Alibaba Cloud

ApsaraDB for Redis

Quick Start

Alibaba Cloud

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
⚠ Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	⚠ **Danger:** Resetting will result in the loss of user configuration data.
🔔 Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	🔔 **Warning:** Restarting will cause business interruption. About 10 minutes are required to restart an instance.
🔊 Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	🔊 **Notice:** If the weight is set to 0, the server no longer receives new requests.
? Note	A note indicates supplemental instructions, best practices, tips, and other content.	? **Note:** You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings> Network> Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
Courier font	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.Overview

This topic describes how to select the series type and specifications of an ApsaraDB for Redis instance. This topic also helps you learn how to create, connect to, develop, and manage an ApsaraDB for Redis instance.

Select a series type and specifications

Before you create an ApsaraDB for Redis instance, you must select a series type and specifications based on various factors, such as performance, price, and workload. For more information, see Select ApsaraDB for Redis instances.

选择Redis系列与规格
在创建Redis实例前，您需要结合性能、价格、工作负载等因素进行选型。
● Redis实例选型最佳实践

Use an ApsaraDB for Redis instance

Step	Description
Step 1: Create an ApsaraDB for Redis instance	ApsaraDB for Redis provides multiple service types and architectures to meet different requirements. You can refer to the relevant topics to create an ApsaraDB for Redis instance.
Step 2: Configure whitelists	Before you use an ApsaraDB for Redis instance, you must add the IP addresses of the clients that are used to access the ApsaraDB for Redis instance to an IP address whitelist of the instance.
Step 3: Connect to an ApsaraDB for Redis instance	You can use Data Management (DMS), a Redis client, or the redis-cli tool to connect to an ApsaraDB for Redis instance.
Step 4: Develop and manage an ApsaraDB for Redis instance	- You can use the ApsaraDB for Redis console, API operations, or SDKs to manage an ApsaraDB for Redis instance. For more information, see Manage ApsaraDB for Redis instances and Quick start. - To make full use of an ApsaraDB for Redis instance, you can follow the standards for business deployment, key design, SDK usage, command usage, and O&M management. For more information, see Development and O&M standards for ApsaraDB for Redis.

References

● Overview
● Limits

2.Step 1: Create an ApsaraDB for Redis instance

ApsaraDB for Redis has two editions: Community Edition and Enhanced Edition (Tair). ApsaraDB for Redis Enhanced Edition (Tair) provides three series types: performance-enhanced instances, persistent memory-optimized instances, and storage-optimized instances. This topic describes how to create an ApsaraDB for Redis instance that meets your business requirements.

Prerequisites

- An Alibaba Cloud account is created. For more information, see Sign up with Alibaba Cloud.

- If you want to create a pay-as-you-go instance, make sure that you have sufficient balance within your account.

Select a series type and specifications

Before you create an ApsaraDB for Redis instance, you must select a series type and specifications based on various factors, such as performance, price, and workload. For more information, see Select ApsaraDB for Redis instances.

选择Redis系列与规格

在创建Redis实例前，你需要结合性能、价格、工作负载等因素进行选型。

- Redis实例选型最佳实践

Create an ApsaraDB for Redis Community Edition instance or a performance-enhanced instance of ApsaraDB for Redis Enhanced Edition (Tair)

1. Log on to the ApsaraDB for Redis console.

2. In the left-side navigation pane, click Instances. In the upper-right corner of the page, click **Create Instance**.

3. On the buy page, select a product type.

   Select a product type that uses local disks

Product Type	Subscription (Local Disk, Including Tair)	Pay-as-you-go (Local Disk, Including Tair)	Tair (Subscription)

   - **Subscription (Local Disk, Including Tair)**: You are charged when you create the subscription instance that uses local disks. For long-term use, the subscription billing method is more cost-effective than the pay-as-you-go billing method. Longer subscription periods help you reduce costs.

   - **Pay-as-you-go (Local Disk, Including Tair)**: You are charged on an hourly basis for using the pay-as-you-go instance. For short-term use, we recommend that you select the pay-as-you-go billing method. If you no longer need a pay-as-you-go instance, you can release the instance to reduce costs.

