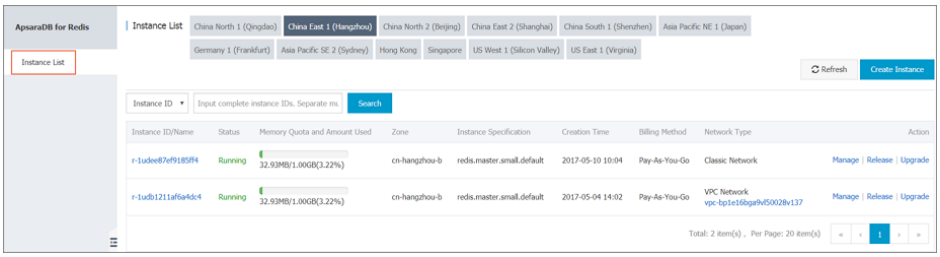
ApsaraDB for Redis

User Guide

User Guide

Log on to the Redis Console with the account used to purchase the ApsaraDB for Redis service. The **Instance List** page is displayed, as shown in the following figure.



Manage instances

You can reset an instance password if you forgot the password, need to change the password, or did not set a password when creating the instance.

Log on to the Redis Console.

Find the target instance and click the instance ID or **Manage** to go to the **Instance Information** page.

In the **Change Password** window, enter the old password and a new password and click **OK**.

Note:

If you forgot your password, click **Forgot Password** in the **Change Password** window. Then you can set a new password in the **Reset Password** window.

The password must consist of 8 to 30 characters, including upper-case letters, lower-case letters, and numbers at the same time.

ApsaraDB supports two types of network: classic and Virtual Private Cloud (VPC). This chapter describes the differences between the two network types and setting methods.

Background

On the Alibaba Cloud platform, a classic network and VPC have the following differences:

Classic network: The cloud services on a classic network are not isolated, and unauthorized access to a cloud service is blocked only by the security group or whitelist policy of the service.

VPC: The VPC helps you build an isolated network environment on Alibaba Cloud. You can customize the route table, IP address range, and gateway in VPC. In addition, you can combine your machine room and cloud resources in the Alibaba Cloud VPC into a virtual machine room through a leased line or VPN to migrate applications to the cloud smoothly.

Note:

A classic network can be converted to VPC, but not vice versa.

When switching the classic network to VPC, you can choose to retain the classic network IP address. For more information, see Hybrid access.

By default, ApsaraDB for Redis adopts the classic network type. If you want to use VPC, make sure that the ApsaraDB for Redis instance and VPC instance are in the same region. You may create a VPC instance by using either of the following methods:

If no ApsaraDB for Redis instance is created, first create a VPC instance and then create an ApsaraDB for Redis instance under the VPC instance. For more information, see the section Create an ApsaraDB for Redis instance scenario.

If an ApsaraDB for Redis instance already exists, create a VPC instance in the same region as the ApsaraDB for Redis instance and add the ApsaraDB for Redis instance to the VPC instance. For more information, see the section Existing ApsaraDB for Redis instance scenario .

Create an ApsaraDB for Redis instance scenario

Create a VPC instance. For more information, see Create a VPC instance.

Create an ApsaraDB for Redis instance in the same region as the VPC instance.

When you purchase the ApsaraDB for Redis instance, select VPC as the network type and select the corresponding VPC instance. For more information, see Create an instance.

Existing ApsaraDB for Redis instance scenario

Create a VPC instance in the same region as the ApsaraDB for Redis instance. For more information, see Create a VPC instance.

Log on to the Redis Console, select the target instance, and click **Manage**.

Click **Switch to VPC** on the **Instance Information** page.

On the **Switch to VPC** page, select VPC and VSwitch. Select whether to retain the classic network IP address and the retention period, and then click **OK**.

ApsaraDB for Redis supports Pay-As-You-Go instances, and the instance configuration can be changed in real time.

Background

Changing instance configuration will incur a change in charges. For more information about the billing standard, see ApsaraDB for Redis pricing details.

Note:

Pay-As-You-Go instances support real-time configuration upgrade/downgrade.

Cluster instances and master-slave instances support mutual configuration upgrade/downgrade.

The instance will experience intermittent interruption for several seconds during configuration change, so perform upgrade during off-peak hours if possible.

Procedure

Log on to the Redis console.

Find the target instance and click **Change Configuration**.

On the **Change Configuration** page, select the expected configuration and click **Confirm to Change**.

