console.

Step 2 Click **Service List**. Under **Management & Governance**, click **Cloud Trace Service**.

Step 3 Choose **Trace List** in the navigation pane on the left.

Step 4 Click **Filter** and specify filter criteria as needed. The following filters are available:

- **Trace Type**: Select **Management** or **Data**.
- **Trace Source**, **Resource Type**, and **Search By**

  Select a filter from the drop-down list.

  When you select **Trace name** for **Search By**, you also need to select a specific trace name.

  When you select **Resource ID** for **Search By**, you also need to select or enter a specific resource ID.

  When you select **Resource name** for **Search By**, you also need to select or enter a specific resource name.
- **Operator**: Select a specific operator (a user rather than tenant).
- **Trace Status**: Available options include **All trace statuses**, **normal**, **warning**, and **incident**. You can only select one of them.
- Start time and end time: You can specify a time range for querying traces.

Step 5 Click ⌄ on the left of the record to be queried to extend its details.

Step 6 Locate a trace and click **View Trace** in the **Operation** column.

----End

3.7 Connecting to an Instance

3.7.1 Configuring a Private Domain Name

This section describes how to configure and resolve private domain names.

Creating a Private Domain Name

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

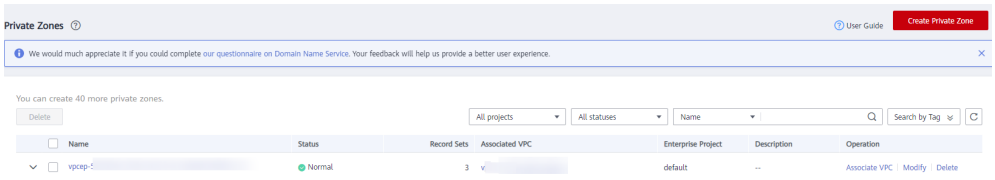
Step 2 Click **Service List**. Under **Network**, click **Domain Name Service**.

Step 3 On the DNS console, choose **Private Zones**.

Figure 3-30 Private zones

Step 4 Click **Create Private Zone**.

Figure 3-31 Creating a private domain name



Step 5 Configure parameters for creating a private domain name.

Figure 3-32 Creating a private zone

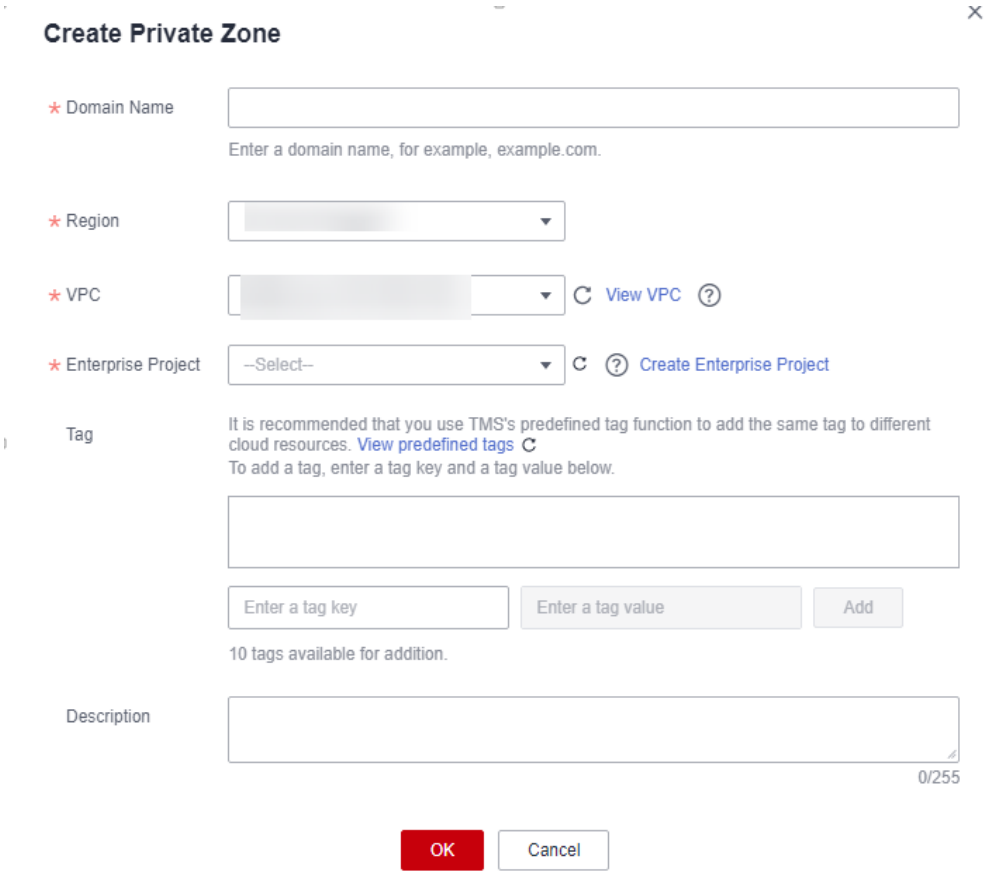


Table 3-4 Parameter description

Parameter	Description	Example
Domain Name	Domain name of the private zone. You can customize any correctly formatted domain names, even top-level ones. For details about the domain name format, see **Domain Name Format and DNS Hierarchy**.	example.com
Region	The region where the tenant is located.	CN East-Shanghai1

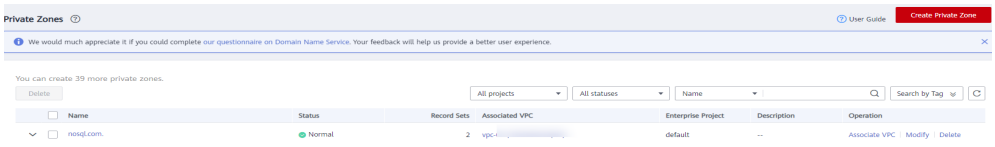
Parameter	Description	Example
VPC	The VPC associated with the private domain name must be the same as the VPC where the GeminiDB Redis instance is located. Otherwise, the private domain name cannot be resolved.	-
Enterprise Project	Enterprise project associated with the private domain name. You can manage private domain names by enterprise project. **NOTE** This parameter is available and mandatory only when **Account Type** is set to **Enterprise Account**. Configuration principles: ● If you do not manage domain names by enterprise project, select the **default** enterprise project. ● If you manage domain names by enterprise project, select an existing enterprise project.	default

Parameter	Description	Example
Tags	(Optional) Identifier of a resource. Each tag contains a key and a value. You can add a maximum of 10 tags to a domain name. The key and value naming rules are as follows: **Key**: • Cannot be left blank. • Must be unique for each resource. • Consists of a maximum of 36 characters. • Cannot start or end with a space or contain special characters =*<>\,|/ **Value**: • Cannot be left blank. • Consists of a maximum of 43 characters. • Cannot start or end with a space or contain special characters =*<>\,|/	example_key1 example_value1
Description	(Optional) Description of the zone, which cannot exceed 255 characters.	This is a zone example.

Step 6 Click **OK**. On the **Private Zones** page, view the created private domain name in the zone list.

If the status of the private domain name is **Normal**, the domain name has been successfully created.

Figure 3-33 Viewing the private domain name status



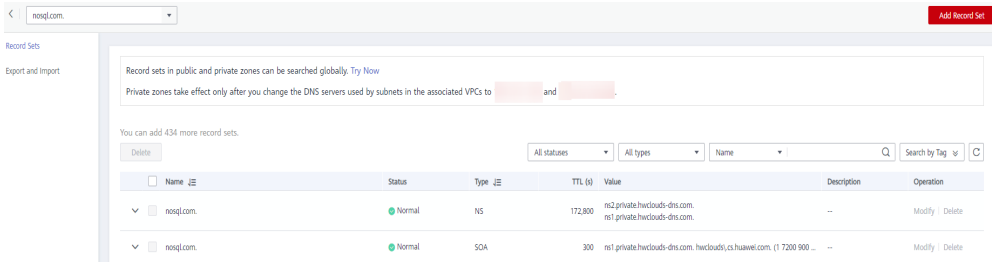
----End

Adding a Record Set for a Domain Name

After creating a private domain name, configure a record set for it so that you can access instances using the domain name.

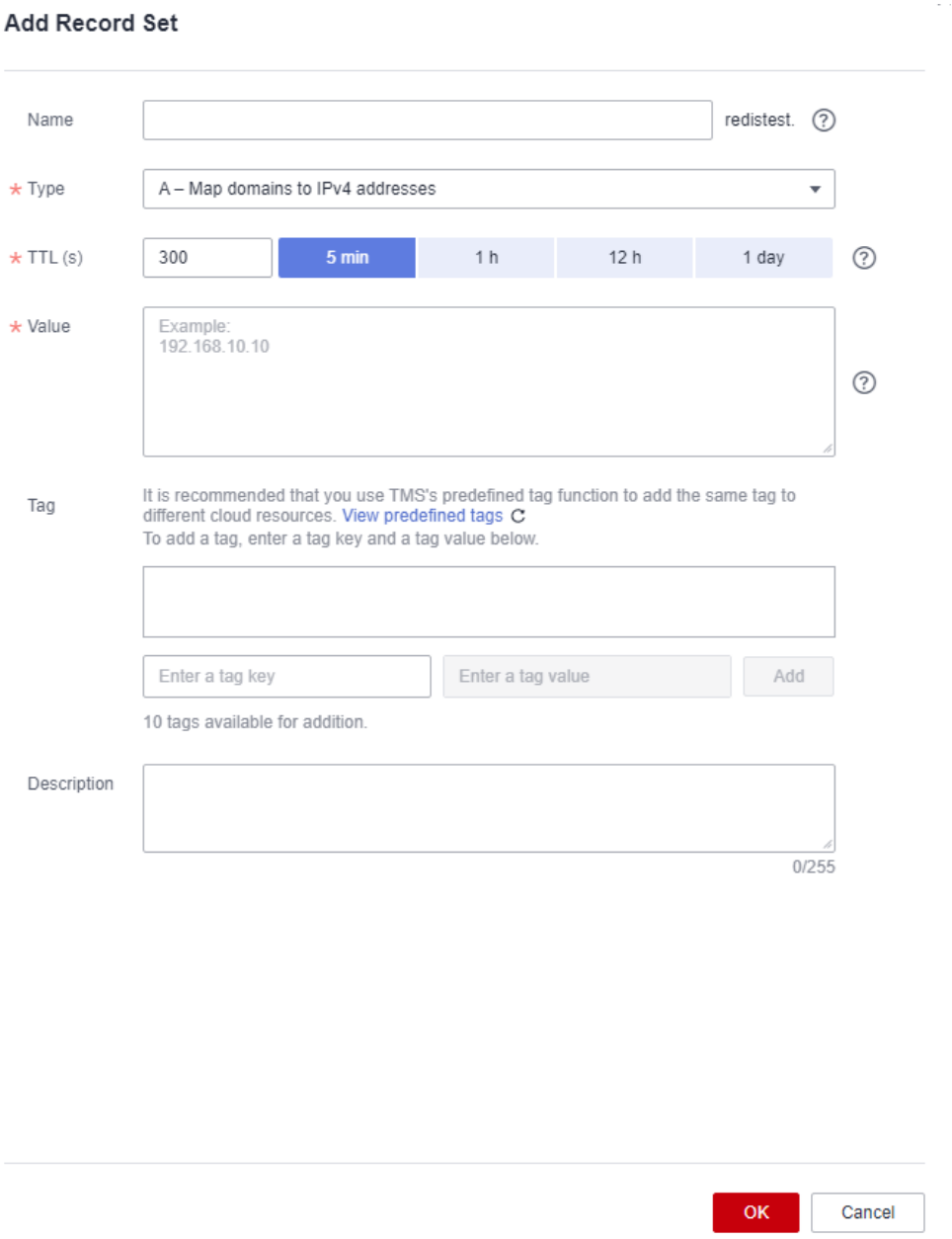
Step 1 Click the private domain name you created. On the displayed page, click **Add Record Set** in the upper right corner.

Figure 3-34 Adding a record set



Step 2 In the displayed **Add Record Set** dialog box, configure the required parameters.

Figure 3-35 Adding a record set



For details about how to configure parameters, see **Adding an A Record Set**.

Step 3 Click **OK**.

Step 4 Switch back to the **Record Sets** page.

Step 5 View the created record set in the record set list. If the status of the record set is **Normal**, the record set is added successfully.

----End

3.7.2 Configuring a Public Domain Name

This section describes how to configure and resolve public domain names.

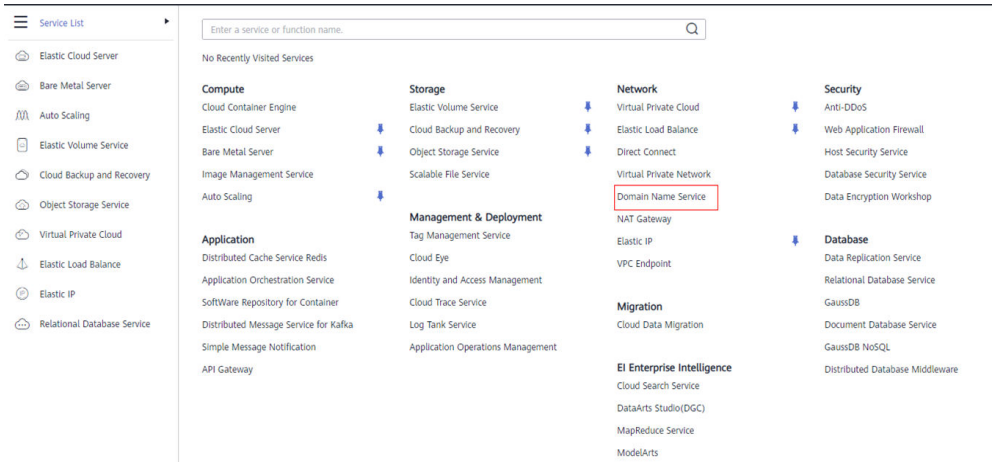
Procedure

If your domain name is registered with a third-party registrar, create a public zone and add record sets to it on the DNS console.

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

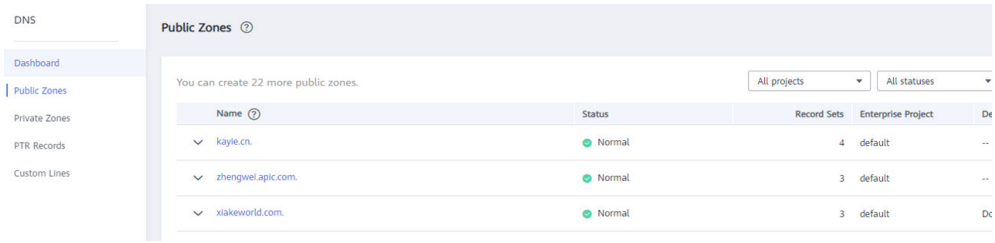
Step 2 Click **Service List** and choose **Network** > **Domain Name Service**.

Figure 3-36 Domain Name Service



Step 3 In the navigation pane on the left, choose **Public Zones**.

Figure 3-37 Public zones



Step 4 In the upper right corner of the page, click **Create Public Zone**.

Step 5 Set the required parameters.