4. Configure the instance parameters. The following table describes the parameters.

Parameter	Description
Region and Zone	The region in which you want to create the instance. You cannot change the region after the instance is created. ○ To maximize access speed, we recommend that you select a region that is close to the geographic location of your users. ○ To enable connections over the internal network, make sure that the ApsaraDB for Redis instance is deployed in the same region as Elastic Compute Service (ECS) instances that need to access the ApsaraDB for Redis instance. Otherwise, these ECS instances can access the ApsaraDB for Redis instance only over the Internet. This prevents the ApsaraDB for Redis instance from delivering its full performance.
Zone	The zone in which you want to create the instance. Each region has multiple isolated locations known as zones. Each zone has its own independent power supply and network. All of the zones in a region provide the same level of service performance. Compared with the access to an ApsaraDB for Redis instance that is deployed in a different zone from specific ECS instances, these ECS instances can access an ApsaraDB for Redis instance that is deployed in the same zone as these instances at a slightly lower latency. ⊘ Note To implement zone-disaster recovery, you can deploy the ApsaraDB for Redis instance across multiple zones in the same region.
Network Type	The network type of the instance. This parameter can be set only to **VPC**. A virtual private cloud (VPC) is an isolated network that provides higher security and better performance than the traditional classic network. ◁) Notice Make sure that the ApsaraDB for Redis instance is connected to the same VPC as the ECS instances or ApsaraDB RDS instances that need to access the ApsaraDB for Redis instance. Otherwise, the ECS instances or ApsaraDB RDS instances cannot access the ApsaraDB for Redis instance over the internal network.
VPC	The VPC in which you want to create the instance. If you do not have a VPC, create one first. For more information, see Create and manage a VPC.
VSwitch	The vSwitch to be used by the instance in the VPC. If no vSwitches are available in the VPC in the current zone, create a vSwitch. For more information, see Work with vSwitches.
Edition	○ **Community Edition**: This edition is compatible with the open source Redis protocol and provides high performance. ○ **Enhanced Edition (Tair)**: This edition is developed based on ApsaraDB for Redis Community Edition. This edition is optimized in terms of performance, storage, and data structures. For more information, see Overview.

Parameter	Description
Series	The series type of the instance. The **Enhanced Performance** series type uses the multi-threading model. This parameter is available only if the **Edition** parameter is set to **Enhanced Edition (Tair)**. The performance of a performance-enhanced instance of Enhanced Edition (Tair) is three times that of a Community Edition instance with the same specifications. This series also provides multiple data structure modules to simplify development. For more information, see Performance-enhanced instances. ⑦ **Note** Hybrid-storage instances are phrased out. For more information, see Sales of ApsaraDB for Redis hybrid-storage instances are discontinued.
Version	The database engine version of the instance. We recommend that you select a new engine version to experience more features.
Architecture Type	○ **Cluster**: eliminates the performance bottleneck that is caused by the single-threading model. You can use the high-performance cluster instance to process large-capacity workloads. ○ **Standard**: runs in a master-replica architecture, provides high-performance caching services, and ensures high data reliability. ○ **Read-Write Splitting**: ensures high availability (HA) and high performance and supports multiple specifications. The read/write splitting architecture allows a large number of concurrent reads of hot data from read replicas. This reduces the loads on the master node and minimizes O&M costs. For more information, see Overview.
Shards	The number of shards for the cluster instance. Data is distributed across the shards in the cluster instance. ⑦ **Note** This parameter is supported only if the **Architecture Type** parameter is set to **Cluster**.
Node Type	○ The node type of the instance. If you set the **Architecture Type** parameter to **Cluster** or **Standard**, this parameter can be set only to **Master-Replica**. ○ If you set the **Architecture Type** parameter to **Read-Write Splitting**, you can select the node type based on the number of read replicas.
Instance Type	The specifications of the instance. Each option contains a group of configurations, such as the memory capacity, maximum number of concurrent connections, and maximum bandwidth. For more information, see Overview. ⑦ **Note** The database metadata is generated after you create an ApsaraDB for Redis instance. The size of the metadata on each shard of a cluster instance ranges from 30 MB to 50 MB. The total size of the metadata for a cluster instance equals the total size of metadata on all shards of the cluster instance.

Parameter	Description

Password Setting	○ **Later**: Specify a password after the instance is created. For more information, see Change or reset the password.
	
	○ **Now**: Specify a password for the instance.
	
	  ■ The password must be 8 to 32 characters in length.
	
	  ■ The password must contain at least three of the following character types: uppercase letters, lowercase letters, digits, and special characters.
	