You will be prompted after the configuration is successfully changed. If the instance is Pay-As-You-Go, it will be billed for the new configuration starting from the billing cycle when the change occurred.

Note: The data cleanup operation will clear all data of the target instance and the cleared data cannot be recovered. Please be careful with this operation.

Log on to the Redis Console and find the target instance.

Click the instance ID or **Manage** to go to the **Instance Information** page.

Click **Clear Data** and then click **OK** in the displayed confirm box.

On the **Mobile Phone Verification** page, obtain and enter the verification code to complete data cleanup.

Note: Pay-As-You-Go instances can be released at any time, whereas subscribed instances cannot be manually deleted or released.

Procedure

Log on to the Redis Console and find the target instance.

Click **Instance ID** or **Manage** to go to the **Instance Information** page.

Click **Release** and then click **OK** in the displayed confirm box.

On the **Mobile Phone Verification** page, obtain and enter the verification code to release the instance.

After setting the retention period for the access address of a classic network, you can prolong the retention time on the console before the time expires.

In the hybrid access period, you can change the retention time of the original classic network at any time as needed. The expiration date is recalculated from the new date. For example, if the Intranet address of the original classic network is set to expire on August 18, 2017 and you change the expiration date to “14 days later” on August 15, 2017, the Intranet address is released on August 29, 2017.

Procedure

Log on to the Redis console.

On the **Instance List** page, find the target instance and click **Manage** to go to the **Instance Information** page.

In the **Retained Connection Address of the Classic Network** area, click **Modify Retention Period**.

In the displayed dialog box, select a new expiration date and click **OK**.

Background

To guarantee the stability of ApsaraDB for Redis instances, the backend system irregularly maintains instances and machines on the Alibaba Cloud platform.

Before the official maintenance, ApsaraDB for Redis sends SMS messages and emails to contacts configured in your Alibaba Cloud account.

To guarantee the stability during maintenance process, instances enter the **Being Maintained** state before the preset O&M time on the day of maintenance. When an instance is in this state, the normal access to data in the database is not affected. However, change-related functions (for example, configuration change) are temporarily unavailable for this instance on the console, whereas query functions such as performance monitoring are still available.

> **Note**: After the preset maintenance window time is reached, instances may experience intermittent interruption during maintenance, so we recommend that instances be maintained during off-peak hours if possible.

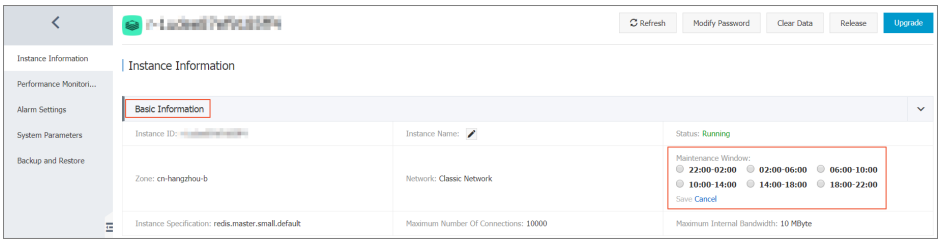
Procedure

Log on to the Redis Console and find the target instance.

Click **Instance ID** or **Manage** to go to the **Instance Information** page.

Click **Set** next to **Maintenance Window** in **Basic Information**, as shown in the following figure.

The default maintenance window for ApsaraDB for Redis is from 02:00 to 06:00.



Select an maintenance window and click **Save**.

> **Note**: The O&M time is in Beijing time.

Context

ApsaraDB for Redis provides 10 monitoring groups. You can custom metrics on the ApsaraDB for Redis console based on business requirements, or enable real-time monitoring for ApsaraDB for Redis instances using DMS for Redis.

Metric descriptions

Monitoring group	Data metric	Description
Basic monitoring group	The basic instance monitoring information	Includes QPS, bandwidth, and memory usage.
Keys monitoring group	Monitoring statistics on the use of key value-related commands	Number of times that commands used to delete keys, determine whether a key exists, and perform other such operations were called
String monitoring group	Monitoring statistics on the use of string data-related commands	Number of times that string data commands, such as append and mget, were