Figure 3-38 Creating a public zone

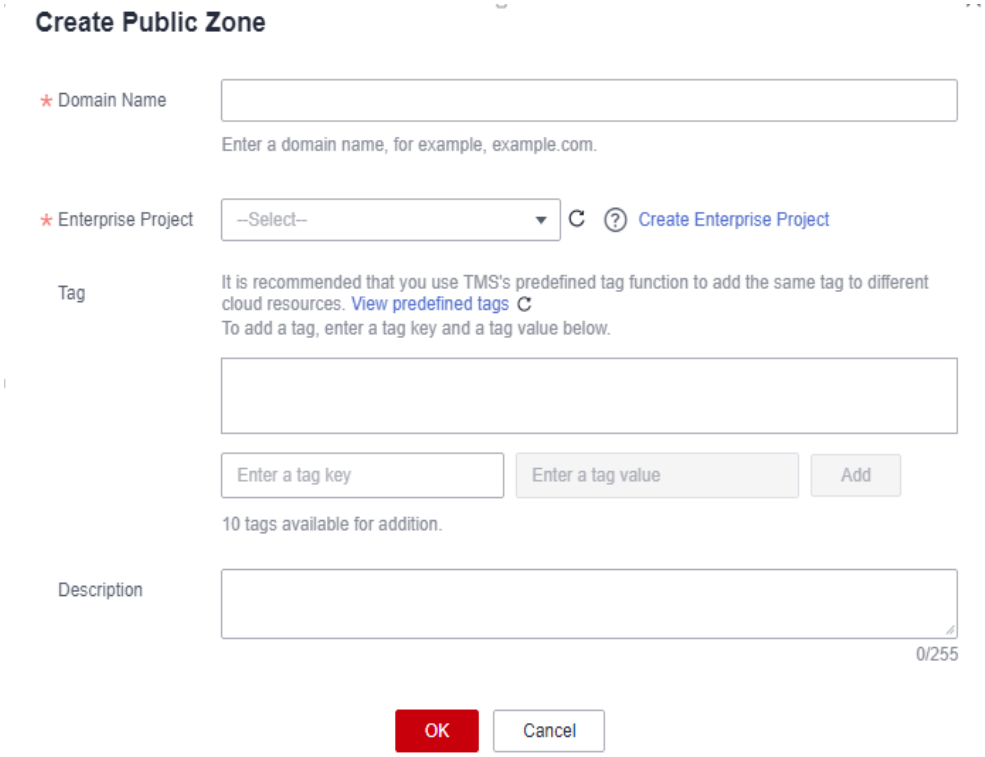


Table 3-5 Public zone parameters

Parameter	Description	Example
Domain Name	The domain name registered with the domain name registrar. The domain name can include two levels in addition to the top-level domain, for example: • abc.example.com, the subdomain name of example.com • abc.example.com.cn, the subdomain name of example.com.cn For details about the domain name format, see **Domain Name Formats and Structure**.	example.com

Parameter	Description	Example
Enterprise Project	Enterprise project associated with the public domain name. You can manage public domain names by enterprise project. **NOTE** This parameter is available and mandatory only when **Account Type** is set to **Enterprise Account**. Configuration principles: • If you do not manage domain names by enterprise project, select the **default** enterprise project. • If you manage domain names by enterprise project, select an existing enterprise project.	default

Parameter	Description	Example
Tag	(Optional) Identifier of a resource. Each tag contains a key and a value. You can add a maximum of 10 tags to a domain name. The key and value naming rules are as follows: **Key**: ● Cannot be left blank. ● Must be unique for each resource. ● Consists of a maximum of 36 characters. ● Cannot start or end with a space or contain special characters =*<>\,|/ **Value**: ● Cannot be left blank. ● Consists of a maximum of 43 characters. ● Cannot start or end with a space or contain special characters =*<>\,|/	example_key1 example_value1
Description	(Optional) Description of the zone, which cannot exceed 255 characters.	This is a zone example.

Step 6 Click **OK**.

After the domain name is created, you can view it in the domain name list on the **Public Zones** page.

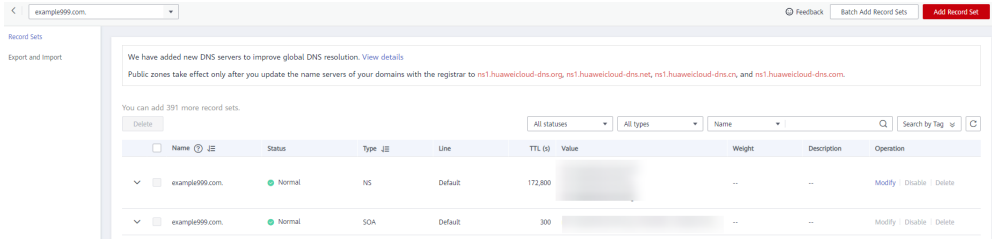
----End

Adding a Record Set for a Domain Name

After creating a public domain name, configure a record set for it so that you can access instances using the domain name.

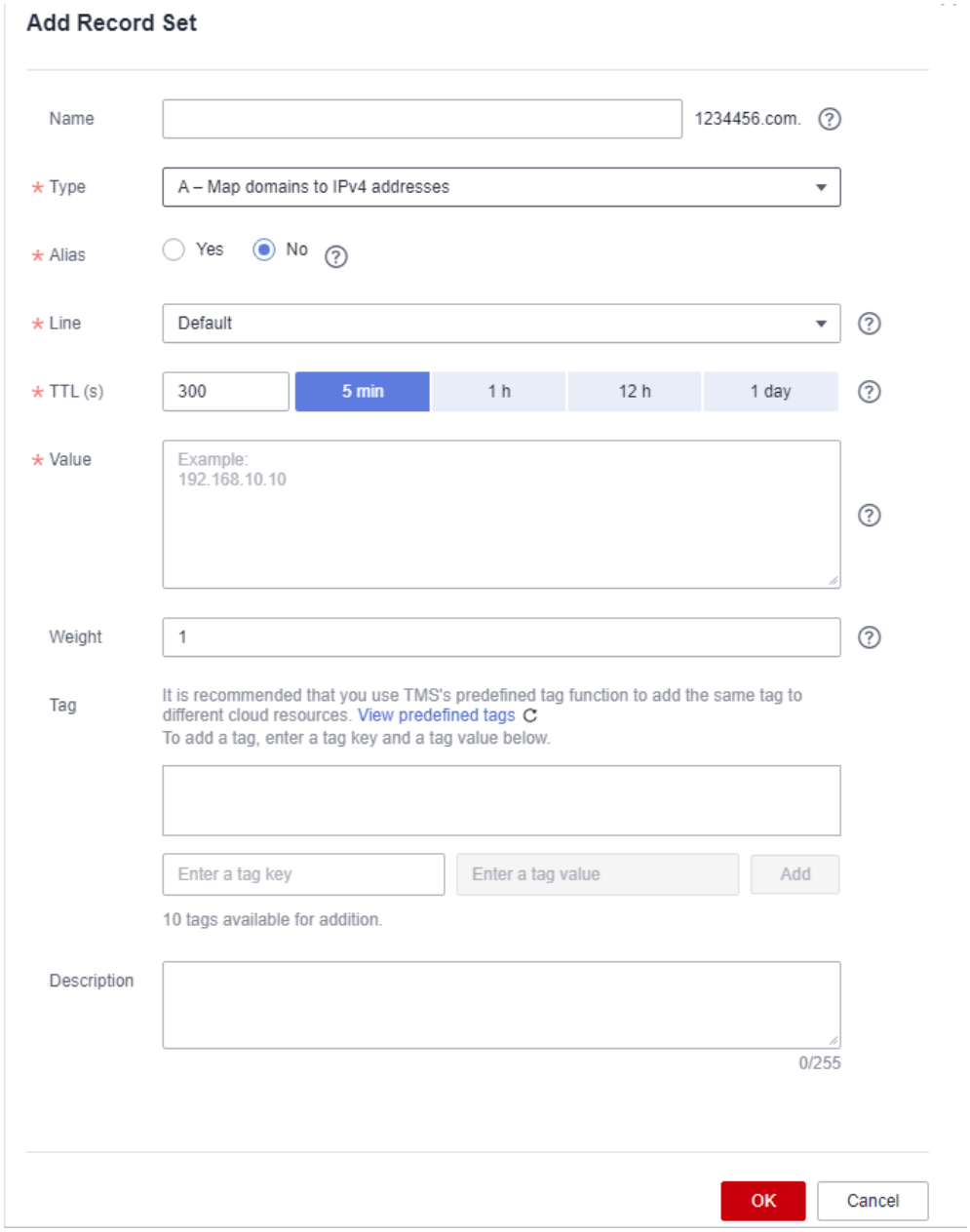
Step 1 Click the name of the public domain name you created. On the displayed page, click **Add Record Set** in the upper right corner.

Figure 3-39 Adding a record set



Step 2 In the displayed **Add Record Set** dialog box, configure the required parameters.

Figure 3-40 Adding a record set



For details about how to configure parameters, see **Adding an A Record Set**.

Step 3 Click **OK**.

Step 4 Switch back to the **Record Sets** page.

Step 5 View the created record set in the record set list. If the status of the record set is **Normal**, the record set is added successfully.

----End

3.7.3 Configuring Security Group Rules

A security group is a collection of access control rules for ECSs and GeminiDB Redis instances that have the same security protection requirements and are mutually trusted in a VPC.

To ensure database security and reliability, configure security group rules to allow specific IP addresses and ports to access the GeminiDB Redis instances.

This section describes how to configure security group rules for a GeminiDB Redis instance that is connected through a private or a public network.

Precautions

- Each account can create up to 500 security group rules by default.
- Too many security group rules will increase the first packet latency, so a maximum of 50 rules for each security group is recommended.
- One security group can be associated with only one GeminiDB Redis instance.
- For details about how to configure security group rules, see **Table 3-6**.

Table 3-6 Parameter description

Scenario	Description
Connecting to an instance over a private network	Configure security group rules as follows: • If a GeminiDB Redis instance and the ECS used for accessing the instance are in the same security group, they can communicate with each other by default. No security group rules need to be configured. • If the instance and the ECS are not in the same security group, configure security group rules, respectively. – Configure inbound rules for the security group associated with the GeminiDB Redis instance. For details, see **Procedure**. – There is no need to configure security rules for the ECS because the default security group rule of the ECS allows all outbound data packets. If not all outbound traffic is allowed in the security group, configure an outbound rule for the ECS.

Scenario	Description
Connecting to an instance over a public network	If you connect to a GeminiDB Redis instance through a public network, configure inbound rules for the security group associated with the GeminiDB Redis instance. For details, see **Procedure**.

Procedure

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

Step 2 In the service list, choose **Databases** > **GeminiDB**.

Step 3 On the **Instances** page, locate the instance that you want to configure security group rules for and click its name.

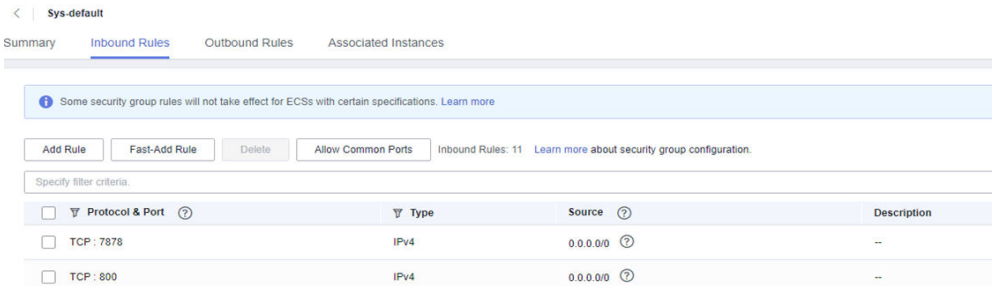
Step 4 Configure security group rules.

Figure 3-41 Security group

Step 5 Add Inbound Rule

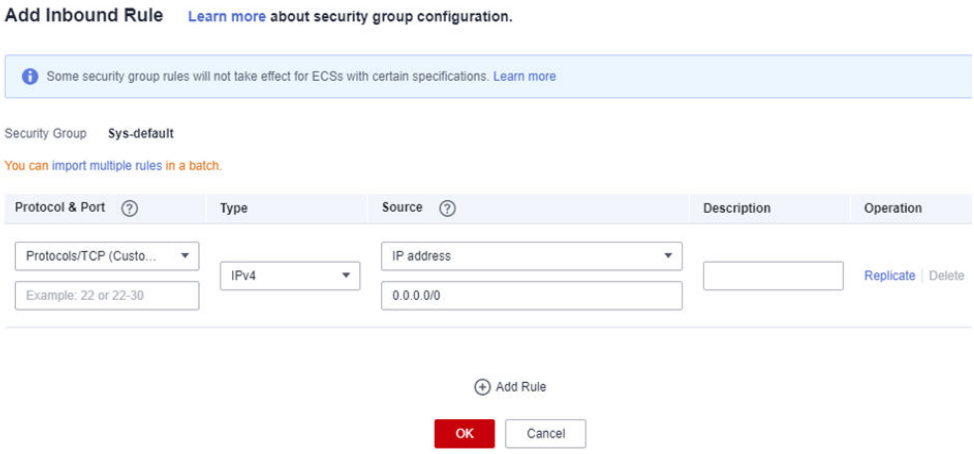
1. Click the **Inbound Rules** tab.

Figure 3-42 Inbound rules



2. Click **Add Rule**. The **Add Inbound Rule** dialog box is displayed.

Figure 3-43 Adding a rule



3. Add a security group rule as prompted.

Table 3-7 Inbound rule settings

Parameter	Description	Example Value
Protocol & Port	– The network protocol required for access. Available options: **All**, **TCP**, **UDP**, **ICMP**, or **GRE** – **Port**: The port or port range that allows the access to the ECS. Range: 1 to 65535 Common ports are listed in .	TCP
Type	IP address type. This parameter is available after IPv6 is enabled. – IPv4 – IPv6	IPv4
Source	The IP address, IP address group, or security group that the rule applies to, which allows access from IP addresses or instances in another security group. Examples: – IPv4 single IP address: 192.168.10.10/32 – Subnet: 192.168.1.0/24 – All IP addresses: 0.0.0.0/0 – sg-abc (security group) For more information about IP address groups, see .	0.0.0.0/0
Description	(Optional) Provides supplementary information about the security group rule. The description can contain up to 255 characters and cannot contain angle brackets (<>).	-

Step 6 Click **OK**.

----End

3.7.4 Binding and Unbinding an EIP

Scenarios

After you create a GeminiDB Redis instance, you can bind an EIP to it to allow external access. If later you want to prohibit external access, you can also unbind the EIP from the DB instance.

Precautions

- To change the EIP that has been bound to a node, unbind it from the node first.
- You need to estimate the bandwidth required by services and purchase an EIP with sufficient bandwidth resources. **Client access exceptions caused by poor public network performance will not be included in the SLA.**

Binding an EIP

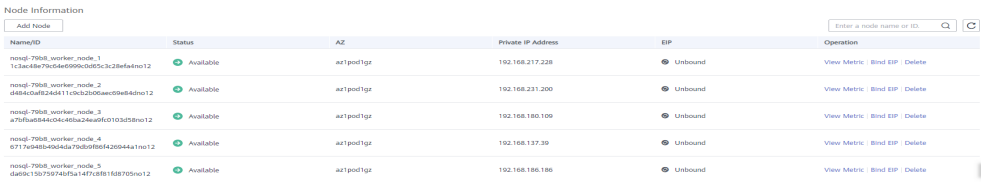
Step 1 **Log in to the management console**.

Step 2 In the service list, choose **Databases** > **GeminiDB**.

Step 3 On the **Instances** page, locate the instance that you want to bind an EIP to and click its name.

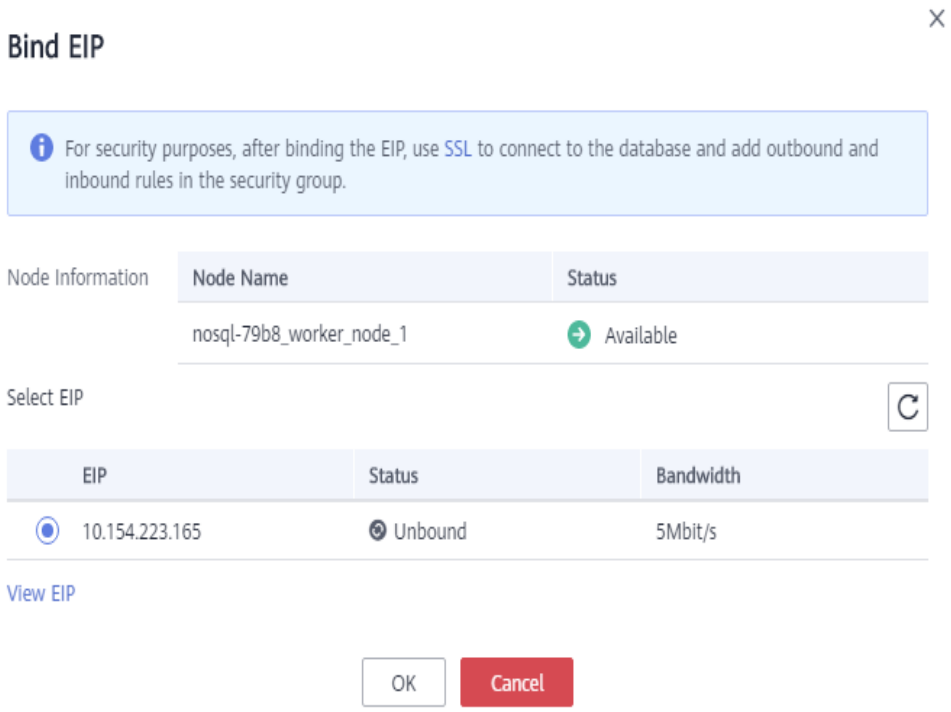
Step 4 In the **Node Information** area, locate the target node and click **Bind EIP** in the **Operation** column.

Figure 3-44 Binding an EIP



Step 5 In the displayed dialog box, view all available EIPs, select the required EIP, and click **OK**. If no available EIPs are displayed, click **View EIP** and create an EIP on the VPC console.