	  ■ Special characters include `! @ # $ % ^ & * ( ) _ + - =`

Bandwidth Auto Scaling	You can choose whether to enable **Bandwidth Auto Scaling** for the instance. If this feature is enabled, bandwidth can be automatically increased or decreased after the bandwidth usage exceeds the specified threshold. This helps you handle expected and unexpected traffic peaks. For more information, see Enable bandwidth auto scaling.
Instance Name	The name of the instance, which is used to identify and manage the instance.
Quantity	The number of instances that you want to create. The instances have the same specifications. You can create up to 99 instances.
Duration	If you select the **Subscription (Local Disk, Including Tair)** product type, you must specify the duration and select whether to enable auto-renewal.
Resource Group	The resource group to which the instance belongs. For more information, see What is Resource Management?

5. Click **Buy Now**.

6. On the **Confirm Order** page, read and accept the ApsaraDB for Redis Agreement of Service and follow the instructions to pay for the instance.
   After your payment is complete, wait for 1 to 5 minutes. To view the created instance, you can select the region where the instance resides on the Instances page of the ApsaraDB for Redis console.

Create a persistent memory-optimized or storage-optimized instance of ApsaraDB for Redis Enhanced Edition (Tair)

1. Log on to the ApsaraDB for Redis console.

2. In the left-side navigation pane, click Instances. In the upper-right corner of the page, click **Create Instance**.

3. On the buy page, set the Product Type parameter to **Tair Subscription**.

Product Type	Subscription (Local Disk, Including Tair)	Pay-as-you-go (Local Disk, Including Tair)	Tair (Subscription)

⑦ **Note**   Only the subscription billing method is supported. In this billing method, you are charged when you create the instance.

4. Configure the instance parameters. The following table describes the parameters.

Parameter	Description
Types	○ **Tair Persistent Memory**: allows users to store and query data in persistent memory. This instance type provides command-level persistence capabilities. It is suitable for scenarios that require high performance and data consistency. For more information, see Persistent memory-optimized instances. ○ **Tair Massive Storage**: allows users to store and query data in enhanced solid-state disks (ESSDs). This instance type provides command-level persistence capabilities and large storage capacities. It is suitable for scenarios that require moderate performance and low costs. For more information, see Storage-optimized instances.
Districts and Regions	The region in which you want to create the instance. You cannot change the region after the instance is created. ○ To maximize access speed, we recommend that you select a region that is close to the geographic location of your users. ○ To enable connections over the internal network, make sure that the ApsaraDB for Redis instance is deployed in the same region as Elastic Compute Service (ECS) instances that need to access the ApsaraDB for Redis instance. Otherwise, these ECS instances can access the ApsaraDB for Redis instance only over the Internet. This prevents the ApsaraDB for Redis instance from delivering its full performance. ○
Primary Zone	The zone in which you want to create the instance. Each region has multiple isolated locations that are known as zones. Each zone has its own independent power supply and network. To minimize the network latency between an ECS instance and an ApsaraDB for Redis instance that are deployed in the same zone, connect them over the internal network. ⑦ **Note** To implement zone-disaster recovery, you can deploy the ApsaraDB for Redis instance across multiple zones in the same region.
Network Type	The network type of the instance. This parameter can be set only to **VPC**. A VPC is an isolated network that provides higher security and better performance than the traditional classic network. 🔊 **Notice** Make sure that the ApsaraDB for Redis instance is connected to the same VPC as the ECS instances or ApsaraDB RDS instances that need to access the ApsaraDB for Redis instance. Otherwise, the ECS instances or ApsaraDB RDS instances cannot access the ApsaraDB for Redis instance over the internal network.
VPC	The VPC in which you want to create the instance. If you do not have a VPC, create one first. For more information, see Create and manage a VPC.

Parameter	Description
vSwitch	The vSwitch to be used by the instance in the VPC. If no vSwitches are created in the VPC in the current zone, create a vSwitch. For more information, see Work with vSwitches.
Architecture	○ Standalone: uses the master-replica architecture. For more information, see Standard master-replica instances. ○ Cluster: uses the sharded cluster architecture. For more information, see 集群版-双副本. ⓘ Note Storage-optimized instances do not support the cluster architecture.
Shard Specification	The specifications of the instance. Each option contains a group of configurations, such as the memory capacity, maximum number of concurrent connections, and maximum bandwidth. For more information, see Persistent memory-optimized instances and Storage-optimized instances. ⓘ Note The database metadata is generated after you create an ApsaraDB for Redis instance. The size of the metadata on each shard of a cluster instance ranges from 30 MB to 50 MB. The total size of the metadata for a cluster instance equals the total size of metadata on all shards of the cluster instance.
Replicas	The number of replicas in the instance. This parameter can be set only to 2 and cannot be modified. Each shard has a master node and a replica node to ensure HA.
Storage Class	The storage type of the instance. This parameter can be set only to ESSD PL1 and cannot be modified. For more information about Alibaba Cloud ESSDs at the PL1 performance level, see ESSDs.
Storage Space	The storage capacity of the instance. If you set the Types parameter to Tair Massive Storage, you can select the storage capacity based on your business requirements. ⓘ Note You cannot modify this parameter for a persistent memory-optimized instance. In a persistent memory-optimized instance, ESSDs are used only to store system operating data, such as logs and backup data. ESSDs are not used as the media to read or write data.