		called
Hashes monitoring group	Monitoring statistics on the use of hash data-related commands	Number of times that hash data commands, such as hget and hdel, were called
Lists monitoring group	Monitoring statistics on the use of list data-related commands	Number of times that list data commands, such as blpop and brpop, were called
Sets monitoring group	Monitoring statistics on the use of set data-related commands	Number of times that set data commands, such as saadd and scard, were called
Zsets monitoring group	Monitoring statistics on the use of zset data-related commands	Number of times that zset data commands, such as zadd and zcard, were called
HyperLog monitoring group	Monitoring statistics on the use of HyperLogLog data-related commands	Number of times that HyperLogLog data commands, such as pfadd and pfcount, were called
Pub/Sub monitoring group	Monitoring statistics by using commands related to pub/sub functions	Number of times that pub/sub function commands, such as publish and subscribe, were called
Transaction monitoring group	Monitoring statistics on the use of transaction-related commands	Number of times that transaction-related commands, such as watch, multi, and exec, were called

Start real-time monitoring

Log on to the Redis Console and locate the target instance.

Click the instance ID or **Manage** to go to the **Instance Information** page.

Click **Log on to Database** in the upper right corner.

On the data console logon page, enter the ID and password of the ApsaraDB for Redis instance to go to the homepage of DMS for Redis.

On the **Performance Monitoring** page, click **Real-time Monitor**.

For more information, see DMS documentation.

Custom metrics

Log on to the Redis Console and locate the target instance.

Click the instance ID or **Manage** to go to the **Instance Information** page.

Select **Performance Monitoring** in the left navigation bar.

Click **Custom Metrics**, select the desired monitoring group, and click **OK**.

View historical monitoring data

Log on to the Redis Console and locate the target instance.

Click the instance ID or **Manage** to go to the **Instance Information** page.

Select **Performance Monitoring** in the left navigation bar.

On the **Performance Monitoring** page, query the historical monitoring data of the instance.

Notes:

You can select a time range to query historical monitoring data.

Cluster instances support viewing of the historical monitoring data of each data node. You can click a data node in **Instance Architecture Diagram** on the **Instance Information** page or select **Data Node** on the **Performance Monitoring** page of a cluster instance to query the historical monitoring data of the data node.

Background

ApsaraDB for Redis provides an instance monitoring function and sends an SMS message to you when detecting an instance exception.

Monitoring and alarming are implemented through CloudMonitor. CloudMonitor enables you to set

metrics and notify all contacts in the alarm contact group when the alarm policies of the metrics are triggered. You can maintain an alarm contact group corresponding to an alarm metric so that relevant contacts are promptly notified when an alarm occurs.

Procedure

Log on to the Redis Console and find the target instance.

Click the instance ID or **Manage** to go to the **Instance Information** page.

Select **Alarm Settings** in the navigation bar on the left.

On the **Alarm Settings** page, click **Alarm Settings** to go to the CloudMonitor Console. You can click **Refresh** to manually refresh the current status of the monitoring metrics.

Select **Alarm Rules** > **Create Alarm Rule**.

Add alarm rules on the **Batch Alarm Rule Settings** page.

Click **Next** to set the notification object. You can click **Quickly Create a Contact Group** to create an alarm contact or alarm contact group.

Click **Confirm** to complete alarm setting.

Note: After the alarm setting is completed, you can modify, disable, and delete alarm rules on the **Alarm Rules** page of the CloudMonitor Console. You can also view the alarm history on this page.

As an increasing number of businesses use ApsaraDB for Redis as the ultimate persistent storage engine, users have posed higher data reliability requirements. The ApsaraDB for Redis backup and recovery solution enables comprehensive data reliability upgrade.

Automatic backup (backup policy setting)

Background

As more and more applications use ApsaraDB for Redis for persistent storage, conventional backup mechanisms are required to quickly recover data in the event of misoperation. Alibaba Cloud

executes RDB snapshot backup on slave nodes to protect the performance of your instance during the backup process. Alibaba Cloud also provides convenient console operations, so you can customize the backup settings.

Procedure

Log on to the **Redis console** and find the target instance.

Click the instance ID or **Manage** to go to the **Instance Information** page.

Select **Backup and Recovery** in the navigation bar on the left.

Click **Backup Settings**.

Click **Edit** to customize the automatic backup cycles and times.

> **Note**: By default, backup data is retained for 7 days. This setting cannot be modified.

Click **OK** to complete automatic backup setting.

Manual backup (instant backup)

In addition to the general backup settings, you can initiate a manual backup request on the console at any time.

Log on to the **Redis console** and find the target instance.

Click the instance ID or **Manage** to go to the **Instance Information** page.