Figure 3-45 Selecting an EIP



Step 6 In the **EIP** column, view the EIP that is successfully bound.

To unbind the EIP from the DB instance, see **Unbinding an EIP**.

----End

Unbinding an EIP

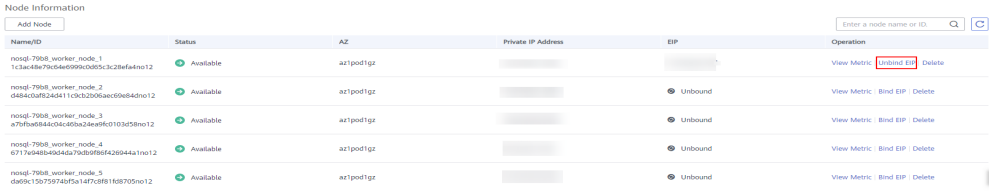
Step 1 **Log in to the management console**.

Step 2 In the service list, choose **Databases** > **GeminiDB**.

Step 3 On the **Instances** page, click the instance that you want to unbind an EIP from.

Step 4 On the **Basic Information** page, in the **Node Information** area, locate the target node and click **Unbind EIP** in the **Operation** column.

Figure 3-46 Unbinding an EIP



Step 5 In the displayed dialog box, click **Yes** to unbind the EIP.

To bind an EIP to the DB instance again, see **Binding an EIP**.

----End

3.7.5 Viewing the IP Address and Port Number

This section describes how to query the IP address and port number of an instance on the management console.

Viewing the Private IP Address or EIP

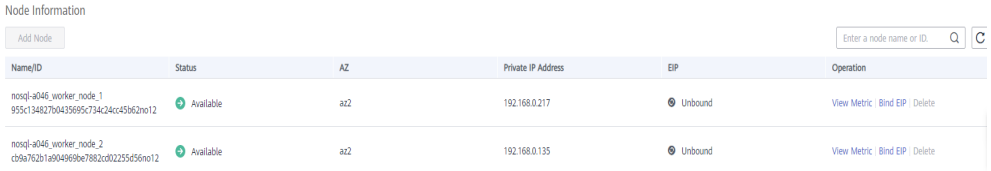
Step 1 Log in to the management console.

Step 2 In the service list, choose **Databases** > **GeminiDB**.

Step 3 On the **Instances** page, locate the instance whose node IP addresses you want to view and click its name.

In the **Node Information** area on the **Basic Information** page, view the private IP address or EIP of each node.

Figure 3-47 Viewing the IP addresses



----End

Viewing the Load Balancer IP Address and Port

Step 1 Log in to the management console.

Step 2 In the service list, choose **Databases** > **GeminiDB**.

Step 3 On the **Instances** page, locate the instance whose load balancer IP address and port you want to view and click its name.

Step 4 In the **Connection Information** area, view the load balancer IP address and corresponding port.

Figure 3-48 Viewing the load balancer IP address and port

----End

Viewing the Port for Accessing Each Instance Node

Step 1 Log in to the management console.

Step 2 In the service list, choose **Databases** > **GeminiDB**.

Step 3 On the **Instances** page, locate the instance whose node access ports you to want view and click its name.

In the **Node Information** area on the **Basic Information** page, view the port of each instance node.

Figure 3-49 Viewing the access port

----End

3.7.6 Configuring an SSL Connection

Secure Socket Layer (SSL) is an encryption-based Internet security protocol for establishing an encrypted link between a server and a client. It provides privacy, authentication, and integrity to Internet communications.

- Authenticates users and servers, ensuring that data is sent to the correct clients and servers.
- Encrypts data to prevent it from being intercepted during transfer.
- Ensures data integrity during transmission.

After SSL is enabled, you can establish an encrypted connection between your client and the instance you want to access to improve data security.

Precautions

- After you enable or disable SSL, the established connection is interrupted. Restart the instance for the change to take effect.
- Enabling SSL will prolong network connection response time and increase CPU usage. So, evaluate impacts on service performance before enabling SSL.
- The SSL function provided by GeminiDB Redis supports only TLS 1.3 or later.

Enabling SSL

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

Step 2 In the service list, choose **Databases** > **GeminiDB**.

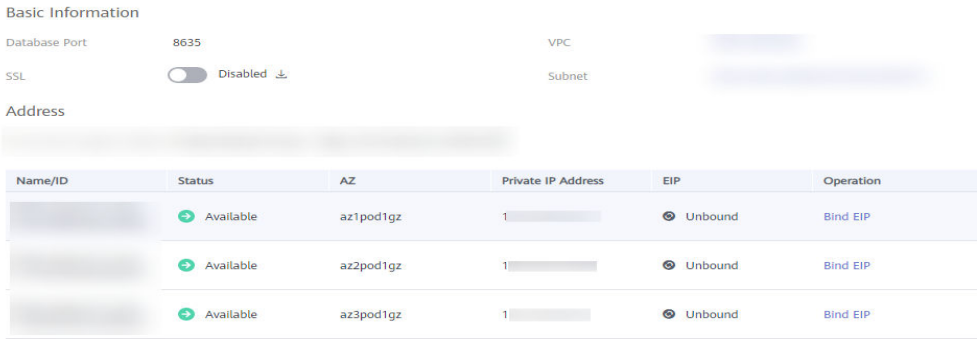
Step 3 On the **Instances** page, locate the instance that you want to enable SSL for.

Step 4 In the **DB Information** area, click  to enable SSL.

Figure 3-50 Enabling SSL

Alternatively, choose **Connections** in the navigation pane on the left. In the **Basic Information** area, click  in the **SSL** field to enable SSL.

Figure 3-51 Enabling SSL



After SSL is enabled, you can connect to the instance through SSL connections. For details, see **SSL (Recommended)**.

----End

Disabling SSL

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

Step 2 In the service list, choose **Databases** > **GeminiDB**.

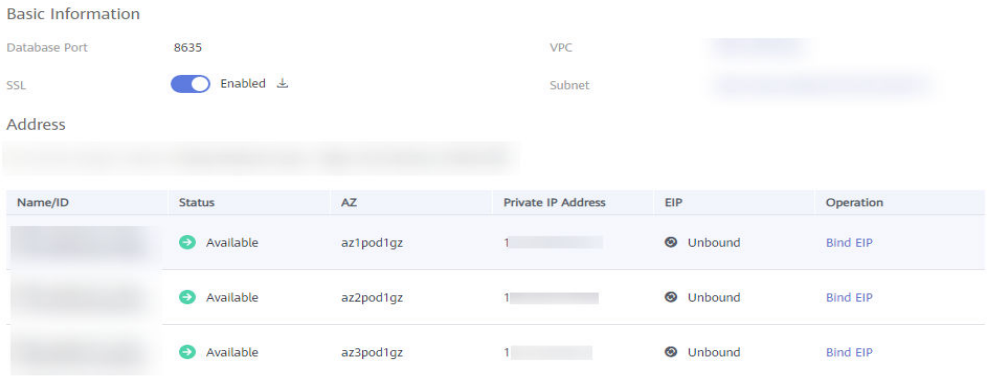
Step 3 On the **Instances** page, locate the instance that you want to disable SSL for.

Step 4 In the **DB Information** area, click  to disable SSL.

Figure 3-52 Disabling SSL

Alternatively, choose **Connections** in the navigation pane on the left. In the **Basic Information** area, click  in the **SSL** field to disable SSL.

Figure 3-53 Disabling SSL



After SSL is disabled, you can connect to the GeminiDB Redis instance through an unencrypted connection. For details, see **Non-SSL Connection**.

----End

3.7.7 Changing a Security Group

Scenarios

You can change security groups of GeminiDB Redis instances.

Precautions

- If you are adding nodes to a DB instance, the security group of the instance cannot be changed.

Procedure

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

Step 2 In the service list, choose **Databases** > **GeminiDB**.

Step 3 On the **Instances** page, locate the instance whose security group you want to change and click its name.

Step 4 In the **Security Group** area, click beside the security group name and select the required security group.

- To submit the change, click . This process takes about 1 to 3 minutes.
- To cancel the change, click .

Step 5 View the modification result.

----End

3.8 Monitoring and Alarm Configuration

3.8.1 GeminiDB Redis Metrics

Description

This section describes GeminiDB Redis metrics reported to Cloud Eye as well as their namespaces and dimensions. You can use APIs provided by Cloud Eye to query the metrics of a monitored object and alarms generated for GeminiDB Redis.

Namespace

SYS.NoSQL

Monitoring Metrics

NOTE

You can view the instance-level and node-level metrics described in **Viewing Monitoring Metrics** on each instance node by referring to **Viewing Monitoring Metrics**. The instance-level metrics displayed on each instance node are the same.

