ALIBABA CLOUD

Alibaba Cloud

Virtual Private Cloud

Best practices

Document Version: 20201123

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.Grant services access to a private network

A virtual private cloud (VPC) is dedicated to you on Alibaba Cloud. Alibaba Cloud provides various products and services that can be deployed in a VPC, such as Express Connect, VPN Gateway, Cloud Enterprise Network (CEN), and Smart Access Gateway (SAG).

The following table describes the different solutions to connect Alibaba Cloud services to a VPC.

Establish connections between VPCs			
Service	**Solution**	**Benefit**	**Limit**
CEN	Establishes connections between VPCs in different regions or under different accounts.	• Enables simple configurations and support automatic route learning and distribution. • Supports low latency and efficient transmission. • Allows instances such as VPCs and VBRs that are attached to the same CEN instance to communicate with each other. • Supports free communication between instances that are deployed in the same region.	-
What is Express Connect?	Supports peering connections between VPCs.	Supports free connections between VPCs in the same region.	-
Connect a VPC to an on-premises data center			
Service	**Scenario**	**Benefit**	**Limit**
VPN Gateway	Connects an on-premises data center to a VPC through an Internet-based and encrypted IPsec-VPN tunnel.	• Minimizes the costs. • Ensures secure connections. • Immediately applies the latest configurations.	Serves your workloads with the network latency and availability that depends on the conditions of the Internet.

CEN	Enables communication among resources that are attached to the same CEN instance. The communication is implemented based on automatic route learning and distribution.	• Enables simple configurations and support automatic route learning and distribution. • Low latency and high speed. • The network instances (VPCs/VBRs) that are attached to the same CEN instance are all connected with each other. • Connecting networks in the same region is free of charge.	-
SAG	Connects an on-premises data center to Alibaba Cloud.	• Supports the out-of-the-box feature to ensure automatic configuration. • Builds a secure hybrid cloud. Data transmission among VPCs and over the Internet is encrypted. • Connects to nearby access points in a metropolitan area network. On-premises networks can be connected to Alibaba Cloud through primary and secondary connections or devices.	-
Express Connect	Connects an on-premises data center and a VPC by using the physical connections of Express Connect.	• Ensures optimal network quality. • Provides a high bandwidth.	• Requires high initial setup costs. • The service activation takes a long time.

VPN software in the Alibaba Cloud Marketplace	Allows you to purchase a VPN gateway in the Alibaba Cloud Marketplace and deploy the VPN gateway in the VPC. You can connect an on-premises data center to the VPC through an Internet-based and encrypted IPsec-VPN tunnel.	• Ensures secure connections. • Supports multiple types of VPN software to meet your business requirements. • Configurations take effect immediately.	• Requires manual deployment and maintenance of the VPN gateway. • The network latency and availability is dependent on the quality of the Internet connection.
Connect multiple sites			
Service	**Scenario**	**Benefit**	**Limit**
VPN Gateway	Establishes secure communication among multiple sites by using the VPN gateway. Supports the VPN-Hub feature to enable communication among sites and between sites and VPCs.	• Low cost. • Zero touch provisioning (ZTP), and configurations immediately take effect.	None
SAG + Express Connect	Allows you to purchase and configure SAGs for local branches. Then, you can add the SAGs to a cloud connect network (CCN).	• Supports the out-of-the-box feature to ensure automatic configuration. • Enables encrypted connections over a private network between local branches and Alibaba Cloud. Encryption and authentication are required for transmission over the Internet. • Access to nearby access points in a metropolitan area network is supported. On-premises networks can be connected to Alibaba Cloud by using primary and secondary connections and devices.	None

VPN Gateway	Allows you to run interconnected applications and offices worldwide by using VPN Gateway and Express Connect.	• High network quality. • Zero touch provisioning (ZTP), and configurations immediately take effect.	The network latency and availability is dependent on the quality of the Internet connection.
Remote access to a VPC			
Service	**Scenario**	**Benefit**	**Limit**
VPN Gateway (SSL-VPN)	Uses the SSL-VPN feature to access a VPC from a remote client.	• Low cost. • Reliable. • Enables simple configuration and deployment.	-
SSL-VPN software in the Alibaba Cloud Marketplace	After you purchase SSL-VPN software from the Alibaba Cloud Marketplace, you can deploy it in a VPC. You can access the VPN server from a remote client.	Supports multiple types of SSL-VPN software and images.	• High cost. • Low reliability. • Requires manual deployment and maintenance of the SSL-VPN software.