Parameter	Description
Password Setting	○ **Later**: Specify a password after the instance is created. For more information, see Change or reset the password. ○ **Now**: Specify a password for the instance. ■ The password must be 8 to 32 characters in length. ■ The password must contain at least three of the following character types: uppercase letters, lowercase letters, digits, and special characters. ■ Special characters include `! @ # $ % ^ & * ( ) _ + - =` ○
Instance Name	The name of the instance, which is used to identify and manage the instance.
Subscription Duration	The subscription duration of the instance.
Resource Group	The resource group to which the instance belongs. For more information, see What is Resource Management?

5. Click **Buy Now**.

6. On the **Confirm Order** page, read and accept the ApsaraDB for Redis Agreement of Service and follow the instructions to pay for the instance.
   After your payment is complete, wait for 1 to 5 minutes. To view the created instance, you can select the region where the instance resides on the Instances page of the ApsaraDB for Redis console.

FAQ

- Q: How long does it take to create an instance?
  A: The time that is required to create an instance depends on the number of shards in the instance. A larger number of shards require more resources. As a result, it takes more time to allocate resources. For example, it takes 2 to 3 minutes to create a standard master-replica instance, 10 to 15 minutes to create a 128-shard cluster master-replica instance, and 20 to 40 minutes to create a 256-shard cluster master-replica instance.

  > ⑦ **Note**
  >
  > ○ A standard instance is regarded as a single-shard instance.
  >
  > ○ The master node of a read/write splitting instance is regarded as a shard that processes both read and write requests. Each read replica of a read/write splitting instance is regarded as a shard that processes only read requests.

- Q: Why am I unable to find the created instance?
  A: The following table describes the possible causes and solutions.

Possible cause	Solution
The region that you selected in the console is not the region in which the instance is deployed.	Log on to the ApsaraDB for Redis console and select the region in which the instance is deployed.
The instance list in the ApsaraDB for Redis console is not updated or is updated before the instance is created.	Wait for several minutes and then update the instance list to check whether the instance appears in the list.
Resources are insufficient.	The system may fail to create the instance due to insufficient resources. In this case, your payment is refunded. You can check your refund on the Orders page. After you confirm that the payment is refunded, you can try to create your instance in another zone. You can also submit a ticket.

- Q: Why am I unable to create an ApsaraDB for Redis standalone instance?
  A: Starting from December 19, 2019, standalone instances of ApsaraDB for Redis were phased out. For more information, see Deprecated standalone instances.

Related API operations

API	Description
CreateInstance	Creates an ApsaraDB for Redis instance.
CreateTairInstance	Creates a persistent memory-optimized or storage-optimized instance of ApsaraDB for Redis Enhanced Edition (Tair).

3.Step 2: Configure whitelists

By default, ApsaraDB for Redis instances block access from all IP addresses to ensure the security and stability of databases. Before you use an ApsaraDB for Redis instance, you must add IP addresses or CIDR blocks that are used to access the ApsaraDB for Redis instance to a whitelist of the instance. Whitelists can be used to improve the access security of ApsaraDB for Redis instances. We recommend that you maintain whitelists on a regular basis.
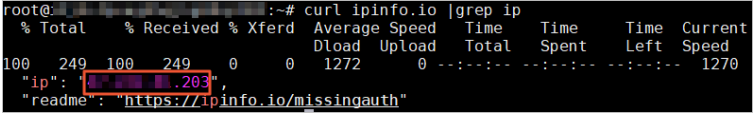
Prerequisites

The ApsaraDB for Redis instance is updated to the latest minor version. For more information, see Update the minor version.

> ⑦ **Note**   If the **Minor Version Update** button on the **Instance Information** page is dimmed, or if a message indicating that the current version is the latest version appears after you click this button, your instance is of the latest minor version.

Preparations

Before you configure a whitelist for an ApsaraDB for Redis instance, you must obtain the IP addresses of clients based on the client installation locations.