Table 3-8 GeminiDB Redis metrics

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
nosql001_cpu_usage	CPU Usage	CPU usage of the monitored system Unit: Percent	0–100	GeminiDB Redis instance nodes	1 minute
nosql002_mem_usage	Memory Usage	Memory usage of the monitored system Unit: Percent	0–100	GeminiDB Redis instance nodes	1 minute
nosql005_disk_usage	Storage Space Usage	Disk usage of the monitored container Unit: Percent	0–100	GeminiDB Redis instances	1 minute
nosql006_disk_total_size	Total Disk Size	Total disk capacity of the monitored container Unit: GB	≥ 0	GeminiDB Redis instances	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
nosql007_disk_used_size	Used Storage Space	Used disk space of the monitored container Unit: GB	≥ 0	GeminiDB Redis instances	1 minute
redis017_proxy_accept	Total Clients Received by Proxy	Total number of clients received by the proxy Unit: count	≥ 0	GeminiDB Redis instance nodes	1 minute
redis018_proxy_request_ps	Request Acceptance Rate	Rate at which the proxy receives client requests Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis019_proxy_response_ps	Proxy Response Rate	Rate at which the proxy returns requests to the client Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis020_proxy_recv_client_bps	Proxy Byte Stream Acceptance Rate	Rate at which the proxy receives byte streams from the client Unit: byte/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis021_proxy_send_client_bps	Proxy Byte Stream Send Rate	Rate at which the proxy sends byte streams to the client Unit: byte/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis032_shard_qps	Shard QPS	QPS of the shard Unit: count	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis036_exists_avg_usec	Average Proxy Latency of exists Command	Average latency when the proxy executes the exists command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis037_exists_max_usec	Maximum Proxy Latency of exists Command	Maximum latency when the proxy executes the exists command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis038_exists_p99	Proxy P99 Latency of exists Command	P99 latency when the proxy executes the exists command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis039_exists_qps	Proxy exists Command Rate	Rate at which the proxy executes the exists command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis040_expire_avg_usec	Average Proxy Latency of expire Command	Average latency when the proxy executes the expire command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis041_expire_max_usec	Maximum Proxy Latency of expire Command	Maximum latency when the proxy executes the expire command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis042_expire_p99	Proxy P99 Latency of expire Command	P99 latency when the proxy executes the expire command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis043_expire_qps	Proxy expire Command Rate	Rate at which the proxy executes the expire command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis044_del_avg_usec	Average Proxy Latency of del Command	Average latency when the proxy executes the del command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis045_del_max_usec	Maximum Proxy Latency of del Command	Maximum latency when the proxy executes the del command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis046_del_p99	Proxy P99 Latency of del Command	P99 latency when the proxy executes the del command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis047_del_qps	Proxy del Command Rate	Rate at which the proxy executes the del command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis048_ttl_avg_usec	Average Proxy Latency of ttl Command	Average latency when the proxy executes the ttl command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis049_ttl_max_usec	Maximum Proxy Latency of ttl Command	Maximum latency when the proxy executes the ttl command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis050_ttl_p99	Proxy P99 Latency of ttl Command	P99 latency when the proxy executes the ttl command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis051_ttl_qps	Proxy ttl Command Rate	Rate at which the proxy executes the ttl command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis052_persist_avg_usec	Average Proxy Latency of persist Command	Average latency when the proxy executes the persist command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis053_persist_max_usec	Maximum Proxy Latency of persist Command	Maximum latency when the proxy executes the persist command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis054_persist_p99	Proxy P99 Latency of persist Command	P99 latency when the proxy executes the persist command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis055_persist_qps	Proxy persist Command Rate	Rate at which the proxy executes the persist command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis056_scan_avg_usec	Average Proxy Latency of scan Command	Average latency when the proxy executes the scan command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis057_scan_max_usec	Maximum Proxy Latency of scan Command	Maximum latency when the proxy executes the scan command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis058_scan_p99	Proxy P99 Latency of scan Command	P99 latency when the proxy executes the scan command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis059_scan_qps	Proxy scan Command Rate	Rate at which the proxy executes the scan command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis060_set_avg_usec	Average Proxy Latency of set Command	Average latency when the proxy executes the set command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis061_set_max_usec	Maximum Proxy Latency of set Command	Maximum latency when the proxy executes the set command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis062_set_p99	Proxy P99 Latency of set Command	P99 latency when the proxy executes the set command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis063_set_qps	Proxy set Command Rate	Rate at which the proxy executes the set command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis064_get_avg_usec	Average Proxy Latency of get Command	Average latency when the proxy executes the get command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis065_get_max_usec	Maximum Proxy Latency of get Command	Maximum latency when the proxy executes the get command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis066_get_p99	Proxy P99 Latency of get Command	P99 latency when the proxy executes the get command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis067_get_qps	Proxy get Command Rate	Rate at which the proxy executes the get command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis068_getset_avg_usec	Average Proxy Latency of getset Command	Average latency when the proxy executes the getset command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis069_getset_max_usec	Maximum Proxy Latency of getset Command	Maximum latency when the proxy executes the getset command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis070_getset_p99	Proxy P99 Latency of getset Command	P99 latency when the proxy executes the getset command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis071_getset_qps	Proxy getset Command Rate	Rate at which the proxy executes the getset command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis072_append_avg_usec	Average Proxy Latency of append Command	Average latency when the proxy executes the append command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis073_append_max_usec	Maximum Proxy Latency of append Command	Maximum latency when the proxy executes the append command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis074_append_p99	Proxy P99 Latency of append Command	P99 latency when the proxy executes the append command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis075_append_qps	Proxy append Command Rate	Rate at which the proxy executes the append command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis076_mget_avg_usec	Average Proxy Latency of mget Command	Average latency when the proxy executes the mget command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis077_mget_max_usec	Maximum Proxy Latency of mget Command	Maximum latency when the proxy executes the mget command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis078_mget_p99	Proxy P99 Latency of mget Command	P99 latency when the proxy executes the mget command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis079_mget_qps	Proxy mget Command Rate	Rate at which the proxy executes the mget command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis080_mset_avg_usec	Average Proxy Latency of mset Command	Average latency when the proxy executes the mset command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis081_mset_max_usec	Maximum Proxy Latency of mset Command	Maximum latency when the proxy executes the mset command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis082_mset_p99	Proxy P99 Latency of mset Command	P99 latency when the proxy executes the mset command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis083_mset_qps	Proxy mset Command Rate	Rate at which the proxy executes the mset command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis084_getrange_avg_usec	Average Proxy Latency of getrange Command	Average latency when the proxy executes the getrange command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis085_getrange_max_usec	Maximum Proxy Latency of getrange Command	Maximum latency when the proxy executes the getrange command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis086_getrange_p99	Proxy P99 Latency of getrange Command	P99 latency when the proxy executes the getrange command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis087_getrange_qps	Proxy getrange Command Rate	Rate at which the proxy executes the getrange command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis088_setrange_avg_usec	Average Proxy Latency of setrange Command	Average latency when the proxy executes the setrange command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis089_setrange_max_usec	Maximum Proxy Latency of setrange Command	Maximum latency when the proxy executes the setrange command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis090_setrange_p99	Proxy P99 Latency of setrange Command	P99 latency when the proxy executes the setrange command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis091_setrange_qps	Proxy setrange Command Rate	Rate at which the proxy executes the setrange command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis092_substr_avg_usec	Average Proxy Latency of substr Command	Average latency when the proxy executes the substr command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis093_substr_max_usec	Maximum Proxy Latency of substr Command	Maximum latency when the proxy executes the substr command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis094_substr_p99	Proxy P99 Latency of substr Command	P99 latency when the proxy executes the substr command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis095_substr_qps	Proxy substr Command Rate	Rate at which the proxy executes the substr command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis096_strlen_avg_usec	Average Proxy Latency of strlen Command	Average latency when the proxy executes the strlen command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis097_strlen_max_usec	Maximum Proxy Latency of strlen Command	Maximum latency when the proxy executes the strlen command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis098_strlen_p99	Proxy P99 Latency of strlen Command	P99 latency when the proxy executes the strlen command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis099_strlen_qps	Proxy strlen Command Rate	Rate at which the proxy executes the strlen command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis100_incr_avg_usec	Average Proxy Latency of incr Command	Average latency when the proxy executes the incr command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis101_incr_max_usec	Maximum Proxy Latency of incr Command	Maximum latency when the proxy executes the incr command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis102_incr_p99	Proxy P99 Latency of incr Command	P99 latency when the proxy executes the incr command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis103_incr_qps	Proxy incr Command Rate	Rate at which the proxy executes the incr command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis104_decr_avg_usec	Average Proxy Latency of decr Command	Average latency when the proxy executes the decr command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis105_decr_max_usec	Maximum Proxy Latency of decr Command	Maximum latency when the proxy executes the decr command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis106_decr_p99	Proxy P99 Latency of decr Command	P99 latency when the proxy executes the decr command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis107_decr_qps	Proxy decr Command Rate	Rate at which the proxy executes the decr command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis108_hset_avg_usec	Average Proxy Latency of hset Command	Average latency when the proxy executes the hset command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis109_hset_max_usec	Maximum Proxy Latency of hset Command	Maximum latency when the proxy executes the hset command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis110_hset_p99	Proxy P99 Latency of hset Command	P99 latency when the proxy executes the hset command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis111_hset_qps	Proxy hset Command Rate	Rate at which the proxy executes the hset command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis112_hget_avg_usec	Average Proxy Latency of hget Command	Average latency when the proxy executes the hget command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis113_hget_max_usec	Maximum Proxy Latency of hget Command	Maximum latency when the proxy executes the hget command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis114_hget_p99	Proxy P99 Latency of hget Command	P99 latency when the proxy executes the hget command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis115_hget_qps	Proxy hget Command Rate	Rate at which the proxy executes the hget command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis116_hmset_avg_usec	Average Proxy Latency of hmset Command	Average latency when the proxy executes the hmset command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis117_hmset_max_usec	Maximum Proxy Latency of hmset Command	Maximum latency when the proxy executes the hmset command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis118_hmset_p99	Proxy P99 Latency of hmset Command	P99 latency when the proxy executes the hmset command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis119_hmset_qps	Proxy hmset Command Rate	Rate at which the proxy executes the hmset command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis120_hmget_avg_usec	Average Proxy Latency of hmget Command	Average latency when the proxy executes the hmget command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis121_hmget_max_usec	Maximum Proxy Latency of hmget Command	Maximum latency when the proxy executes the hmget command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis122_hmget_p99	Proxy P99 Latency of hmget Command	P99 latency when the proxy executes the hmget command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis123_hmget_qps	Proxy hmget Command Rate	Rate at which the proxy executes the hmget command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis124_hdel_avg_usec	Average Proxy Latency of hdel Command	Average latency when the proxy executes the hdel command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis125_hdel_max_usec	Maximum Proxy Latency of hdel Command	Maximum latency when the proxy executes the hdel command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis126_hdel_p99	Proxy P99 Latency of hdel Command	P99 latency when the proxy executes the hdel command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis127_hdel_qps	Proxy hdel Command Rate	Rate at which the proxy executes the hdel command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis128_hgetall_avg_usec	Average Proxy Latency of hgetall Command	Average latency when the proxy executes the hgetall command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis129_hgetall_max_usec	Maximum Proxy Latency of hgetall Command	Maximum latency when the proxy executes the hgetall command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis130_hgetall_p99	Proxy P99 Latency of hgetall Command	P99 latency when the proxy executes the hgetall command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis131_hgetall_qps	Proxy hgetall Command Rate	Rate at which the proxy executes the hgetall command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis132_hexists_avg_usec	Average Proxy Latency of hexists Command	Average latency when the proxy executes the hexists command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis133_hexists_max_usec	Maximum Proxy Latency of hexists Command	Maximum latency when the proxy executes the hexists command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis134_hexists_p99	Proxy P99 Latency of hexists Command	P99 latency when the proxy executes the hexists command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis135_hexists_qps	Proxy hexists Command Rate	Rate at which the proxy executes the hexists command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis136_hincrby_avg_usec	Average Proxy Latency of hincrby Command	Average latency when the proxy executes the hincrby command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis137_hincrby_max_usec	Maximum Proxy Latency of hincrby Command	Maximum latency when the proxy executes the hincrby command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis138_hincrby_p99	Proxy P99 Latency of hincrby Command	P99 latency when the proxy executes the hincrby command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis139_hincrby_qps	Proxy hincrby Command Rate	Rate at which the proxy executes the hincrby command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis140_hkeys_avg_usec	Average Proxy Latency of hkeys Command	Average latency when the proxy executes the hkeys command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis141_hkeys_max_usec	Maximum Proxy Latency of hkeys Command	Maximum latency when the proxy executes the hkeys command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis142_hkeys_p99	Proxy P99 Latency of hkeys Command	P99 latency when the proxy executes the hkeys command Unit: µs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis143_hkeys_qps	Proxy hkeys Command Rate	Rate at which the proxy executes the hkeys command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis144_hlen_avg_usec	Average Proxy Latency of hlen Command	Average latency when the proxy executes the hlen command Unit: µs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis145_hlen_max_usec	Maximum Proxy Latency of hlen Command	Maximum latency when the proxy executes the hlen command Unit: µs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis146_hlen_p99	Proxy P99 Latency of hlen Command	P99 latency when the proxy executes the hlen command Unit: µs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis147_hlen_qps	Proxy hlen Command Rate	Rate at which the proxy executes the hlen command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis148_hstrlen_avg_usec	Average Proxy Latency of hstrlen Command	Average latency when the proxy executes the hstrlen command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis149_hstrlen_max_usec	Maximum Proxy Latency of hstrlen Command	Maximum latency when the proxy executes the hstrlen command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis150_hstrlen_p99	Proxy P99 Latency of hstrlen Command	P99 latency when the proxy executes the hstrlen command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis151_hstrlen_qps	Proxy hstrlen Command Rate	Rate at which the proxy executes the hstrlen command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis152_hvals_avg_usec	Average Proxy Latency of hvals Command	Average latency when the proxy executes the hvals command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis153_hvals_max_usec	Maximum Proxy Latency of hvals Command	Maximum latency when the proxy executes the hvals command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis154_hvals_p99	Proxy P99 Latency of hvals Command	P99 latency when the proxy executes the hvals command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis155_hvals_qps	Proxy hvals Command Rate	Rate at which the proxy executes the hvals command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis156_hscan_avg_usec	Average Proxy Latency of hscan Command	Average latency when the proxy executes the hscan command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis157_hscan_max_usec	Maximum Proxy Latency of hscan Command	Maximum latency when the proxy executes the hscan command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis158_hscan_p99	Proxy P99 Latency of hscan Command	P99 latency when the proxy executes the hscan command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis159_hscan_qps	Proxy hscan Command Rate	Rate at which the proxy executes the hscan command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis160_lpush_avg_usec	Average Proxy Latency of lpush Command	Average latency when the proxy executes the lpush command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis161_lpush_max_usec	Maximum Proxy Latency of lpush Command	Maximum latency when the proxy executes the lpush command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis162_lpush_p99	Proxy P99 Latency of lpush Command	P99 latency when the proxy executes the lpush command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis163_lpush_qps	Proxy lpush Command Rate	Rate at which the proxy executes the lpush command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis164_lpop_avg_usec	Average Proxy Latency of lpop Command	Average latency when the proxy executes the lpop command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis165_lpop_max_usec	Maximum Proxy Latency of lpop Command	Maximum latency when the proxy executes the lpop command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis166_lpop_p99	Proxy P99 Latency of lpop Command	P99 latency when the proxy executes the lpop command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis167_lpop_qps	Proxy lpop Command Rate	Rate at which the proxy executes the lpop command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis168_rpush_avg_usec	Average Proxy Latency of rpush Command	Average latency when the proxy executes the rpush command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis169_rpush_max_usec	Maximum Proxy Latency of rpush Command	Maximum latency when the proxy executes the rpush command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis170_rpush_p99	Proxy P99 Latency of rpush Command	P99 latency when the proxy executes the rpush command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis171_rpush_qps	Proxy rpush Command Rate	Rate at which the proxy executes the rpush command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis172_rpop_avg_usec	Average Proxy Latency of rpop Command	Average latency when the proxy executes the rpop command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis173_rpop_max_usec	Maximum Proxy Latency of rpop Command	Maximum latency when the proxy executes the rpop command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis174_rpop_p99	Proxy P99 Latency of rpop Command	P99 latency when the proxy executes the rpop command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis175_rpop_qps	Proxy rpop Command Rate	Rate at which the proxy executes the rpop command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis176_rpoplpush_avg_usec	Average Proxy Latency of rpoplpush Command	Average latency when the proxy executes the rpoplpush command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis177_rpoplpush_max_usec	Maximum Proxy Latency of rpoplpush Command	Maximum latency when the proxy executes the rpoplpush command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis178_rpoplpush_p99	Proxy P99 Latency of rpoplpush Command	P99 latency when the proxy executes the rpoplpush command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis179_rpoplpush_qps	Proxy rpoplpush Command Rate	Rate at which the proxy executes the rpoplpush command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis180_llen_avg_usec	Average Proxy Latency of llen Command	Average latency when the proxy executes the llen command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis181_llen_max_usec	Maximum Proxy Latency of llen Command	Maximum latency when the proxy executes the llen command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis182_llen_p99	Proxy P99 Latency of llen Command	P99 latency when the proxy executes the llen command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis183_llen_qps	Proxy llen Command Rate	Rate at which the proxy executes the llen command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis184_lindex_avg_usec	Average Proxy Latency of lindex Command	Average latency when the proxy executes the lindex command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis185_lindex_max_usec	Maximum Proxy Latency of lindex Command	Maximum latency when the proxy executes the lindex command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis186_lindex_p99	Proxy P99 Latency of lindex Command	P99 latency when the proxy executes the lindex command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis187_lindex_qps	Proxy lindex Command Rate	Rate at which the proxy executes the lindex command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis188_linsert_avg_usec	Average Proxy Latency of linsert Command	Average latency when the proxy executes the linsert command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis189_linsert_max_usec	Maximum Proxy Latency of linsert Command	Maximum latency when the proxy executes the linsert command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis190_linsert_p99	Proxy P99 Latency of linsert Command	P99 latency when the proxy executes the linsert command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis191_linsert_qps	Proxy linsert Command Rate	Rate at which the proxy executes the linsert command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis192_lrange_avg_usec	Average Proxy Latency of lrange Command	Average latency when the proxy executes the lrange command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis193_lrange_max_usec	Maximum Proxy Latency of lrange Command	Maximum latency when the proxy executes the lrange command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis194_lrange_p99	Proxy P99 Latency of lrange Command	P99 latency when the proxy executes the lrange command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis195_lrange_qps	Proxy lrange Command Rate	Rate at which the proxy executes the lrange command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis196_lrem_avg_usec	Average Proxy Latency of lrem Command	Average latency when the proxy executes the lrem command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis197_lrem_max_usec	Maximum Proxy Latency of lrem Command	Maximum latency when the proxy executes the lrem command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis198_lrem_p99	Proxy P99 Latency of lrem Command	P99 latency when the proxy executes the lrem command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis199_lrem_qps	Proxy lrem Command Rate	Rate at which the proxy executes the lrem command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis200_lset_avg_usec	Average Proxy Latency of lset Command	Average latency when the proxy executes the lset command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis201_lset_max_usec	Maximum Proxy Latency of lset Command	Maximum latency when the proxy executes the lset command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis202_lset_p99	Proxy P99 Latency of lset Command	P99 latency when the proxy executes the lset command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis203_lset_qps	Proxy lset Command Rate	Rate at which the proxy executes the lset command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis204_ltrim_avg_usec	Average Proxy Latency of ltrim Command	Average latency when the proxy executes the ltrim command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis205_ltrim_max_usec	Maximum Proxy Latency of ltrim Command	Maximum latency when the proxy executes the ltrim command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis206_ltrim_p99	Proxy P99 Latency of ltrim Command	P99 latency when the proxy executes the ltrim command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis207_ltrim_qps	Proxy ltrim Command Rate	Rate at which the proxy executes the ltrim command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis208_sadd_avg_usec	Average Proxy Latency of sadd Command	Average latency when the proxy executes the sadd command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis209_sadd_max_usec	Maximum Proxy Latency of sadd Command	Maximum latency when the proxy executes the sadd command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis210_sadd_p99	Proxy P99 Latency of sadd Command	P99 latency when the proxy executes the sadd command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis211_sadd_qps	Proxy sadd Command Rate	Rate at which the proxy executes the sadd command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis212_spop_avg_usec	Average Proxy Latency of spop Command	Average latency when the proxy executes the spop command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis213_spop_max_usec	Maximum Proxy Latency of spop Command	Maximum latency when the proxy executes the spop command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis214_spop_p99	Proxy P99 Latency of spop Command	P99 latency when the proxy executes the spop command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis215_spop_qps	Proxy spop Command Rate	Rate at which the proxy executes the spop command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis216_scard_avg_usec	Average Proxy Latency of scard Command	Average latency when the proxy executes the scard command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis217_scard_max_usec	Maximum Proxy Latency of scard Command	Maximum latency when the proxy executes the scard command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis218_scard_p99	Proxy P99 Latency of scard Command	P99 latency when the proxy executes the scard command Unit: µs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis219_scard_qps	Proxy scard Command Rate	Rate at which the proxy executes the scard command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis220_smembers_avg_usec	Average Proxy Latency of smembers Command	Average latency when the proxy executes the smembers command Unit: µs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis221_smembers_max_usec	Maximum Proxy Latency of smembers Command	Maximum latency when the proxy executes the smembers command Unit: µs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis222_smembers_p99	Proxy P99 Latency of smembers Command	P99 latency when the proxy executes the smembers command Unit: µs	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis223_smembers_qps	Proxy smembers Command Rate	Rate at which the proxy executes the smembers command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis224_srem_avg_usec	Average Proxy Latency of srem Command	Average latency when the proxy executes the srem command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis225_srem_max_usec	Maximum Proxy Latency of srem Command	Maximum latency when the proxy executes the srem command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis226_srem_p99	Proxy P99 Latency of srem Command	P99 latency when the proxy executes the srem command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis227_srem_qps	Proxy srem Command Rate	Rate at which the proxy executes the srem command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis228_sunion_avg_usec	Average Proxy Latency of sunion Command	Average latency when the proxy executes the sunion command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis229_sunion_max_usec	Maximum Proxy Latency of sunion Command	Maximum latency when the proxy executes the sunion command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis230_sunion_p99	Proxy P99 Latency of sunion Command	P99 latency when the proxy executes the sunion command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis231_sunion_qps	Proxy sunion Command Rate	Rate at which the proxy executes the sunion command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis232_sinter_avg_usec	Average Proxy Latency of sinter Command	Average latency when the proxy executes the sinter command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis233_sinter_max_usec	Maximum Proxy Latency of sinter Command	Maximum latency when the proxy executes the sinter command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis234_sinter_p99	Proxy P99 Latency of sinter Command	P99 latency when the proxy executes the sinter command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis235_sinter_qps	Proxy sinter Command Rate	Rate at which the proxy executes the sinter command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis236_sismember_avg_usec	Average Proxy Latency of sismember Command	Average latency when the proxy executes the sismember command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis237_sismember_max_usec	Maximum Proxy Latency of sismember Command	Maximum latency when the proxy executes the sismember command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis238_sismember_p99	Proxy P99 Latency of sismember Command	P99 latency when the proxy executes the sismember command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis239_sismember_qps	Proxy sismember Command Rate	Rate at which the proxy executes the sismember command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis240_sdiff_avg_usec	Average Proxy Latency of sdiff Command	Average latency when the proxy executes the sdiff command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis241_sdiff_max_usec	Maximum Proxy Latency of sdiff Command	Maximum latency when the proxy executes the sdiff command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis242_sdiff_p99	Proxy P99 Latency of sdiff Command	P99 latency when the proxy executes the sdiff command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis243_sdiff_qps	Proxy sdiff Command Rate	Rate at which the proxy executes the sdiff command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis244_srandmember_avg_usec	Average Proxy Latency of srandmember Command	Average latency when the proxy executes the srandmember command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis245_srandmember_max_usec	Maximum Proxy Latency of srandmember Command	Maximum latency when the proxy executes the srandmember command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis246_srandmember_p99	Proxy P99 Latency of srandmember Command	P99 latency when the proxy executes the srandmember command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis247_srandmember_qps	Proxy srandmember Command Rate	Rate at which the proxy executes the srandmember command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis248_zadd_avg_usec	Average Proxy Latency of zadd Command	Average latency when the proxy executes the zadd command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis249_zadd_max_usec	Maximum Proxy Latency of zadd Command	Maximum latency when the proxy executes the zadd command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis250_zadd_p99	Proxy P99 Latency of zadd Command	P99 latency when the proxy executes the zadd command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis251_zadd_qps	Proxy zadd Command Rate	Rate at which the proxy executes the zadd command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis252_zcard_avg_usec	Average Proxy Latency of zcard Command	Average latency when the proxy executes the zcard command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis253_zcard_max_usec	Maximum Proxy Latency of zcard Command	Maximum latency when the proxy executes the zcard command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis254_zcard_p99	Proxy P99 Latency of zcard Command	P99 latency when the proxy executes the zcard command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis255_zcard_qps	Proxy zcard Command Rate	Rate at which the proxy executes the zcard command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis256_zscan_avg_usec	Average Proxy Latency of zscan Command	Average latency when the proxy executes the zscan command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis257_zscan_max_usec	Maximum Proxy Latency of zscan Command	Maximum latency when the proxy executes the zscan command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis258_zscan_p99	Proxy P99 Latency of zscan Command	P99 latency when the proxy executes the zscan command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis259_zscan_qps	Proxy zscan Command Rate	Rate at which the proxy executes the zscan command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis260_zincrby_avg_usec	Average Proxy Latency of zincrby Command	Average latency when the proxy executes the zincrby command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis261_zincrby_max_usec	Maximum Proxy Latency of zincrby Command	Maximum latency when the proxy executes the zincrby command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis262_zincrby_p99	Proxy P99 Latency of zincrby Command	P99 latency when the proxy executes the zincrby command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis263_zincrby_qps	Proxy zincrby Command Rate	Rate at which the proxy executes the zincrby command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis264_zrevrange_avg_usec	Average Proxy Latency of zrevrange Command	Average latency when the proxy executes the zrevrange command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis265_zrevrange_max_usec	Maximum Proxy Latency of zrevrange Command	Maximum latency when the proxy executes the zrevrange command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis266_zrevrange_p99	Proxy P99 Latency of zrevrange Command	P99 latency when the proxy executes the zrevrange command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis267_zrevrange_qps	Proxy zrevrange Command Rate	Rate at which the proxy executes the zrevrange command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis268_zrange_avg_usec	Average Proxy Latency of zrange Command	Average latency when the proxy executes the zrange command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis269_zrange_max_usec	Maximum Proxy Latency of zrange Command	Maximum latency when the proxy executes the zrange command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis270_zrange_p99	Proxy P99 Latency of zrange Command	P99 latency when the proxy executes the zrange command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis271_zrange_qps	Proxy zrange Command Rate	Rate at which the proxy executes the zrange command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis272_zcount_avg_usec	Average Proxy Latency of zcount Command	Average latency when the proxy executes the zcount command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis273_zcount_max_usec	Maximum Proxy Latency of zcount Command	Maximum latency when the proxy executes the zcount command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis274_zcount_p99	Proxy P99 Latency of zcount Command	P99 latency when the proxy executes the zcount command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis275_zcount_qps	Proxy zcount Command Rate	Rate at which the proxy executes the zcount command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis276_zrem_avg_usec	Average Proxy Latency of zrem Command	Average latency when the proxy executes the zrem command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis277_zrem_max_usec	Maximum Proxy Latency of zrem Command	Maximum latency when the proxy executes the zrem command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis278_zrem_p99	Proxy P99 Latency of zrem Command	P99 latency when the proxy executes the zrem command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis279_zrem_qps	Proxy zrem Command Rate	Rate at which the proxy executes the zrem command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis280_zscore_avg_usec	Average Proxy Latency of zscore Command	Average latency when the proxy executes the zscore command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis281_zscore_max_usec	Maximum Proxy Latency of zscore Command	Maximum latency when the proxy executes the zscore command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis282_zscore_p99	Proxy P99 Latency of zscore Command	P99 latency when the proxy executes the zscore command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis283_zscore_qps	Proxy zscore Command Rate	Rate at which the proxy executes the zscore command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis284_zrank_avg_usec	Average Proxy Latency of zrank Command	Average latency when the proxy executes the zrank command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis285_zrank_max_usec	Maximum Proxy Latency of zrank Command	Maximum latency when the proxy executes the zrank command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis286_zrank_p99	Proxy P99 Latency of zrank Command	P99 latency when the proxy executes the zrank command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis287_zrank_qps	Proxy zrank Command Rate	Rate at which the proxy executes the zrank command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis288_zrevrank_avg_usec	Average Proxy Latency of zrevrank Command	Average latency when the proxy executes the zrevrank command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis289_zrevrank_max_usec	Maximum Proxy Latency of zrevrank Command	Maximum latency when the proxy executes the zrevrank command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis290_zrevrank_p99	Proxy P99 Latency of zrevrank Command	P99 latency when the proxy executes the zrevrank command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis291_zrevrank_qps	Proxy zrevrank Command Rate	Rate at which the proxy executes the zrevrank command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis292_zlexcount_avg_usec	Average Proxy Latency of zlexcount Command	Average latency when the proxy executes the zlexcount command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis293_zlexcount_max_usec	Maximum Proxy Latency of zlexcount Command	Maximum latency when the proxy executes the zlexcount command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis294_zlexcount_p99	Proxy P99 Latency of zlexcount Command	P99 latency when the proxy executes the zlexcount command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis295_zlexcount_qps	Proxy zlexcount Command Rate	Rate at which the proxy executes the zlexcount command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis296_zpopmax_avg_usec	Average Proxy Latency of zpopmax Command	Average latency when the proxy executes the zpopmax command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis297_zpopmax_max_usec	Maximum Proxy Latency of zpopmax Command	Maximum latency when the proxy executes the zpopmax command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis298_zpopmax_p99	Proxy P99 Latency of zpopmax Command	P99 latency when the proxy executes the zpopmax command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis299_zpopmax_qps	Proxy zpopmax Command Rate	Rate at which the proxy executes the zpopmax command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis300_zpopmin_avg_usec	Average Proxy Latency of zpopmin Command	Average latency when the proxy executes the zpopmin command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis301_zpopmin_max_usec	Maximum Proxy Latency of zpopmin Command	Maximum latency when the proxy executes the zpopmin command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis302_zpopmin_p99	Proxy P99 Latency of zpopmin Command	P99 latency when the proxy executes the zpopmin command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis303_zpopmin_qps	Proxy zpopmin Command Rate	Rate at which the proxy executes the zpopmin command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis304_zremrangebyrank_avg_usec	Average Proxy Latency of zremrangebyrank Command	Average latency when the proxy executes the zremrangebyrank command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis305_zremrangebyrank_max_usec	Maximum Proxy Latency of zremrangebyrank Command	Maximum latency when the proxy executes the zremrangebyrank command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis306_zremrangebyrank_p99	Proxy P99 Latency of zremrangebyrank Command	P99 latency when the proxy executes the zremrangebyrank command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis307_zremrangebyrank_qps	Proxy zremrangebyrank Command Rate	Rate at which the proxy executes the zremrangebyrank command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis308_zremrangebyscore_avg_usec	Average Proxy Latency of zremrangebyscore Command	Average latency when the proxy executes the zremrangebyscore command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis309_zremrangebyscore_max_usec	Maximum Proxy Latency of zremrangebyscore Command	Maximum latency when the proxy executes the zremrangebyscore command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis310_zremrangebyscore_p99	Proxy P99 Latency of zremrangebyscore Command	P99 latency when the proxy executes the zremrangebyscore command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis311_zremrangebyscore_qps	Proxy zremrangebyscore Command Rate	Rate at which the proxy executes the zremrangebyscore command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis312_zremrangebylex_avg_usec	Average Proxy Latency of zremrangebylex Command	Average latency when the proxy executes the zremrangebylex command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis313_zremrangebylex_max_usec	Maximum Proxy Latency of zremrangebylex Command	Maximum latency when the proxy executes the zremrangebylex command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis314_zremrangebylex_p99	Proxy P99 Latency of zremrangebylex Command	P99 latency when the proxy executes the zremrangebylex command Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis315_zremrangebylex_qps	Proxy zremrangebylex Command Rate	Rate at which the proxy executes the zremrangebylex command Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis316_all_avg_usec	Average Proxy Latency of Commands	Average latency when the proxy executes commands Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis317_all_max_usec	Maximum Proxy Latency of Commands	Maximum latency when the proxy executes commands Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis318_all_p99	Proxy P99 Latency of Commands	P99 latency when the proxy executes all commands Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis319_all_qps	Proxy Command Rate	Rate at which the proxy executes commands Unit: count/s	≥ 0	GeminiDB Redis instance nodes	1 minute
redis661_rsync_ops	rsync Rate	Rate that rsync transfers data in a collection period Unit: count	≥ 0	GeminiDB Redis instance nodes	1 minute
redis662_rsync_wal_size	Size of WAL Files to Be Synchronized	Size of WAL files to be synchronized by rsync in a collection period Unit: byte	≥ 0	GeminiDB Redis instance nodes	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
redis663_rsync_push_cost	Average Push Time	Average time required for rsync to push data in a collection period Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis664_rsync_send_cost	Average Send Time	Average time required for rsync to send data in a collection period Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis665_rsync_max_push_cost	Maximum Push Time	Maximum time required for a push operation in a collection period Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute
redis666_rsync_max_send_cost	Maximum Send Time	Maximum time required for a send operation in a collection period Unit: μs	≥ 0	GeminiDB Redis instance nodes	1 minute