Connect VPCs

You can run applications within the same VPC that are deployed in multiple regions. This enables access to the applications from the locations closest to users. This also minimizes the network latency and ensures high reliability based on redundant connections.

You can use CEN and VPN Gateway to connect VPCs in the same region or in different regions.

- CEN

  CEN can be used to establish internal connections and connect resources within multiple VPCs based on automatic route distribution and learning. This allows you to accelerate network convergence and improve the quality and security of cross-network communication.

- VPN Gateway

  VPN Gateway is an Internet-based service that ensures secure and reliable connections among enterprise data centers, corporate networks, or Internet clients with a VPC through encrypted tunnels over the Internet. The hot-standby architecture of VPN Gateway ensures automatic failovers within a few seconds. You can use a VPN gateway to establish IPsec-VPN connections between your on-premises data centers and VPCs.

Connect a VPC to an on-premises data center

You can connect a VPC to an on-premises data center to build a hybrid cloud. You can establish secure and reliable connections between the VPC and the on-premises data center. This allows you to integrate the computing, storage, network, CDN and BGP resources of Alibaba Cloud with your IT infrastructure and support the scaling of workloads.

You can connect an on-premises data center to a VPC by using Express Connect, VPN Gateway, or CEN.

- Express Connect

  Express Connect supports connections through leased lines. After a leased line has accessed an Alibaba cloud access point, you can create a VBR to connect your on-premises data center with Alibaba Cloud. This way, you can build a hybrid cloud to enable connections over a private network, instead of the Internet.

  Physical connections of Express Connect support communication over private networks, instead of the Internet. This optimizes user experience in terms of security, reliability, transmission rate, and latency.

- VPN gateways

  VPN Gateway is an Internet-based service that securely and reliably connects enterprise data centers, corporate networks, or Internet clients with an Alibaba Cloud VPC through encrypted tunnels over the Internet. The hot-standby architecture of VPN Gateway ensures automatic failovers within a few seconds. You can use VPN Gateway to establish IPsec-VPN connections between your on-premises data centers and VPCs.

- CEN

  CEN can be used to establish internal connections and connect resources within multiple VPCs based on automatic route distribution and learning. After you attach the VBR that is associated with an on-premises data center to a CEN instance, the on-premises data center can communicate with all cloud resources that are attached to the same CEN instance based on VPCs or VBRs.

- SAG

  Smart Access Gateway provides an end-to-end cloud deployment solution. SAG allows enterprises to connect to the nearest access points of VPC through encrypted connections over the Internet. SAG provides more intelligent, reliable, and secure connections to the cloud.

  You can buy SAG devices for the on-premises data center, and attach the CCN instance that is associated with the devices to the CEN instance. This allows you to connect the on-premises data center to Alibaba Cloud.

- VPN software in the Alibaba Cloud Marketplace

  The Alibaba Cloud Marketplace provides various types of VPN software and images. You can purchase the required VPN software from the Alibaba Cloud Marketplace and deploy it on your ECS instance. Then you can use an elastic IP address (EIP) to connect the VPC to the gateway of your on-premises data center through the Internet.

Connect multiple sites

You can connect multiple sites by using SAG or the VPN-Hub feature of VPN Gateway.

- SAG

SAG is an all-in-one solution for connecting your workloads to Alibaba Cloud. SAG allows enterprises to connect to the nearest access points of VPCs through encrypted connections over the Internet. SAG supports more intelligent, reliable, and secure connections to the cloud.

You can purchase SAG devices for local branches, and attach the CCN instance associated with the devices to the CEN instance. This allows you to connect the local branches.