Client installation location	Network type	How to obtain the IP address of a client
Elastic Compute Service (ECS) instance (recommended)	VPC	Query the IP address of an ECS instance ⑦ **Note** • Make sure that the ECS instance and the ApsaraDB for Redis instance are deployed in the same VPC. The basic information pages of the instances must display the same VPC ID. If the instances are deployed in different VPCs, you can change the VPC to which the ECS instance belongs. For more information, see Change the VPC of an ECS instance. • The network types of the ECS instance and the ApsaraDB for Redis instance may be different. For example, the ECS instance belongs to the classic network and the ApsaraDB for Redis instance belongs to a VPC. For more information about how to connect to an ApsaraDB for Redis instance from an ECS instance when the instances are deployed in different types of networks, see Connect an ECS instance to an ApsaraDB for Redis instance in different types of networks.

Client installation location	Network type	How to obtain the IP address of a client

On-premises device or third-party cloud	Internet	Select one of the following methods based on the operating system of the on-premises device:
		
		• Linux operating system: Run the **curl ipinfo.io |grep ip** command on the on-premises device to obtain the public IP address. The following figure shows the sample result.
		
		``
		root@ :~# curl ipinfo.io |grep ip
		  % Total % Received % Xferd Average Speed Time Time Time Current
		                                 Dload Upload Total Spent Left Speed
		100 249 100 249 0 0 1272 0 --:--:-- --:--:-- --:--:-- 1270
		  "ip": " .203",
		  "readme": "https://ipinfo.io/missingauth"
		``
		
		• Windows operating system: Visit ipinfo to obtain the public IP address of the on-premises device.

Methods to configure a whitelist

Method	Description
Method 1: Manually add a whitelist	Manually add the IP address of a client to a whitelist of the ApsaraDB for Redis instance to allow the client to access the instance.
Method 2: Add ECS security groups as whitelists	A security group is a virtual firewall that is used to control the inbound and outbound traffic of ECS instances in the security group. For more information, see Overview. To authorize multiple ECS instances to access an ApsaraDB for Redis instance, you can associate the ApsaraDB for Redis instance with the security group of these ECS instances. This method is more convenient than manually adding the IP addresses of these ECS instances to a whitelist. ⑦ **Note** The engine version of the ApsaraDB for Redis instance must be Redis 4.0 or later. For more information about how to upgrade the engine version, see Upgrade the major version.

⑦ **Note** You can set IP address whitelists and specify ECS security groups as whitelists of an ApsaraDB for Redis instance. Both IP addresses in the IP address whitelists and ECS instances in the security groups are allowed to access the instance.
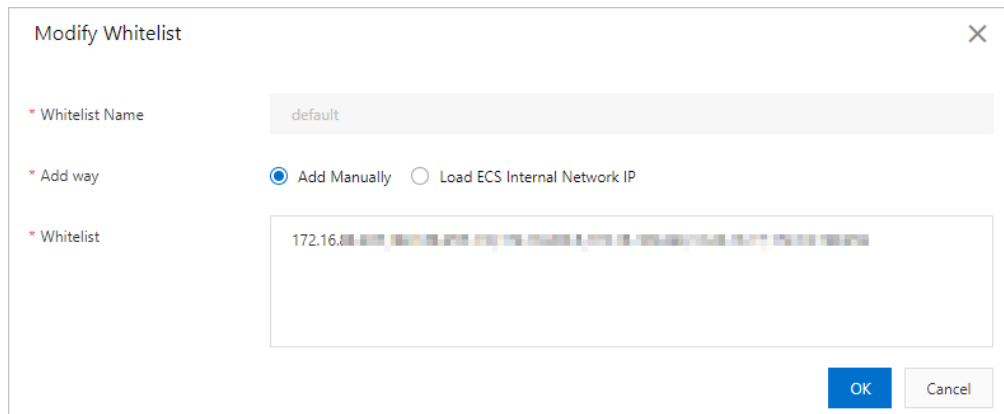
Method 1: Manually add a whitelist

1. Log on to the ApsaraDB for Redis console.

2. In the top navigation bar, select the region in which the instance is deployed.

3. On the **Instances** page, find the instance and click the instance ID.

4. In the left-side navigation pane, click **Whitelist Settings**.

5. Find the **default** security group and click **Modify**.

> ⑦ **Note**   You can also click **Add Whitelist** to create a whitelist. The name of a whitelist must be 2 to 32 characters in length and can contain lowercase letters, digits, and underscores (_). It must start with a lowercase letter and end with a lowercase letter or digit.