Dimensions

Key	Value
redis_cluster_id	Cluster ID of the GeminiDB Redis instance
redis_node_id	Node ID of the GeminiDB Redis instance

3.8.2 Configuring Alarm Rules

Scenarios

Setting alarm rules allows you to customize objects to be monitored and notification policies so that you can closely monitor your instances.

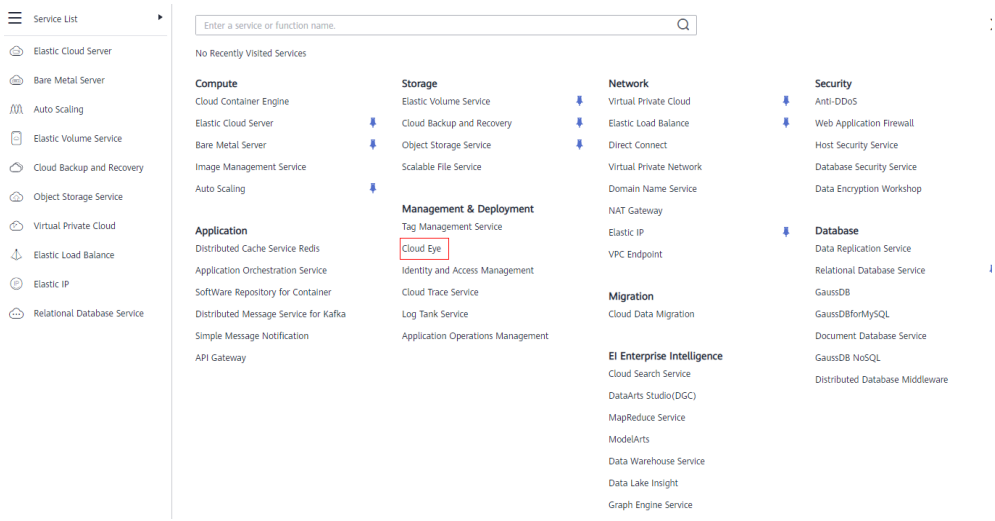
Alarm rules include the alarm rule name, instance, metric, threshold, monitoring interval, and whether to send notifications. This section describes how to set alarm rules.

Procedure

Step 1 Log in to the management console.

Step 2 Click **Service List**. Under **Management & Deployment**, click **Cloud Eye**.

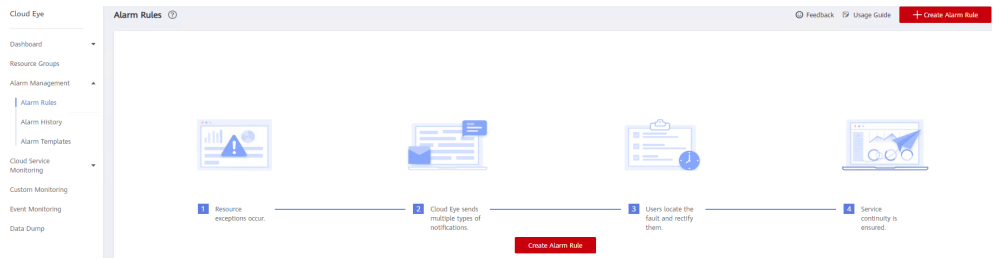
Figure 3-54 Selecting Cloud Eye



Step 3 In the navigation pane on the left, choose **Alarm Management** > **Alarm Rules**.

Step 4 On the **Alarm Rules** page, click **Create Alarm Rule**.

Figure 3-55 Creating an alarm rule



Step 5 Set alarm parameters.

1. Configure basic alarm information.

Figure 3-56 Configuring basic information for an alarm rule

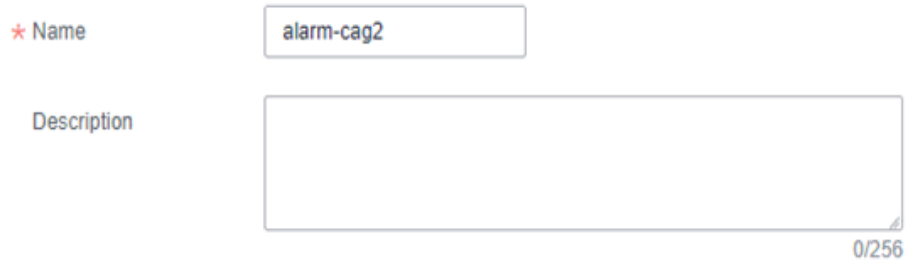


Table 3-9 Basic alarm rule information

Parameter	Description	Example Value
Name	Name of the rule. The system generates a random name and you can modify it.	alarm-cag2
Description	(Optional) Alarm rule description.	-

2. Select objects to be monitored and specify the monitoring scope.

Table 3-10 Parameter description

Parameter	Description	Example Value
Alarm Type	Alarm type that the alarm rule is created for. The value can be **Metric** or **Event**.	Metric
Resource Type	Type of the resource the alarm rule is created for. Select **GeminiDB**.	-
Dimension	Metric dimension of the alarm rule. Select **Redis-Redis Nodes**.	-
Monitoring Scope	Monitoring scope the alarm rule applies to. **NOTE** – If you select **Resource groups** and any resource in the group meets the alarm policy, an alarm notification will be sent. – After you select **Specific resources**, select one or more resources and click » to add them to the box on the right.	All resources
Group	This parameter is mandatory when **Monitoring Scope** is set to **Resource groups**.	-

3. Configure an alarm policy.

Figure 3-57 Configuring the alarm policy

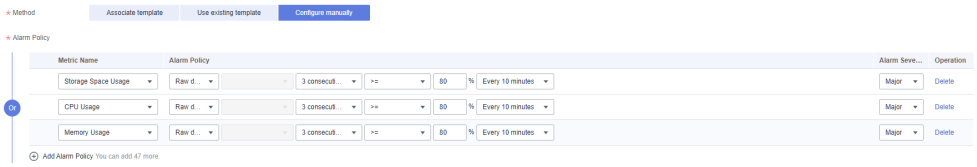


Table 3-11 Parameter description

Parameter	Description	Example Value
Method	Select **Associate template**, **Use existing template**, or **Configure manually**. **NOTE** If you set **Monitoring Scope** to **Specific resources**, you can set **Method** to **Use existing template**.	Configure manually
Template	Select the template to be used. This parameter is available only when you select **Use existing template** for **Method**.	-

Parameter	Description	Example Value
Alarm Policy	Policy for triggering an alarm. You can configure the threshold, consecutive periods, alarm interval, and alarm severity based on service requirements. – **Metric Name**: specifies the the metric that the alarm rule is created for. The following metrics are recommended: **Storage Space Usage**, which is used to monitor the storage usage of GeminiDB Redis instances. If the storage usage is greater than 80%, scale up the storage in a timely manner by referring to **Scaling Up Storage Space**. **CPU Usage** and **Memory Usage**, which are used to monitor the compute resource usage of each GeminiDB Redis instance node. If the CPU usage or memory usage is greater than 80%, you can **add nodes** or **upgrade node specifications** in a timely manner. For more metrics, see **GeminiDB Redis Metrics**. – **Alarm Severity**: specifies the severity of the alarm. Valid values are **Critical**, **Major**, **Minor**, and **Informational**. **NOTE** A maximum of 50 alarm policies can be added to an alarm rule. If any one of these alarm policies is met, an alarm is triggered.	Take the CPU usage as an example. The alarm policy configured in **Figure 3-57** indicates that a major alarm notification will be sent to users every 10 minutes if the original CPU usage reaches 80% or above for three consecutive periods.