- VPN Gateway

  The IPSec-VPN feature of VPN Gateway provides site-to-site VPN connection. Each VPN Gateway supports up to10 IPsec-VPN connections. You can purchase a VPN gateway to establish connections among up to 10 on-premises data centers or branches in different regions.

  You can create multiple site-to-site IPsec connections among sites, or between sites and VPCs by using VPN-Hub. VPN-Hub allows large enterprises to establish internal connections across offices that run business in different regions.

  By default, the VPN-Hub function is enabled. You must configure the IPsec-VPN connection between each office site and Alibaba Cloud. No additional configurations or payments are required. A VPN gateway supports up to 10 IPsec connections. You can connect 10 office sites in different areas by using one VPN gateway. The following figure shows how to establish connections among the offices in Shanghai, Hangzhou, and Ningbo by using a VPN gateway.

- Build a high-speed global network

  You can run applications and offices worldwide by using VPN Gateway and Express Connect. This ensures secure transmission and optimal network quality, and minimizes the costs of your business.

  The following figure shows how to establish connections among the offices that are connected to the VPC in the US (Virginia) region and the VPC in the China (Shanghai) region. You can run applications in both VPCs, connect the VPCs by using Express Connect, and connect the offices to each VPC by using IPsec-VPN.

Remote access to a VPC

The SSL-VPN feature of VPN Gateway provides point-to-site VPN connection. You can use a client to access a VPC without the need to configure a gateway. You can deploy internal applications in a VPC and enable access to the applications through SSL-VPN connections over internal networks. For example, network maintenance and management can be implemented through the connections between an office and the VPC. Remote access is allowed for the applications in the VPC.

Both VPN Gateway or VPN software or images from the Alibaba Cloud Marketplace can be used to achieve remote access to the VPC.

- VPN Gateway (SSL-VPN)

  You can create an SSL-VPN connection to connect a remote client to applications and services that are deployed in a VPC. After you deploy your applications or services, you must import the certificate to the client to initiate a connection. The hot-standby architecture of SSL-VPN server ensures automatic failovers within a few seconds.

- Purchase SSL-VPN software in Alibaba Cloud Marketplace

  The Alibaba Cloud Marketplace provides various types of SSL-VPN software and images. You can purchase the required SSL-VPN software from the Alibaba Cloud Marketplace and deploy it on your ECS instance. Then you can use an EIP to connect the VPC to a client over the Internet.

2.Select a product to gain access to the Internet

In the VPC network, you can use an Elastic IP Address (EIP), a NAT Gateway, an Internet Server Load Balancer (SLB) instance, or the public IP address of an ECS instance to access the Internet.

Public IP address

In Alibaba Cloud, there are various types of public IP addresses, such as the public IP address of an ECS instance, the public IP address of a NAT bandwidth package, the public IP address of an Internet SLB instance, and the public IP address of a VPN Gateway. To facilitate the management of public IP addresses, ECS instances of the VPC network, NAT Gateways, and intranet SLB instances can all be associated with EIPs.

You can add EIPs to an Internet Shared Bandwidth instance or a Data Transfer Plan to flexibly cope with traffic and bandwidth fluctuations and reduce the Internet cost.

Products with access to the Internet

The following table lists the features of Alibaba Cloud products that have access to the Internet.

Apart from the following products, Alibaba Cloud provides Internet Shared Bandwidth and Data Transfer Plan for VPCs to help you reduce the cost of Internet bandwidth and traffic. You can select a suitable product based on your service needs to reduce costs.