6. In the dialog box that appears, perform one of the following operations:

   ○ Manually add IP addresses or CIDR blocks to the whitelist

     Manually modify the whitelist

Modify Whitelist	×

     * Whitelist Name   default

     * Add way   ⦿ Add Manually   ◯ Load ECS Internal Network IP

     * Whitelist   172.16.████████████████████████████████████

     OK   Cancel

     > ⑦ Note
     >
     > ■ Separate multiple IP addresses with commas (,). A maximum of 1,000 unique IP addresses can be added. You can enter specific IP addresses such as 10.23.12.24 and CIDR blocks such as 10.23.12.24/24. /24 indicates the length of the IP address prefix. An IP address prefix can be 1 to 32 bits in length. For more information about CIDR blocks, see CIDR block FAQ.
     >
     > ■ If you enter CIDR blocks that have a prefix length of 0 such as 0.0.0.0/0 and 127.0.0.1/0, all IP addresses are allowed to access the instance. This poses a high security risk. Proceed with caution.

   ○ Add private IP addresses of ECS instances to the whitelist

     a. Click **Load ECS Internal Network IP**.
        The private IP addresses of ECS instances that are deployed in the same region as the ApsaraDB for Redis instance are displayed.

  b. Select IP addresses based on your business requirements.

    Select private IP addresses of ECS instances

> ⑦ **Note**　To find the ECS instance that is assigned a specific IP address, you can move the pointer over the IP address. Then, the system displays the ID and name of the ECS instance.

  ○ Remove all IP addresses from the whitelist

   To remove all IP addresses from the whitelist but retain the whitelist, click **Delete**.

7. Click **OK**.

Method 2: Add ECS security groups as whitelists

You can add ECS security groups as whitelists of the ApsaraDB for Redis instance. Then, the ECS instances in the security groups can access the ApsaraDB for Redis instance over an internal network or the Internet. The ApsaraDB for Redis instance must have a public endpoint if you want to access the ApsaraDB for Redis instance over the Internet. For more information, see Use a public endpoint to connect to an ApsaraDB for Redis instance.
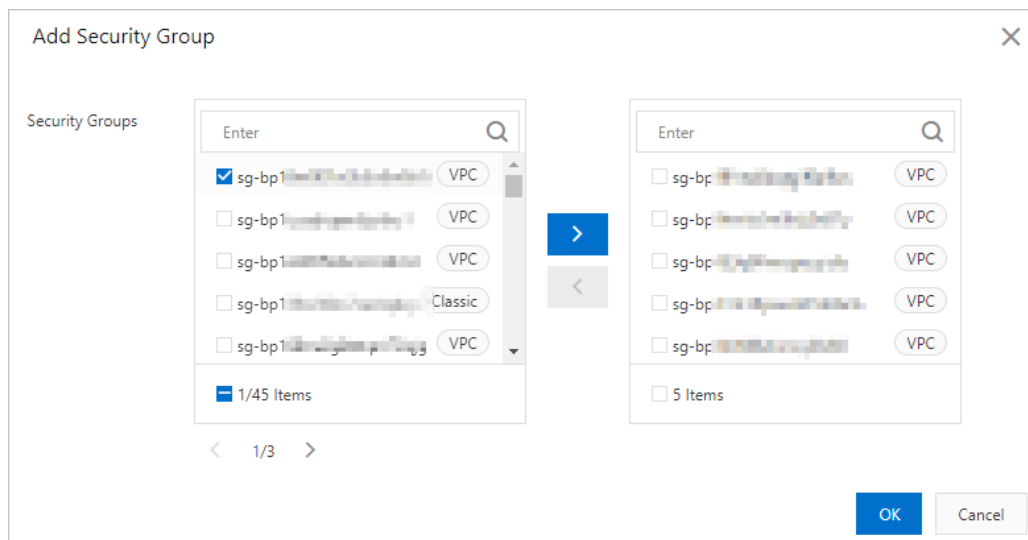
> ⑦ **Note**
>
> ● Before you add a security group as a whitelist, make sure that the network types of the ApsaraDB for Redis instance and the ECS instances in the security group are the same. If the network types of the ApsaraDB for Redis instance and ECS instances are VPC, make sure that they are deployed in the same VPC.
>
> ● You cannot add ECS security groups as whitelists for ApsaraDB for Redis instances deployed in the following regions: China (Heyuan), China (Guangzhou), China (Nanjing), and China (Ulanqab).