4. Configure alarm notification information.

Figure 3-58 Configuring alarm notification information

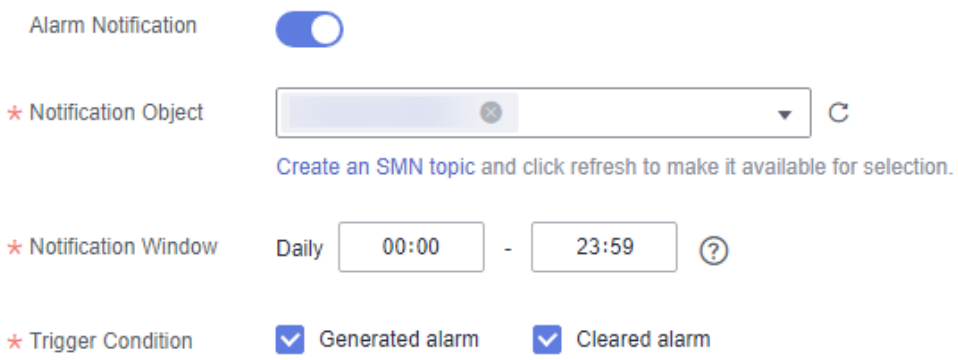


Table 3-12 Parameter description

Parameter	Description	Example Value
Alarm Notification	Whether to notify users when alarms are triggered. Notifications can be sent by email, text message, or HTTP/HTTPS message. Enabling alarm notification is recommended. When the metric data reaches the threshold set in the alarm rule, Cloud Eye immediately notifies you through SMN that an exception has occurred.	Enabled **Alarm Notification**.
Notification Object	Object that receives alarm notifications. You can select the account contact or a topic. – **Account contact** is the mobile phone number and email address of the registered account. – **Topic** is used to publish messages and subscribe to notifications. If the required topic is unavailable, create one first and add subscriptions to it.	-
Notification Window	Cloud Eye sends notifications only within the notification window specified in the alarm rule. For example, if **Notification Window** is set to **00:00-8:00**, Cloud Eye sends notifications only within 00:00-08:00.	-
Trigger Condition	Condition for triggering an alarm notification. You can select **Generated alarm** (when an alarm is generated), **Cleared alarm** (when an alarm is cleared), or both.	-

5. Configure advanced settings.

Figure 3-59 Advanced settings

Table 3-13 Parameter description

Parameter	Description	Example Value
Enterprise Project	Enterprise project that the alarm rule belongs to. Only users with the enterprise project permissions can view and manage the alarm rule.	default

Step 6 After the configuration is complete, click **Create**.

When the metric data reaches the threshold set in the alarm rule, Cloud Eye immediately notifies you through SMN that an exception has occurred.

----End

3.8.3 Viewing Monitoring Metrics

Scenarios

Cloud Eye monitors GeminiDB Redis instance running statuses. You can view the GeminiDB Redis monitoring metrics on the management console.

Monitored data requires a period of time for transmission and display. The status of the monitored object displayed on the Cloud Eye page is the status obtained 5 to 10 minutes before. You can view the monitored data of a newly created DB instance 5 to 10 minutes later.

Prerequisites

- The DB instance is running properly.

  Cloud Eye does not display the metrics of a faulty or deleted DB instance. You can view the monitoring information only after the instance is restarted or recovered.
- The DB instance has been properly running for at least 10 minutes.

  The monitoring data and graphics are available for a new DB instance after the instance runs for at least 10 minutes.

Method 1

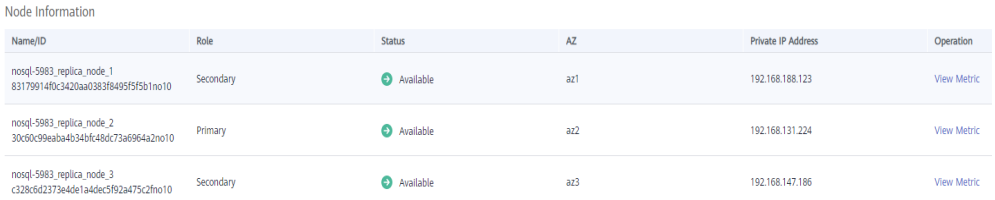
Step 1 **Log in to the management console**.

Step 2 In the service list, choose **Databases** > **GeminiDB**.

Step 3 On the **Instances** page, click the instance whose metrics you want to view and click its name.

Step 4 In the **Node Information** area on the **Basic Information** page, click **View Metric** in the **Operation** column.

Figure 3-60 Viewing metrics



Step 5 In the monitoring area, you can select a duration to view the monitoring data.

You can view the monitoring data of the service in the last 1, 3, or 12 hours.

To view the monitoring curve in a longer time range, click to enlarge the graph.

----End

Method 2

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

Step 2 In the service list, choose **Databases** > **GeminiDB**.

Step 3 On the **Instance** page, click the instance whose metrics you want to view and click its name.

Step 4 In the navigation pane on the left, choose **Advanced O&M**.

Step 5 On the displayed page, click the **Real-Time Monitoring** tab to view real-time monitoring data such as CPU usage, memory usage, and storage space usage.

On the **Real-Time Monitoring** tab, you can also click **View details** to view more metric details.

NOTE

This function is in the open beta test (OBT) phase. To use this function, contact customer service.

----End

3.8.4 Configuring a Dashboard

Dashboards, serving as custom monitoring platforms, allow you to view metrics.

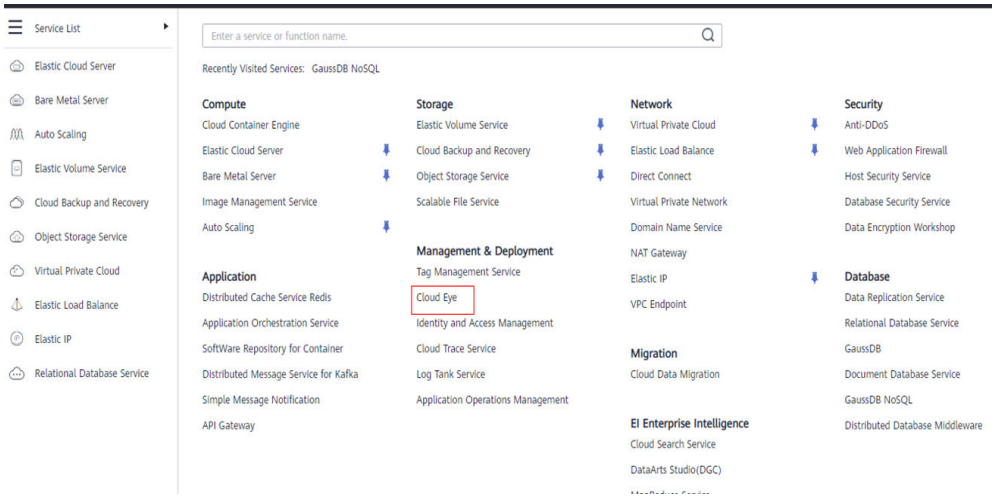
This section describes how to configure a dashboard for GeminiDB Redis.

Procedure

Step 1 Log in to the management console.

Step 2 In the service list, click **Cloud Eye** to go to the Cloud Eye console.

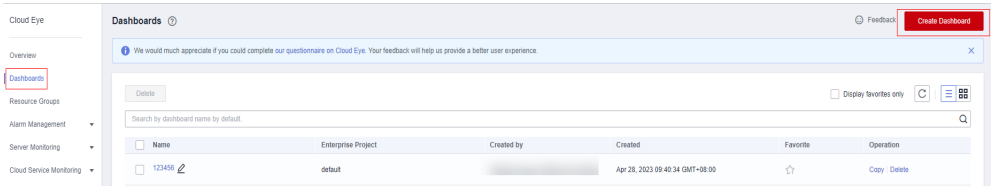
Figure 3-61 Logging in to the Cloud Eye console



Step 3 Create a monitoring dashboard.

1. In the navigation pane on the left, choose **Dashboards**. On the displayed page, click **Create Dashboard**.

Figure 3-62 Creating a dashboard



2. In the displayed **Create Dashboard** dialog box, set required parameters.

Figure 3-63 Configuring parameters

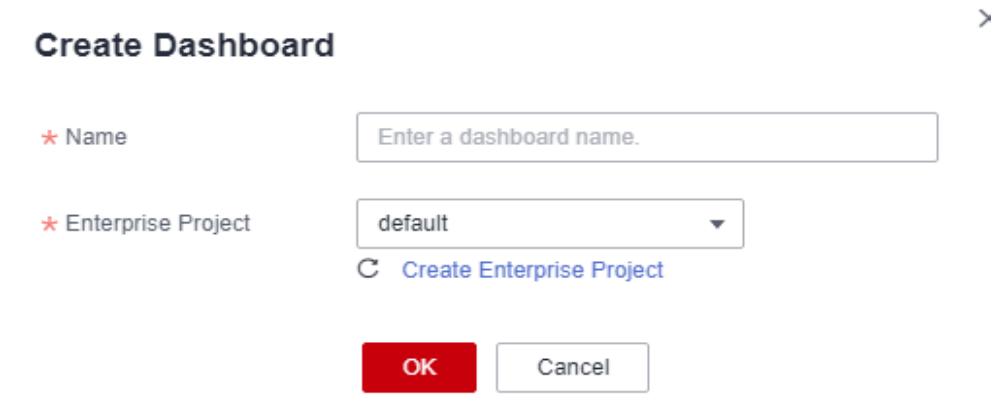


Table 3-14 Parameter description

Parameter	Description
Name	Dashboard name. The name can include a maximum of 128 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed.
Enterprise Project	If you associate a monitoring dashboard with an enterprise project, only users who have the permissions of the enterprise project can manage the monitoring dashboard. **NOTE** The enterprise project feature is available only in some regions.

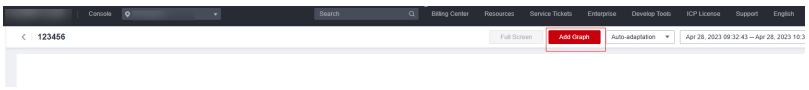
3. Click **OK**.

Step 4 Add a graph to the monitoring dashboard.

After a dashboard is created, you can add graphs to monitor your GeminiDB Redis instances.

1. In the navigation pane on the left, choose **Dashboard**. Locate the dashboard that you want to add a graph to, and click **Add Graph**.

Figure 3-64 Adding a graph



2. On the **Add Graph** page, select a line chart or bar chart.
   - A curve chart reflects changes and peak values of a metric over time.
   - A bar chart reflects metric data of top-ranked resources of the same type, helping you to understand upper and lower limits of a metric.
3. At the **Monitoring Item Configuration** area, configure required parameters by referring to **Table 3-15**.

Figure 3-65 Monitored item configuration

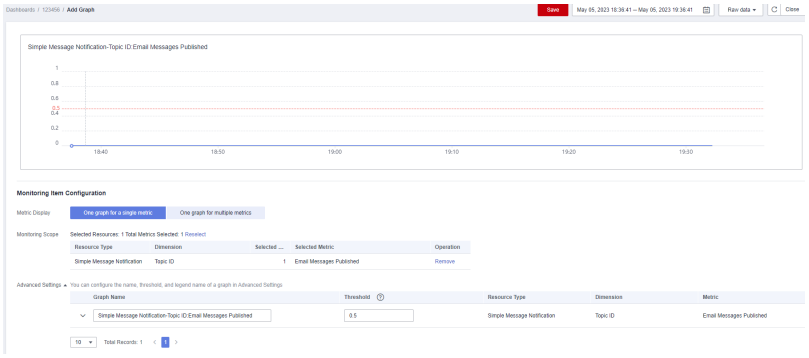


Table 3-15 Parameter description

Parameter	Description
Metric Display	– **One graph for a single metric**: One or more graphs can be generated, and all monitoring items in each graph represent the same metric. – **One graph for multiple metrics**: One graph is generated for multiple metrics, and monitoring items can represent different metrics.
Monitoring Scope	Specify resources and metrics.
Graph Name	Specifies the title of the graph to be added. The name can contain a maximum of 128 characters. Only letters, digits, underscores (_), and hyphens (-) are allowed. Example: CPU usage
Threshold	Configure a threshold to generate an auxiliary line. Data points higher than the line are highlighted in red.
Legend Name	The legend name is displayed on the line in a monitoring graph and can be changed. If you do not configure the legend name, it is displayed in the following format by default: *monitored object* (*resource type*) - *metric*. *monitored data*.

NOTE

When you add a graph, select **One graph for a single metric**. Then a graph is generated for each metric, making it easy for you to view and analyze monitored data. If you need multiple metrics, add monitoring graphs.

4. On the selected dashboard, view metric trends on the added graph.

----End

3.9 Data Backup

3.9.1 Overview

GeminiDB Redis allows you to back up instances to protect your data. After an instance is deleted, the manual backup data is retained. Automatic backup data is released together with instances. Backup data cannot be downloaded or exported.

Backup Methods

Both automatic backup and manual backup are supported.

- Automated backup

  You can **modify backup policy** on the GeminiDB console, and the system will automatically back up your instance data based on the time window and

backup cycle you configure in the backup policy and will store the data for a length of time you specify.

Automated backups cannot be manually deleted. You can adjust their retention period by referring to **Modifying an Automated Backup Policy**, and backups that expire will be automatically deleted.

- Manual backup

  A manual backup is a full backup of a DB instance and can be retained until you manually delete it. Manual backup can be triggered at any time to meet your service requirements.

  Regularly backing up your database is recommended. If your database becomes faulty or data is corrupted, you can restore it from backup.

Table 3-16 Backup methods

Method	Scenario
Automated backup	After you set a backup policy, the system automatically backs up your database based on the policy. You can also modify the policy based on service requirements.
Manual backup	You can manually create full backups for your instance based on service requirements.

How Backup Works

GeminiDB Redis API takes snapshots of persistent data in seconds an d then stores them as compressed packages in OBS, without using any of the storage space of your instance. GeminiDB Redis API consumes a few compute resources during backup, so it is normal if the instance CPU usage and memory usage increase slightly.

Redis Community Edition is slow in backup and jitter may happen in performance. By contrast, GeminiDB Redis API backs up data faster, and almost no jitter occurs during the backup.

Backup Storage

Backups are stored in OBS buckets to provide disaster recovery and save storage space.

After you purchase an instance, GeminiDB Redis will provide additional backup storage of the same size as what you purchased. For example, if you purchase an instance with 100 GB of storage, you will obtain additional 100 GB of storage free of charge. If the backup data does not exceed 100 GB, it is stored on OBS free of charge. If there is more than 100 GB of data, you will be billed at standard OBS rates.

3.9.2 Managing Automated Backups

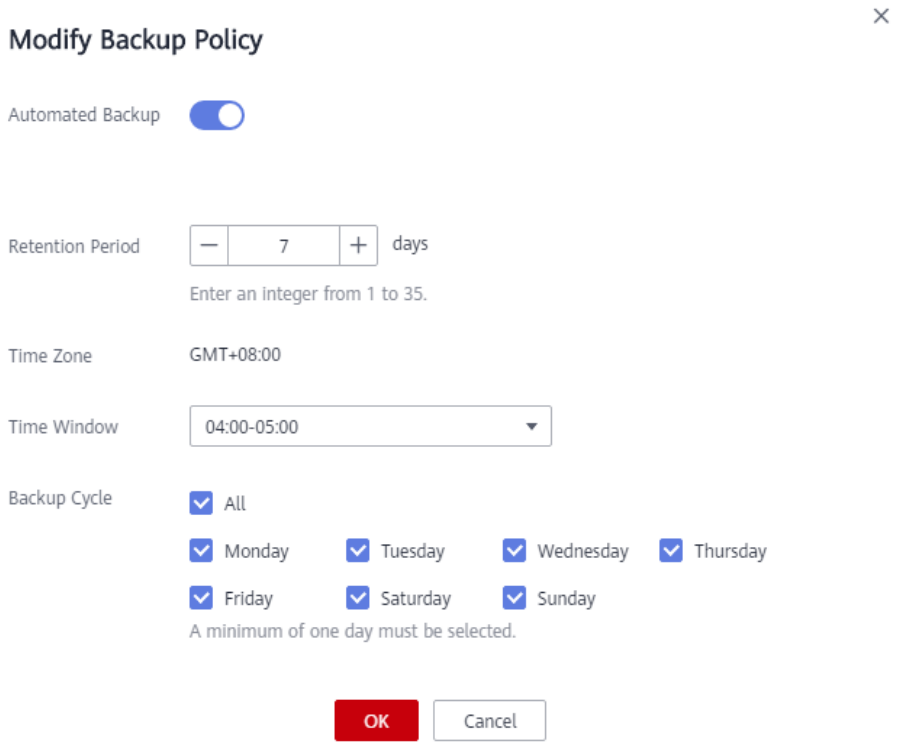
GeminiDB Redis allows you to create automated backups to protect your data. If a database or table is deleted, maliciously or accidentally, backups can help recover your data.