Service	Feature	Benefit
ECS public IP address	When you create an Elastic Compute Service (ECS) instance in a VPC network, you can allow the system to automatically assign a public IP address to the ECS instance. Then, the ECS instance can use the public IP address to communicate with the Internet. You cannot unbind a public IP address from an ECS instance when the ECS instance is running. However, you can convert the public IP address to an elastic IP address (EIP). For more information, see Convert an automatically assigned public IP address to an EIP for a VPC-connected ECS instance.	You can purchase data transfer plans for an ECS instance that is assigned public IP addresses. You can also purchase EIP bandwidth plans for an ECS instance after you convert the public IP address of the ECS instance to an EIP. For more information, see What is EIP bandwidth plan and What is a data transfer plan.
Elastic IP Address	EIPs can be associated with or disassociated from ECS instances anytime. ECS instances can use EIPs to communicate with the Internet based on Source Network Address Translation (SNAT) and Destination Network Address Translation (DNAT).	EIPs can be associated with or disassociated from ECS instances anytime. You can use EIP bandwidth plans and data transfer plans to reduce the costs of data transfer over the Internet.

Service	Feature	Benefit
NAT Gateway	You can create SNAT and DNAT entries on a NAT gateway to enable one or more ECS instances in a VPC network to communicate with the Internet. **Note** Unlike Server Load Balancer (SLB), NAT gateways are incapable of balancing the load of ECS instances.	A NAT gateway can provide Internet access for more than one ECS instance while an EIP can serve only one ECS instance.
Server Load Balancer	Server Load Balancer (SLB) is a port-based service that provides Layer-4 and Layer-7 load balancing. ECS instances that are connected to SLB can be accessed over the Internet. **Note** SLB does not support SNAT. ECS instances deployed in VPC networks cannot access the Internet through SLB.	SLB supports DNAT. Each port on an SLB instance can be mapped to one or more ECS instances. SLB distributes traffic to ECS instances to balance the load of the ECS instances. This improves the availability of application systems and eliminates single points of failure. After you associate an EIP with an SLB instance, you can purchase EIP bandwidth plans and data transfer plans to reduce costs.

Scenario 1: Provide external services

- Provide external services by using a single ECS instance

  If you have only one application with relatively low traffic, a single ECS instance can meet your requirements. You can deploy applications, databases, and files on this ECS instance. Then, associate an EIP to the ECS instance. In this way, users can access your application through the Internet.

- Provide external services by using the Layer-4 load balancing function

  If the traffic is high and one ECS instance cannot handle all access traffic, you can configure multiple ECS instances and a simple load balancing function. Specifically, you can create an Internet SLB instance with a Layer-4 listener and add the ECS instances as backend servers.

- Provide external services by using the Layer-7 load balancing function

  If you want to distribute different requests to different backend servers, you can add domain name-based or URL-based forwarding rules to a Layer-7 listener. Specifically, you can create an Internet SLB instance with a Layer-7 listener and add the ECS instances as backend servers.

Scenario 2: Internet access of an ECS instance without a public IP address

- Associate an EIP

If the number of ECS instances is relatively small, you can associate an EIP with each ECS instance. The ECS instance then can access the Internet by using the EIP. You can also disassociate the EIP from the ECS instance when Internet access is no longer needed.

- Use NAT Gateway and configure SNAT entries

  If the number of ECS instances is large, associating an EIP with each ECS instance incurs high costs. Also, users accessing ECS instances through the EIPs poses some risks. In this case, we recommend that you configure an SNAT entry for the ECS instances, but do not configure any DNAT entries. In this way, the ECS instances can access the Internet, but users cannot access these ECS instances over the Internet, as shown in the following figure.

3.Reduce the costs of data transfer over the Internet

how to save the costs of data transfer over the Internet by using data transfer plans and EIP bandwidth plans.

Data transfer plan

A data transfer plan supports the billing of data transfer over the Internet on a subscription basis. The plan offers a price lower than that of the pay-as-you-go billing method and provides off-peak data plans. This reduces the costs of data transfer over the Internet. Each data transfer plan applies to Elastic Cloud Service (ECS) instances, elastic IP addresses (EIPs), and Server Load Balancer (SLB) instances that are billed by data transfer.

Data transfer plans are easy to use. After you activate a data transfer plan, fees are automatically deducted from your resource plan. You can view the usage of data transfer plan on the Billing Management page.