  (Optional)

1. Log on to the ApsaraDB for Redis console.

2. In the top navigation bar, select the region in which the instance is deployed.

3. On the **Instances** page, find the instance and click the instance ID.

4. In the left-side navigation pane, click **Whitelist Settings**.

5. Click **Security Groups**.

6. On the **Security Groups** tab, click **Add Security Group**.

7. In the dialog box that appears, select the security groups that you want to add as whitelists.

Select security groups

> ⑦ *Note*
>
> ○ To identify a security group, you can move the pointer over the ID of the security group.
> Then, the name and description of the security group are displayed. If you move the
> pointer over the VPC icon, you can view the ID of the VPC.
>
> ○ You can add up to 10 security groups as whitelists to each ApsaraDB for Redis instance.

8. In the message that appears, click **OK.**

9. (Optional)To remove all security groups, click **Delete.**

References

- Use a public endpoint to connect to an ApsaraDB for Redis instance
- Connect an ECS instance to an ApsaraDB for Redis instance in different types of networks

Related API operations

Operation	Description
DescribeSecurityIps	Queries the IP address whitelists of an ApsaraDB for Redis instance.
ModifySecurityIps	Modifies the IP address whitelists of an ApsaraDB for Redis instance.
DescribeSecurityGroupConfiguration	Queries the security groups that are added as whitelists to an ApsaraDB for Redis instance.

Operation	Description
ModifySecurityGroupConfiguration	Modifies the security groups that are added as whitelists to an ApsaraDB for Redis instance.

FAQ

- Q: Why are whitelists automatically created for an ApsaraDB for Redis instance? Can I delete these whitelists?

  A: After you create an ApsaraDB for Redis instance, a default whitelist is automatically created. After you perform specific operations on the instance, more whitelists are automatically created, as described in the following table.

Whitelist name	Source
default	The default whitelist that cannot be deleted.
ali_dms_group	This whitelist is automatically created by Data Management (DMS) when you log on to an ApsaraDB for Redis instance from DMS. For more information, see Use DMS. Do not delete or modify this whitelist. Otherwise, you may fail to log on to the ApsaraDB for Redis instance from DMS.
hdm_security_ips	This whitelist is automatically created by Database Autonomy Service (DAS) when you use CloudDBA-related features such as cache analysis. For more information, see Use the cache analysis feature to display details about big keys. Do not delete or modify this whitelist. Otherwise, the CloudDBA-related features may become unavailable.

- Q: A whitelist contains IP address 127.0.0.1 in addition to client IP addresses. In this case, can these clients connect to the ApsaraDB for Redis instance?

  A: These clients can connect to the ApsaraDB for Redis instance. If only 127.0.0.1 exists in the whitelist, all IP addresses are not allowed to connect to the ApsaraDB for Redis instance.

- Q: Why does the `(error) ERR illegal address` message appear after I use redis-cli to connect to an ApsaraDB for Redis instance?

  A: The IP address of the client where you run redis-cli is not added to a whitelist of the ApsaraDB for Redis instance. You must check the whitelists of the ApsaraDB for Redis instance.

- Q: If the IP address of my client is not added to a whitelist of an ApsaraDB for Redis instance, can I check port connectivity by running the telnet command?

  A: Yes. The following message is returned after you run the telnet command:

```
Escape character is '^]'.
Connection closed by foreign host.
```

4.Connect to an ApsaraDB for Redis instance

You can use a Redis client, Data Management (DMS), or the redis-cli tool to connect to an ApsaraDB for Redis instance.

Precautions

ApsaraDB for Redis can monitor the health status of nodes. If a master node in an instance becomes unavailable, ApsaraDB for Redis automatically triggers a master-replica switchover. The roles of master and replica nodes are switched over to ensure the high availability of the instance. Before a client is officially released, we recommend that you manually trigger the master-replica switchover. This can help you verify the error handling capabilities or disaster recovery logic of the client. For more information, see Manually switch workloads from a master node to a replica node.

Endpoint types

After an ApsaraDB for Redis instance is created, you can view the endpoint of the instance on the Instance Information page. By default, ApsaraDB for Redis provides an endpoint of the following network type: or If you want to connect to the ApsaraDB for Redis instance by using a direct connection endpoint or a public endpoint, you must apply for the corresponding endpoint. For more information about endpoints, see View endpoints. VPCclassic network

Endpoints

Connection Information	Endpoint	Port Number:	Account Management	Enable Password-free Access
Connection Type	Endpoint	Port Number:	Actions	
Direct Connection			Apply for Endpoint	
VPC Network	r-bp████ ██████.redis.rds.aliyuncs.com	6379	Modify Public Endpoint	
Public Access			Apply for Endpoint	

> ⓘ **Note** We recommend that you deploy your client on an ECS instance and use the client to connect the ECS instance to an ApsaraDB for Redis instance over a VPC. This way, you can improve security, reduce network latency, and avoid performance degradation caused by network latency. For more information, see What is ECS?