Configuring an Automated Backup Policy

Automated backups are generated based on a backup policy and saved as packages in OBS buckets to secure and protect your data. Regularly backing up your database is recommended. If your database becomes faulty or data is corrupted, you can restore it from backup. Backing up data affects the database read and write performance, so you are advised to set the automated backup time window to off-peak hours.

When you create an instance, an automated backup policy is enabled by default.

Figure 3-66 Enabling automated backup



- **Retention Period**: Automated backup files are saved for seven days by default. The backup retention period can range from 1 to 35 days. Full backups are retained till the retention period expires.
  - Extending the retention period improves data reliability. You can extend the retention period as needed.
  - If you shorten the retention period, the new backup policy takes effect for existing backups. Any automated backups (including full and incremental backups) that have expired will be automatically deleted. Manual backups will not be automatically deleted but you can delete them manually.

NOTE

- If the retention period is less than seven days, the system automatically backs up data daily.
- The system checks existing automated backups and deletes any backups that exceed the backup retention period you configure.
- **Time Window**: A one-hour period the backup will be scheduled for, such as 04:00–05:00. The backup time is in GMT format. If the DST or standard time is switched, the backup time segment changes with the time zone.

If **Retention Period** is set to **2**, full and incremental backups that have been stored for more than two days will be automatically deleted. For instance, a backup generated on Monday will be deleted on Wednesday; or a backup generated on Tuesday will be deleted on Thursday.

Policy for automatically deleting full backups:

To ensure data integrity, even after the retention period expires, the most recent backup will be retained, for example,

If **Backup Cycle** was set to **Monday** and **Tuesday** and the **Retention Period** was set to **2**:

– A full backup generated on Monday will be automatically deleted on Thursday. The reasons are as follows:

  The full backup generated on Monday expires on Wednesday, but it is the last backup, so it will be retained until a new backup expires. The next backup will be generated on Tuesday and will expire on Thursday. So the full backup generated on Monday will not be automatically deleted until Thursday.

– The full backup generated on Tuesday will be automatically deleted on the following Wednesday. The reasons are as follows:

  The backup generated on Tuesday will expire on Thursday, but as it is the last backup, so it will be retained until a new backup expires. The next backup will be generated on the following Monday and will expire on the following Wednesday. So the full backup generated on Tuesday will not be automatically deleted until the following Wednesday.

- **Backup Cycle**: All options are selected by default.
  – **All**: Each day of the week is selected. The system automatically backs up data every day.
  – Select a cycle: You can select one or more days in a week. The system automatically backs up data at the specified time.

  NOTE

  A full backup starts within one hour of the time you specify. The amount of time required for the backup depends on the amount of data to be backed up. The more data has to be backed up, the longer it will take.

- After the DB instance is created, you can modify the automated backup policy as needed. You can change the time window after the DB instance is created. The system backs up data based on the automated backup policy you have set.
- If the automated backup policy is disabled, any automated backups in progress stop immediately.

Modifying an Automated Backup Policy

Step 1 Log in to the management console.

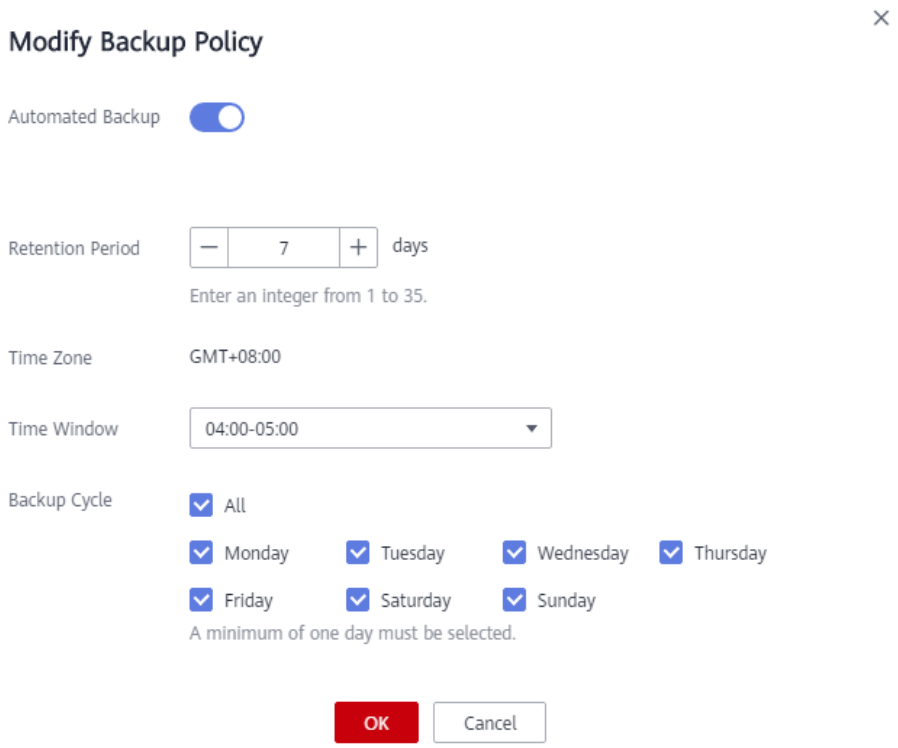
Step 2 In the service list, choose **Databases** > **GeminiDB**.

Step 3 On the **Instances** page, click the instance whose backup policy you want to modify.

Step 4 Choose **Backups & Restorations** in the navigation pane one the left, and click **Modify Backup Policy**. In the displayed dialog box, set the backup policy. Then, click **OK**.

For details about how to set a backup policy, see **Configuring an Automated Backup Policy**.

Figure 3-67 Modifying a backup policy



Step 5 Check or manage the generated backups on the **Backups** or **Backups & Restorations** page.

----End

Disabling Automated Backup

Step 1 Log in to the management console.

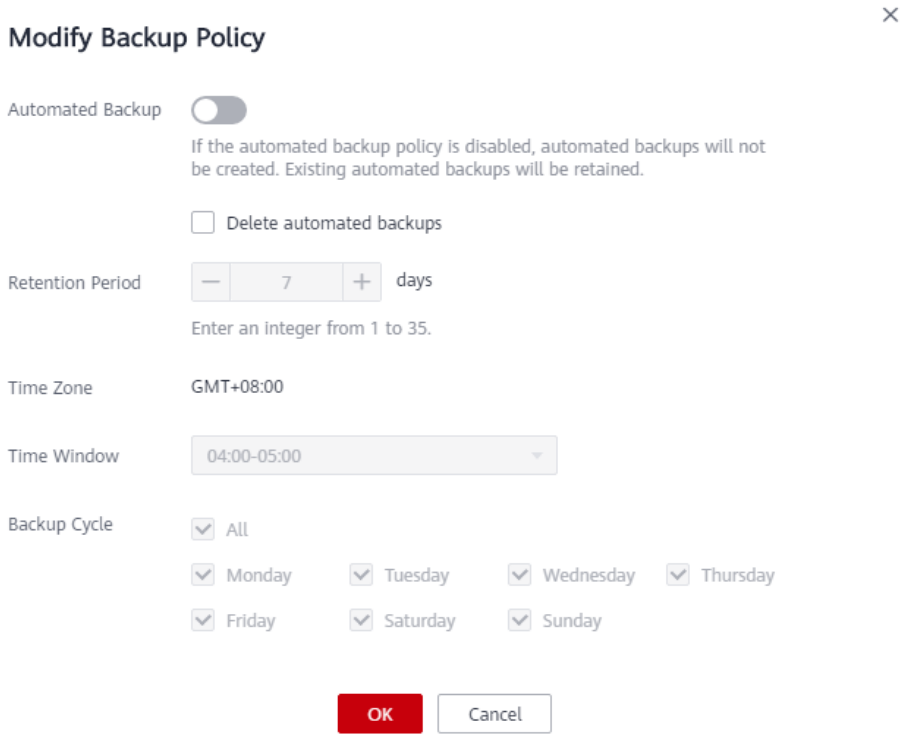
Step 2 In the service list, choose **Databases** > **GeminiDB**.

Step 3 On the **Instances** page, click the instance whose backup policy you want to modify.

Step 4 Choose **Backups & Restorations** in the navigation pane one the left, and click **Modify Backup Policy**.

Step 5 In the displayed dialog box, click  to disable the backup policy and click **OK**.

Figure 3-68 Disabling the automated backup policy



When disabling the automated backup policy, you can decide whether to delete the automated backups by selecting **Delete automated backups**.

- If you select it, all backup files within the retention period will be deleted. No automated backups are displayed in the backup list until you enable the automated backup policy again.
- If you do not select it, all backup files within the retention period will be retained, but you can still manually delete them later if needed. For details, see **Deleting an Automated Backup**.

If automated backup is disabled, any automated backups in progress stop immediately.

----End

Deleting an Automated Backup

If automated backup is disabled, you can delete stored automated backups to free up storage space.

If automated backup is enabled, the system will delete automated backups as they expire. You cannot delete them manually.

NOTICE

Deleted backups cannot be recovered. Exercise caution when performing this operation.

- **Method 1**
  a. Log in to the management console.
  b. In the service list, choose **Databases** > **GeminiDB**.
  c. On the **Instances** page, click the instance whose backup you want to delete.
  d. On the **Backups & Restorations** page, locate the backup you want to delete and click **Delete**.
  e. In the **Delete Backup** dialog box, confirm the backup details and click **Yes**.
- **Method 2**
  a. Log in to the management console.
  b. In the service list, choose **Databases** > **GeminiDB**.
  c. On the **Backups** page, locate the backup that you want to delete and click **Delete**.
  d. In the **Delete Backup** dialog box, confirm the backup details and click **Yes**.

3.9.3 Managing Manual Backups

GeminiDB Redis allows you to manually back up instances whose status is **Available** to protect your data. If a database or table is deleted, maliciously or accidentally, backups can help recover your data.

NOTE

- By default, you can create up to 50 backups.
- Manual backups are full backups.

Creating a Manual Backup

Step 1 Log in to the management console.

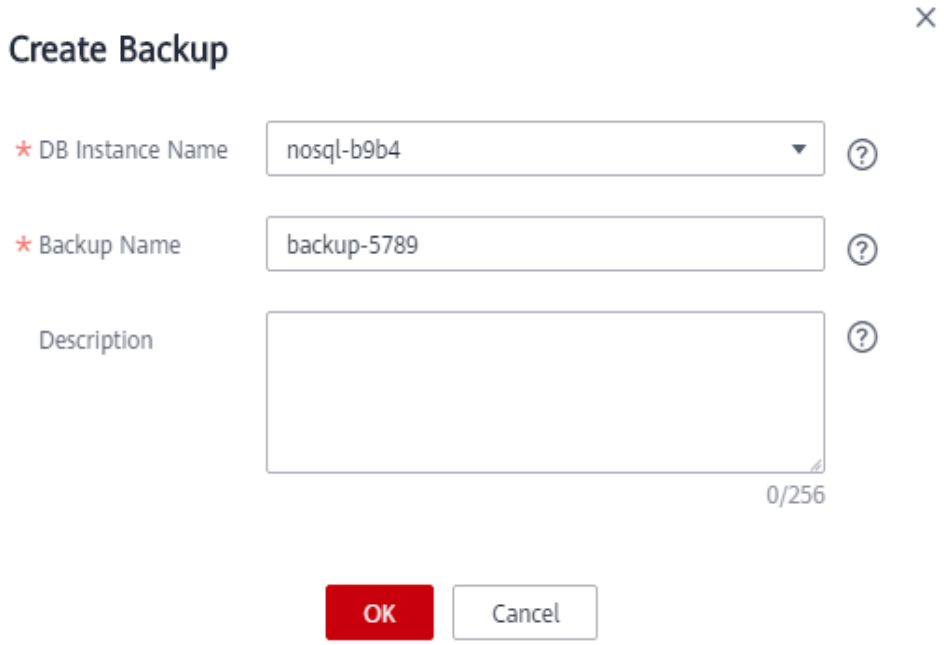
Step 2 In the service list, choose **Databases** > **GeminiDB**.

Step 3 Create a manual backup.

Method 1

On the **Instances** page, locate the instance you want to back up and choose **More** > **Create Backup** in the **Operation** column.

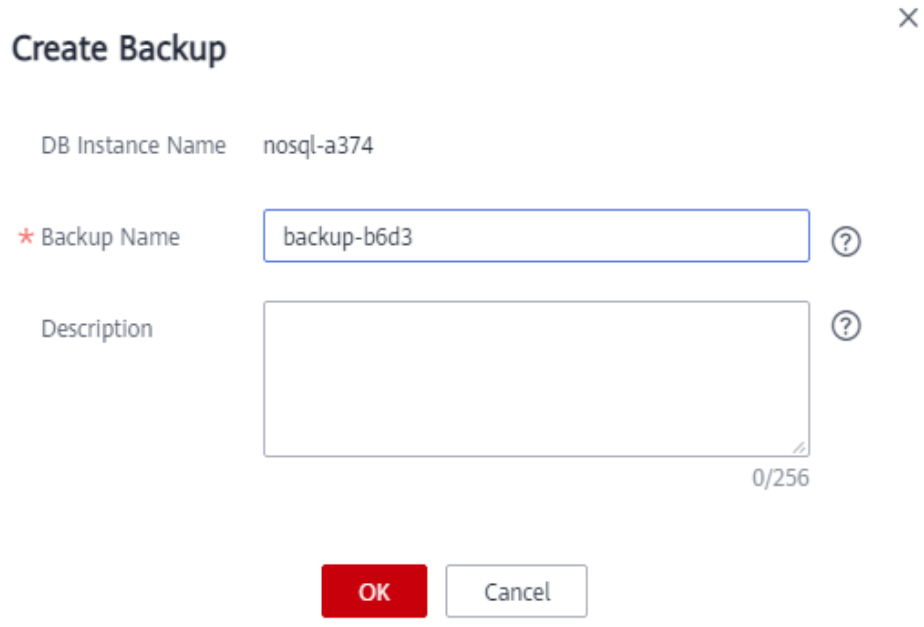
Figure 3-69 Creating a manual backup



Method 2

1. On the **Instances** page, click the instance you want to back up.
2. Choose **Backups & Restorations** in the navigation pane on the left, and click **Create Backup**.

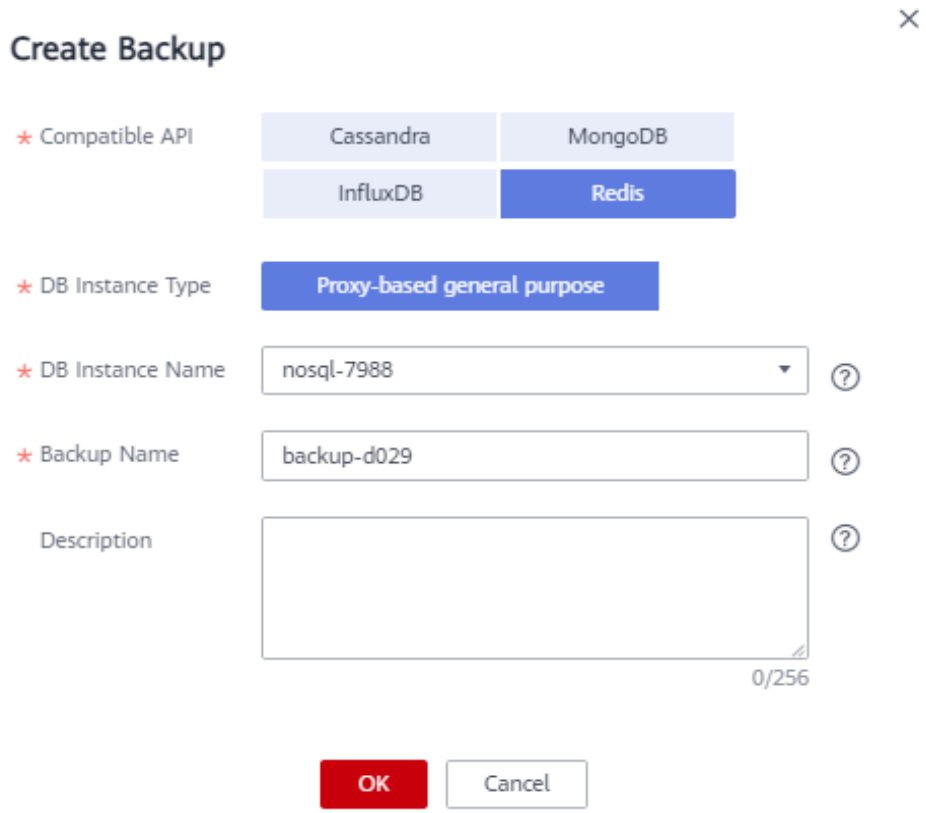
Figure 3-70 Creating a manual backup



Method 3

In the navigation pane on the left, choose **Backups**. On the displayed page, click **Create Backup**.