The following section describes the benefits of data transfer plans:

- Minimizes the costs of data transfers

  Data transfer plans reduces the prices of data transfers at off-peak hours. The China (Hong Kong) region is used as an example. The costs of data transfers are compared among the scenarios when the pay-as-you-go billing method, full-time data transfer plan, and off-peak data transfer plan are used.

  Assume that your cloud resources consume a total of 5 TB traffic in the China (Hong Kong) region. The costs of the preceding scenarios are compared in the following table.

Billing solution of 5 TB of data transferred in the China (Hong Kong) region	Unit price (CNY/GB)	Total price (CNY)	Reduced cost (CNY)	Reduce cost by
Pay-as-you-go billing method	1	5120	0	0
Full-time data transfer plan	0.75	3727	1393	27.2%
off-peak data transfer plan	0.51	2609	2511	49%

- Supports multiple scenarios

  All ECS instances, EIPs, and SLB instances that are billed by data transfer support data transfer plans. Data transfer plans allow you to minimize the costs when a large amount of data is transferred.

- Easy to use

- Each plan has a validity period. After a plan expires, the remaining data usage quota is unavailable. We recommend that you choose a plan the provides the necessary data usage quota based on the data usage history of your workloads. You can first purchase a plan with the lowest required data usage quota. You can raise the quota in the future to support your business requirements.
- After the resources of the data transfer plan are exhausted, the system applies the pay-as-you-go billing method. This ensures continuous service of your workloads.
- If you have purchased multiple data transfer plans, data allowance in the plan that expires first is used in priority.

EIP bandwidth plan

EIP Bandwidth Plan is an independent bandwidth service. It provides high-quality multi-line BGP bandwidth and supports multiple billing methods. This allows these EIPs to share the bandwidth that is supported by the EIP bandwidth plan You can associate the EIPs with ECS instances, NAT gateways, or SLB instances in a VPC. Therefore, these services can share the bandwidth of EIP bandwidth plan.

EIP Bandwidth Plan supports multiple metering methods, such as pay-by-95th-percentile and pay-by-bandwidth. The EIP bandwidth plans with different metering methods allow you to minimize the bandwidth costs and optimize auto scaling of your workloads.

> **Note** By default, each EIP bandwidth plan is provided without a public IP address. You can add EIPs to an EIP bandwidth plan.

You can use an EIP bandwidth plan to share the bandwidth that is included in the plan. This allows you to minimize the bandwidth costs. This applies if traffic spikes may occur. For example, you have deployed 10 ECS instances in the China (Hong Kong) region. EIPs are associated with these ECS instances. You can use the pay-by-bandwidth metering method for the resources and set the maximum bandwidth to 100 Mbit/s. For these 10 EIPs with the peak bandwidth of 100 Mbit/s, you must pay CNY 3,253 per day.

However, traffic analysis of the 10 EIPs shows that the bandwidth for each of the ECS instances fluctuates at different points in time. The peak outbound bandwidth of the 10 ECS instances is about 500 Mbit/s, as shown in the following figure.

In this case, you can use EIP Bandwidth Plan. You can purchase an EIP bandwidth plan that supports the maximum bandwidth of 500 Mbit/s. These ECS instances can share the bandwidth. In this way, each ECS instance can use a peak bandwidth five times that of the 100 Mbit/s EIP, and you pay only CNY 1,680 per day for the 500 Mbit/s EIP bandwidth plan. Therefore, the daily bandwidth cost is reduced by 50%. This amounts to CNY 1,573.

EIP Bandwidth Plan also provides 95th percentile bandwidth billing with unlimited peak bandwidth. This billing method minimizes the bandwidth costs, and avoids the impact of maximum bandwidth on your workloads. If your bandwidth fluctuates, it is difficult to estimate a suitable peak bandwidth. A high peak bandwidth may cause the waste of bandwidth resources. A low peak bandwidth may cause packet loss. This may affect service development and user experience. In this case, 95th percentile bandwidth billing is an optimal solution.