Select **Backup and Recovery** in the navigation bar on the left.

Click **Create Backup** in the upper-right corner.

Click **OK** to instantly back up the instance.

> **Note**: On the **Backup Data** page, you can select time ranges to query historical backup data. By default, backup data is retained for 7 days, so you can query historical backup data from the last 7 days.

Backup archiving

Background

Due to industry regulatory or corporate policy requirements, you may need to regularly archive Redis data backups. ApsaraDB for Redis provides a backup archiving function at no charge currently and saves automatic and manual backup files to OSS. Now, Alibaba Cloud stores your backup archives on OSS for 7 days at no charge. After 7 days, the files will be automatically deleted.

If you must retain these archives for a longer period of time, you can copy the link on the console and manually download the database backup files for local storage.

Procedure

1. Log on to the Redis console and find the target instance.
2. Click the instance ID or **Manage** to go to the **Instance Information** page.
3. Select **Backup and Recovery** in the navigation bar on the left.
4. On the backup data page, select the backup data to be archived and click **Download**.

Data recovery

The data recovery function minimizes the damage caused by database misoperations. Now, ApsaraDB for Redis supports data recovery from backups.

1. Log on to the Redis console and find the target instance.
2. Click the instance ID or **Manage** to go to the **Instance Information** page.
3. Select **Backup and Recovery** in the navigation bar on the left.
4. Click the **Backup Data** tab on the **Backup and Recovery** page.
5. Select the time range for recovery and click **Search**. Then select the target backup file and click **Recover Data**.
6. In the **Data Recovery** window, click **OK** to recover the data directly to the original instance. Alternatively, you can choose **Clone Instance** to recover the backup data to a new instance.

After verifying that the recovered data is correct, you can recover the data to the original instance.

Note: As the data recovery operation is highly risky, we suggest using the clone instance method if time permits. This method creates a Pay-As-You-Go instance based on the backup data set to be recovered. After verifying that the data is correct, you can recover the data to the original instance.

Clone instance

Background

During routine maintenance projects, O&M engineers often need to quickly deploy a new application. When application deployment is relatively simple, a new instance can be conveniently created based on an ECS image file. At the database level, however, deployment is more complex. O&M engineers must purchase or install a new database and then initialize relevant database scripts (to create tables, triggers, and views). In such a scenario, many trivial operations must be performed and the error rate is relatively high. Especially in the gaming industry with fast service activation, the rapid deployment of new applications often needs to be repeated many times each day.

To address this pain point, ApsaraDB for Redis develops the clone instance function, enabling you to clone a new subscribed instance or Pay-As-You-Go instance from backup files quickly. Then you can perform complex operations of database development and deployment with a single click on a graphic interface, significantly improving productivity.

Procedure

Log on to the Redis console and find the target instance.

Click the instance ID or **Manage** to go to the **Instance Information** page.

Select **Backup and Recovery** in the navigation bar on the left.

On the **Backup Data** page, select the expected backup data set and click **Clone Instance**.

ApsaraDB for Redis allows you to customize some instance parameters. For details about the parameters that can be modified, refer to **Parameter Settings** on the Redis Console.

Background

As ApsaraDB for Redis is completely compatible with the native database service, their parameter setting methods are similar for users. You can modify parameters through the ApsaraDB for Redis

Console by referring to this example, or through other methods such as redis-cli.

For a description of the database parameters, click the following link to refer to the official documentations for different database versions.

redis.conf for Redis 3.0

redis.conf for Redis 2.8

Procedure

Log on to the Redis Console and find the target instance.

Click the instance ID or **Manage** to go to the **Instance Information** page.

Select **Parameter Settings** in the navigation bar on the left.

Select the desired parameter and click **Modify**.

Modify the parameter value and click **OK**.

Background

To guarantee database security and stability, you must add IP addresses or IP address segments used for database access to the whitelist of the target instance before using ApsaraDB for Redis. Correct use of the whitelist improves access security protection for ApsaraDB for Redis. We recommend that the whitelist be regularly maintained.

Prerequisites

The whitelist feature works properly only with the support by a specific kernel version. If the instance version is not the latest, you will be prompted a messsage during the whitelist setting. For instructions on minor version upgrade, see Upgrade minor versions.

Procedure

Log on to the Redis console and find the target instance.

Click the instance ID or **Manage** to go to the **Instance Information** page.