Figure 3-71 Creating a manual backup



Step 4 In the displayed dialog box, specify a backup name and description and click **OK**.

Table 3-17 Parameter description

Parameter	Description
DB Instance Name	Must be the name of the DB instance to be backed up and cannot be modified.
Backup Name	Must be 4 to 64 characters long and start with a letter. It is case-insensitive and contains only letters, digits, hyphens (-), and underscores (_).
Description	Can include a maximum of 256 characters and cannot contain line breaks and the following special characters: >!<"&'=

Step 5 View the backup status.

- When the backup is being created, query the backup status on the **Backups** or **Backups & Restorations** page. The backup status is **Backing up**.

- After the backup is created, the backup status changes to **Completed**.

----End

Deleting a Manual Backup

If you do not need a manual backup any longer, delete it on the **Backups** or **Backups & Restorations** page.

Deleted backups are not displayed in the backup list.

NOTICE

Deleted backups cannot be recovered. Exercise caution when performing this operation.

Method 1

1. Log in to the management console.
2. In the service list, choose **Databases** > **GeminiDB**.
3. On the **Instances** page, locate the instance whose backup you want to delete and click its name.
4. Choose **Backups & Restorations** in the navigation pane on the left, locate the backup you want to delete, and click **Delete** in the **Operation** column.
5. In the displayed dialog box, confirm the backup details and click **Yes**.

Method 2

1. Log in to the management console.
2. In the service list, choose **Databases** > **GeminiDB**.
3. On the **Backups** page, locate the backup that you want to delete and click **Delete**.
4. In the displayed dialog box, confirm the backup details and click **Yes**.

3.10 Data Restoration

3.10.1 Restoration Methods

GeminiDB Redis supports multiple forms of data restoration. You can select one based on service requirements.

Table 3-18 Restoration methods

Method	Scenario
Restoring Data to a New Instance	You can restore an existing backup file to a new instance.

3.10.2 Restoring Data to a New Instance

Scenarios

GeminiDB Redis allows you to use an existing backup to restore data to a new instance.

Procedure

Step 1 Log in to the management console.

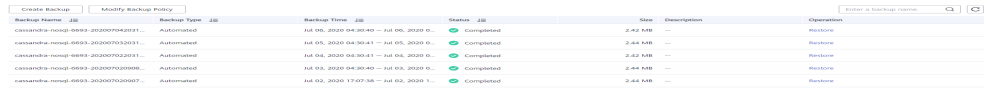
Step 2 In the service list, choose **Databases** > **GeminiDB**.

Step 3 Restore a DB instance from the backup.

Method 1

1. On the **Instances** page, locate the instance whose backup you want to restore and click its name.
2. Choose **Backups & Restorations** in the navigation pane on the left, locate the backup that you want to restore and click **Restore** in the **Operation** column.

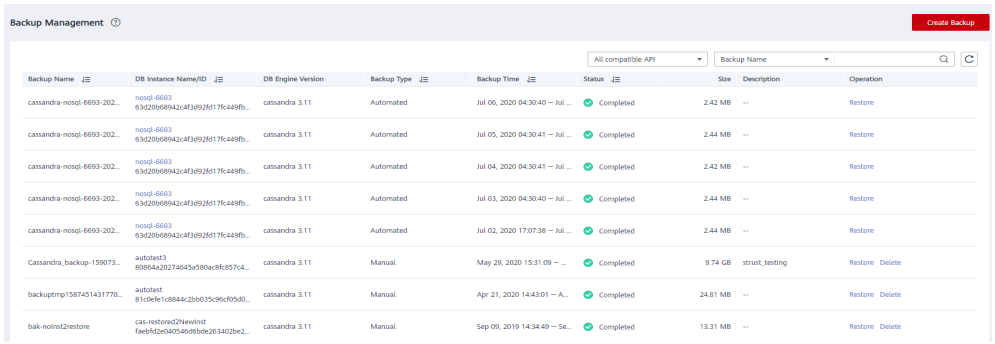
Figure 3-72 Backups and restorations



Method 2

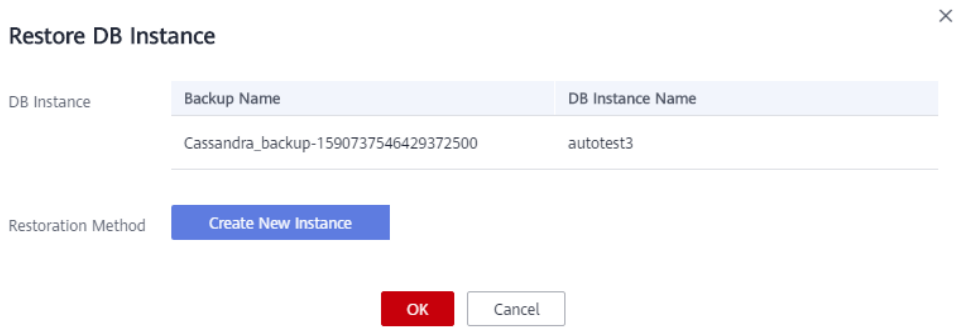
On the **Backups** page, locate the backup that you want to restore and click **Restore** in the **Operation** column.

Figure 3-73 Backup management



Step 4 In the displayed dialog box, confirm the current instance details and restoration method and click **OK**.

Figure 3-74 Restoring data to a new DB instance



- The default API type and DB engine version are the same as those of the original instance and cannot be changed.
- The new instance must have no less than nodes than the original instance.
- GeminiDB automatically calculates the minimum storage space required for restoration based on the size of the selected backup file. The storage capacity depends on the instance specifications, and must be an integer.
- You need to set a new administrator password.
- To modify other parameters, see the description of buying instances of other DB APIs in *Getting Started*.

Step 5 View the restoration results.

A new instance is created using the backup data. The status of the new instance changes from **Creating** to **Available**.

After the restoration, the system will perform a full backup.

The new DB instance is independent from the original one.

----End

4 FAQs

4.1 Most Asked Questions

Database Connection

- How Do I Access GeminiDB Redis?
- What Can I Do with IP Addresses of GeminiDB Redis Nodes?
- How Does Load Balancing Work in GeminiDB Redis?
- Can I Change the VPC of a GeminiDB Redis Instance?

Database Usage

- How Do I Select Specifications and Nodes When Creating a GeminiDB Redis Instance?
- Why Is the Key Not Returned Using Scan Match?
- How Do I Process Existing Data Shards After Migrating Workloads to GeminiDB Redis?

4.2 Product Consulting

4.2.1 What Should I Pay Attention to When Using GeminiDB Redis?

1. DB instance operating systems (OSs) are invisible to you. Your applications can access a database only through an IP address and a port.
2. The backup files stored in OBS and the system containers used by GeminiDB Redis are invisible to you. They are visible only in the GeminiDB Redis management system.
3. Precautions after purchasing instances:

   After purchasing instances, you do not need to perform basic database O&M operations, such as applying HA and security patches, but you should still note:

a. The CPU, input/output operations per second (IOPS), and space are insufficient for the DB instances.
b. The DB instance has performance problems and whether optimization is required.

4.2.2 What Is the Availability of a GeminiDB Redis Instance?

The formula for calculating the instance availability is as follows:

DB instance availability = (1 – Failure duration/Total service duration) × 100%

The failure duration refers to the total duration of faults that occur during the running of a DB instance after you buy the instance. The total service duration refers to the total running time of the DB instance.

4.3 Billing

4.3.1 What Are the Differences Between Yearly/Monthly and Pay-per-use Billing Mode?

Yearly/Monthly is a prepaid billing mode in which resources are billed based on the service duration. This cost-effective mode is ideal when the duration of resource usage is predictable. It is recommended for long-term users.

Pay-per-use is a post payment mode, so you can start or stop an instance at any time. Pricing is listed on a per-hour basis, but bills are calculated based on the actual usage duration.

4.3.2 Can I Switch Between Yearly/Monthly and Pay-per-Use Payments?

You can change the billing mode from yearly/monthly to pay-per-use or vice versa.

- For details about how to change the billing mode from yearly/monthly to a pay-per-use, see **Changing the Billing Mode from Yearly/Monthly to Pay-per-Use**.
- For details about how to change the billing mode from pay-per-use to yearly/monthly, see **Changing the Billing Mode from Pay-per-Use to Yearly/Monthly**.

4.4 Database Usage

4.4.1 Why Is the Key Not Returned Using Scan Match?

Symptom

As shown in the following figure, the value of key is **test** and exists in the database. However, no data is returned using this scan match command.


```
139.9.177.148: 8635> scan 1 match tes*
1) "21"
2) (empty list or set)
139.9.177.148: 8635> get test
"abc"
139.9.177.148:8635>scan 0 match tes*
1) "21"
2) (empty list or set)
139.9.177.148: 8635>
```

Possible Causes

The MATCH command is used to iterate elements that only match a specified pattern. Pattern matching is performed after the command obtain elements from the data set and before the elements are returned to the client. If all the extracted elements do not match the pattern, no element is returned.

Solution

If multiple scans are performed, the iteration is complete when the returned cursor is 0. The cursor returned from the last scan is used for the next scan.

4.4.2 How Do I Select Specifications and Nodes When Creating a GeminiDB Redis Instance?

GeminiDB Redis provides multiple instance specifications. The performance depends on the instance specifications and the number of nodes. This section summarizes some practical experience to help you determine the instance specifications and node quantity.

1. Higher specifications can provide better performance. For details about the supported instance specifications, see **Instance Specifications**.
2. If the instance specifications are the same, more nodes provide better performance.
3. Select specifications that can meet your service requirements based on the test data and reserve some resources for reliability redundancy and future service growth.
4. Generally, a single-core CPU has good performance when the data size is 16 GB. For example, if the service data volume is 128 GB and is not expected to increase any further, you can purchase two instances each with 4 vCPUs and 16 GB memory.

4.4.3 How Do I Process Existing Data Shards After Migrating Workloads to GeminiDB Redis?

GeminiDB Redis uses decoupled compute and storage and allows adding data shards dynamically, making scaling smooth. After the GeminiDB Redis instance is connected, data sharding is not required on the service side.

4.4.4 Does GeminiDB Redis Support Fuzzy Query Using the Keys Command?

Yes.

An OOM error or high latency may occur when you query data using the KEYS command. You can use the KEYS command for service tests, but not for production. You can use SCAN and MATCH commands for fuzzy match.

4.4.5 Does the GeminiDB Redis Support Multiple Databases?

GeminiDB Redis allows you to create multiple databases in an instance since March 2022. Instances created before March 2022 do not support this function and cannot be upgraded to support it.

This feature has the following constraints:

- The number of databases ranges from 0 to 65535.
- The SWAPDB command is not supported.
- The result of the **dbsize** command is not updated in real time. The result does not decrease to 0 immediately after **flushdb** is executed, and will change to 0 after a while.
- Executing SELECT and FLUSHDB commands in LUA scripts is not supported.
- Executing SELECT and FLUSHDB commands in transactions is not supported.
- The MOVE command is not supported.

4.4.6 Why the Values Returned by Scan Operations Are Different Between GeminiDB Redis and Open-source Redis 5.0?

GeminiDB Redis may return values in a different sequence from open-source Redis, but they both comply with open-source document description requirements. This is because open-source Redis does not specify the sorting rules for:

- Returned values of SCAN/HSCAN/SSCAN operations
- Returned values of ZSCAN operations ZSET when its elements have the same score

4.4.7 Why Are Error Messages Returned by Some Invalid Commands Different Between GeminiDB Redis and Open-Source Redis 5.0?

GeminiDB Redis checks command syntax and checks for keys each time it executes a command. However, open-source Redis has no specific rules and returns the results for invalid commands in random. Therefore, error messages returned by some invalid commands may be different.

4.5 Database Connection

4.5.1 How Do I Access GeminiDB Redis?

You can access GeminiDB Redis over a private network, public network, domain name, load balancer IP address, or program code. For details, see **Connection Methods**.

4.5.2 What Can I Do with IP Addresses of GeminiDB Redis Nodes?

GeminiDB Redis provides multiple IP addresses for you to access a cluster and achieve load balancing and disaster recovery.

You can use multiple IP addresses in any of the following ways.

1. Use the connection pool on the service side implement load balancing and fault detection.
2. Contact customer service to configure the Elastic Load Balance (ELB) service and provide a unique IP address.
3. Configure domain names for multiple proxy IP addresses. For details about how to connect to a DB instance through a private domain name, see **Connecting to an Instance Using a Load Balancer Address (Recommended)**.

4.5.3 How Does Load Balancing Work in GeminiDB Redis?

For details, see **Elastic Load Balance**.

4.5.4 How Can I Create and Connect to an ECS?

1. To create an ECS, see *Elastic Cloud Server User Guide*.
   - The ECS to be created must be in the same VPC and security group with the GeminiDB Redis instance to which it connects.
   - Configure the security group rules to allow the ECS to access to the instance.
2. To connect to an ECS, see "Logging in to an ECS" *Getting Started with Elastic Cloud Server User Guide*.

4.5.5 Can I Change the VPC of a GeminiDB Redis Instance?

After a GeminiDB Redis instance is created, the VPC where the instance resides cannot be changed.

However, you can change a VPC by restoring the full backup of your instance to the VPC you want to use. For details, see **Restoring Data to a New Instance**.

4.6 Backup and Restoration

4.6.1 How Long Can a GeminiDB Redis Instance Backup Be Saved?

Automated backup data is kept based on the backup retention period you specified. There is no limit for the manual backup retention period. You can delete manual backups as needed.

For more backup information, see **Managing Automated Backups** and **Managing Manual Backups**.

4.7 Instance Freezing, Release, Deletion, and Unsubscription

Why Are My GeminiDB Redis Instances Released?

If your subscriptions have expired but not been renewed, or you are in arrears due to insufficient balance, your instances enter a grace period. If you do not renew the subscriptions or top up your account after the grace period expires, your instances will enter a retention period and become unavailable. If you still do not renew them or top up your account after the retention period ends, your instances will be released and your data stored will be deleted.

Why Are My GeminiDB Redis Instances Frozen?

Your instances may be frozen for a variety of reasons. The most common reason is that you are in arrears.

Can I Still Back Up Data If My Instances Are Frozen?

No. If your GeminiDB Redis instances are frozen because your account is in arrears, go to top up your account to unfreeze your instances and then back up instance data.

How Do I Unfreeze My Instances?

If your GeminiDB Redis instances are frozen because your account is in arrears, you can unfreeze them by renewing them or topping up your account. The frozen GeminiDB Redis instances can be renewed, released, or deleted. Yearly/Monthly instances that have expired cannot be unsubscribed from, while those that have not expired can be unsubscribed from.

What Impacts Does Instance Freezing, Unfreezing or Release Have on My Services?

- After an instance is frozen:
  - It cannot be accessed, and your services will be interrupted. For example, if a GeminiDB Redis instance is frozen, it cannot be connected.
  - No changes can be performed on it if it is a yearly/monthly instance.
  - It can be unsubscribed from or deleted manually.
- After it is unfrozen, you can connect to it again.
- Releasing an instance means deleting it. Before the deletion, GeminiDB Redis API determines whether to **move the instance to the recycle bin** based on the recycling policy you specified.

How Do I Renew My Instances?

After a yearly/monthly GeminiDB Redis instance expires, you can renew it on the **Renewals** page. For details, see **Renewal Management**.

Can My Instances Be Recovered After They Are Released or Unsubscribed From?

If your instance is moved to the recycle bin after being deleted, you can recover it from the recycle bin by referring to **Recycling an Instance**. If the recycling policy is not enabled, you cannot recover it.

When you unsubscribe from an instance, confirm the instance information carefully. If you have unsubscribed from an instance by mistake, purchase a new one.

How Do I Delete a GeminiDB Redis Instance?

- To delete a pay-per-use instance, see **Deleting a Pay-per-Use Instance**.
- To delete a yearly/monthly instance, see **Unsubscribing from a Yearly/Monthly Instance**.

A Change History

Release Date	Description
2023-03-27	This issue is the second official release. In **Instance Specifications**, added the description of instances, each with a vCPUs to memory ratio of 1:4.
2023-02-19	This issue is the first official release.