Common connection methods

Connection method	Description
Use DMS	You can use DMS to connect to ApsaraDB for Redis instances without the need to install a client. DMS allows you to manage ApsaraDB for Redis instances on a visual interface.

Connection method	Description
Use a client to connect to ApsaraDB for Redis	ApsaraDB for Redis is compatible with open source Redis. You can connect to ApsaraDB for Redis and open source Redis in a similar manner. Therefore, you can use a client that is compatible with the Redis protocol to connect to ApsaraDB for Redis. ⑦ **Note** You can also enable the SSL encryption feature to enhance the security of data links and ensure data integrity. For more information, see Connect to an ApsaraDB for Redis instance that has SSL encryption enabled by using a client.
Use redis-cli to connect to an ApsaraDB for Redis instance	The redis-cli tool is a CLI of open source Redis. You can use redis-cli to connect to an ApsaraDB for Redis instance from an ECS instance or your device. Then, you can manage data.

Special connection methods

Connection method	Description
Use a public endpoint to connect to an ApsaraDB for Redis instance	If you want to test or manage an ApsaraDB for Redis instance that is deployed on your device, you can apply for a public endpoint for the instance and connect to the instance over the public endpoint by using your device.
Use a private endpoint to connect to an ApsaraDB for Redis instance	You can apply for a direct connection endpoint for a cluster master-replica instance. You can use the endpoint to connect to backend data shards in the instance in the similar manner as you would connect to an open source Redis cluster. For more information, see Cluster master-replica instances. Compared with the direct connection mode reduces the response time of ApsaraDB for Redis because requests do not need to pass through proxy servers. For more information about how to enable the direct connection mode, see Enable the direct connection mode. the proxy mode
Use the Sentinel-compatible mode to connect to ApsaraDB for Redis instances	ApsaraDB for Redis provides the Sentinel-compatible mode. If you enable this mode, clients can connect to ApsaraDB for Redis instances in the same way as they connect to native Redis Sentinel.

FAQ

- Connect an ECS instance to an ApsaraDB for Redis instance in different types of networks
- Troubleshooting for connection issues in ApsaraDB for Redis

5.Manage ApsaraDB for Redis instances

You can manage ApsaraDB for Redis instances in a convenient manner by using the ApsaraDB for Redis console, API operations, or SDKs.

Understand the limits, development standards, and O&M standards

使用限制

了解云数据库Redis中，各数据类型和功能特性的相关使用限制。

- 使用限制

开发运维规范

介绍业务部署、Key设计、SDK、命令、运维管理等规范，帮助您充分发挥Redis的能力。

- 云数据库Redis开发运维规范

Limits

The limits on different data types and features that are supported by ApsaraDB for Redis.

- Limits

Development and O&M standards

The development and O&M standards, such as standards for business deployment, key design, SDK usage, command usage, and O&M management. These standards help you make full use of ApsaraDB for Redis.

- Development and O&M standards for ApsaraDB for Redis

Management methods

Management method	Description
ApsaraDB for Redis console	The ApsaraDB for Redis console is a web application that is used to manage ApsaraDB for Redis instances. It provides various O&M and management features to help you manage instances in a convenient and visualized manner.

Management method	Description
API operations and SDKs	• O&M engineers: ApsaraDB for Redis provides a wide range of API operations for you to manage ApsaraDB for Redis instances. For example, you can call the CreateInstance operation to create an instance. You can also call the API operations of different Alibaba Cloud services to implement complex custom features. • Business developers: You can use SDKs that are integrated in clients to run database commands to manage data in ApsaraDB for Redis instances. For example, you can run the **SET** command to set the value of a key. For more information, see Quick start.

Operations in the ApsaraDB for Redis console

Click a tab to show the details. Click that tab again to hide the details.

数据迁移与同步 ❯
管理计划内运维事件 ❯
管理Redis实例 ❯
账号与安全 ❯
连接实例与操作数据 ❯
性能与监控 ❯
审计与日志 ❯
备份与恢复 ❯
性能调优与问题排查 ❯

Data migration and synchronization ❯
Scheduled O&M event management ❯
Manage ApsaraDB for Redis instances ❯
Account and security management ❯
Instance connection and data management ❯
Performance monitoring ❯
Audit logs ❯
Backup and restoration ❯
Troubleshooting ❯