Select **Security Settings** from the left-side navigation pane, and click **Modify** of the **default** whitelist group.

> **Note**: If you want to add a custom whitelist group to the Redis instance, you can click **Add a Whitelist Group**. The setting steps for a custom whitelist are similar to the following step.

In the **Modify Whitelist Group** window, enter **Group Name** and **Intra-group Whitelist** and then click **OK**.

Parameters description:

Group Name: It can contain 2 to 32 characters, including lowercase letters, digits, or underscores. The group name must start with a lowercase letter and end with a letter or digit. This name cannot be modified when the whitelist group is successfully created.

Whitelist: You can enter the custom IP addresses or IP segments that can access the Redis instance. To allow all IP addresses to access the database, set the whitelist to 0.0.0.0/0. To disable database access from all IP addresses, set the whitelist to 127.0.0.1.

If you enter an IP segment, such as 10.10.10.0/24, it indicates that any IP address in the format of 10.10.10.X can access the Redis instance.

To enter multiple IP addresses or IP segments, separate them by commas. Do not add blank spaces before or after the commas.

For one instance, up to 1,000 IP addresses or IP segments can be set.

Background

Deep kernel optimization is performed on ApsaraDB for Redis to fix security vulnerabilities and improve the service’ s stability. You can upgrade to the latest kernel version in one click on the console.

Note:

The system automatically detects the kernel version of your instance. If the current version is the latest, the **Basic Information** page of the console does not show the **Upgrade Minor Version** button.

Upgrading the kernel version will interrupt your connection for 30 seconds, so perform upgrade during off-peak hours and make sure your applications have a reconnection mechanism.

Procedure

Log on to the **Redis console** and find the target instance.

Click the instance ID or **Manage** to go to the **Instance Information** page.

Click **Upgrade Minor Version** in the **Basic Information** column.

Click **Upgrade Now** in the **Upgrade Minor Version** window.

On the **Basic Information** page, the instance status shows **Upgrading minor version...** Upgrade is completed when the instance status shows **In use**.

Migrate self-built Redis to ApsaraDB for Redis

Redis-cli is the Redis command line interface. ApsaraDB for Redis allows you to use redis-cli to import existing Redis data to ApsaraDB for Redis for seamless migration.

Considerations

Because ApsaraDB for Redis only supports access from the Alibaba Cloud intranet, the following steps only take effect on Alibaba Cloud ECS. If your ApsaraDB for Redis instance is not on ECS, you must copy the existing AOF file to ECS before importing data.

Redis-cli is the Redis command line interface. If you cannot use redis-cli on ECS, you can first

download and install Redis before using redis-cli. See the official document here to download and install Redis on ECS.

Procedure

Follow these steps if you have created an ApsaraDB for Redis instance on ECS:

1. Enable the AOF function for the existing ApsaraDB for Redis instance (skip this step if the AOF function has been enabled).

```
# redis-cli -h old_instance_ip -p old_instance_port config set appendonly yes
```

2. Use the AOF file to import data to the new ApsaraDB for Redis instance (assume that the generated AOF file is named append.aof).

```
# redis-cli -h aliyun_redis_instance_ip -p 6379 -a password --pipe < appendonly.aof
```

Note: If the AOF function does not need to be enabled for the existing ApsaraDB for Redis instance, you can run the following command to disable the function after data is imported:

```
# redis-cli -h old_instance_ip -p old_instance_port config set appendonly no
```

Background

To ensure service availability, ApsaraDB for Redis provides the SLA indicators for your instance from the last two months. Indicators with a value greater than or equal to 99.95% are normal (highlighted in green). If there are indicators with a value smaller than 99.95% (highlighted in red), you can apply for compensation on the console.

For details about the service availability calculation method and compensation standard, refer to Service Level Agreement.

Compensation request time limit

You can apply for compensation for the instance that fell short of the availability standard during the last month after the fifth working day of every month. The application period is limited to the two months following the month when your ApsaraDB for Redis instance fell short of the availability

standard. Application beyond this period will not be accepted.

Procedure

Log on to the Redis Console.

Select the target instance and click **Apply for Compensation**.

On the **SLA Compensation Management** page, submit your application and click **Confirm Compensation Application**.

Note:

After the application is submitted, you can view the application record on the **Applied Compensation** page.

If you have any doubt about the compensation amount, click **Appeal** on the **SLA Compensation Management** page, or click **Apply for Review** on the **Instance List** page to open a ticket for compensation appeal.