Therefore, if your workloads have multiple EIPs and experience obvious bandwidth fluctuations, an EIP bandwidth plan can help you save costs. If traffic spikes often occur in your workloads, you can use the 95th percentile bandwidth billing method. This avoids the impact of the maximum bandwidth on your workloads. This also minimizes the waste of bandwidth resources that is caused by a high maximum bandwidth.

Note We recommend that you analyze the traffic model of your service and select an appropriate billing method:

- If your workloads process stable network traffic, you can choose the subscription billing method. This can help you save 20% to 30% costs compared with the pay-as-you-go billing method.
- If traffic spikes often occur in your workloads, you can choose the 95th percentile billing method.

4.How to use cloud products in a VPC?

This topic provides an overview of how to use cloud products in the Virtual Private Cloud (VPC) network. Most cloud products support the VPC network. You can select the VPC network when creating cloud resources, or create a VPC first and then create cloud resources in the VPC.

How to use VPC?

VPC is an isolated private network. By default, different VPCs cannot communicate with one another through intranet. Elastic Compute Service (ECS) instances in a VPC cannot access the Internet or be accessed by the Internet, and cannot access the classic network through intranet. However, Alibaba Cloud provides a range of connectivity options to allow Internet and intranet access.

> **Note** Cloud products requiring intranet communication must use the same network type. For example, if an ECS instance in a VPC network needs to access a Server Load Balancer (SLB) instance or ApsaraDB for RDS (RDS) instance through intranet, the SLB instance and the RDS instance must also use the VPC network, otherwise the access will fail.

For different cloud products, the way you choose to use VPC is different:

- Choose to use VPC on the purchase page

  This method mainly applies to cloud products such as ECS, RDS and SLB. These cloud products provide different networks for you to choose. You can select the VPC when purchasing an instance. After an instance is created, a private IP address or a private endpoint will be allocated to the instance.

- Choose to use VPC on the console

  This method applies to cloud products such as Table Store, Container Service, E-MapReduce and Network Attached Storage.

  You can set a VPC endpoint for a Table Store instance on the Table Store console, choose to use VPC when creating a Container Service cluster or E-MapReduce cluster on the console.

- View VPC endpoints

  This applies to cloud products such as Log Service, Object Storage Service and ECS. You can view help documents of the following products:

  - VPC endpoint of Log Service
  - VPC endpoint of Object Storage Service
  - VPC endpoint of ECS

  You can call APIs for other cloud products through the PrivateZone intranet. For more information, see Activate PrivateZone.

How to change the network type?

- For some instance type cloud products such as ApsaraDB for RDS, you can change the network type from the classic network to VPC on the console.
- Server Load Balancer does not support network type changes. You can purchase an SLB instance of the VPC network and then add ECS instances of the VPC network to it.

For more information, see Overview.

5.Classic network-to-VPC migration

5.1. Overview

This topic provides an overview of the solutions that are used to migrate cloud resources from a classic network to a virtual private cloud (VPC). A VPC is an isolated network environment and ensures high security for your workloads.

Benefits

A VPC is a private network in Alibaba Cloud. You can use Alibaba Cloud resources in your VPC. VPCs provide the following benefits:

- Secure network environment

  VPCs isolate the data link layer based on the tunneling technique. VPCs provide an independent, isolated, and secure network for each tenant. Different VPCs are isolated from each other.

- Flexible network configurations

  You can specify the CIDR blocks and configure route tables and gateways in your VPC. Furthermore, you can connect your VPC to other VPCs or on-premises data centers to create a custom network environment through a physical connection or VPN gateways. This allows you to extend the capacity of on-premises data centers and migrate applications to Alibaba Cloud.

Migration solutions

You can use the following solutions to migrate your cloud resources from a classic network to a VPC. You can use either of these solutions or combine them to meet your business requirements.

- Hybrid migration

  If your system is deployed on ApsaraDB RDS, Server Load Balancer (SLB), or other cloud services, we recommend that you use the hybrid migration solution. This solution allows you to migrate your system to a VPC without service disruptions.

  This solution can be integrated with the ClassicLink feature to allow ECS instances in the classic network to access cloud resources in the VPC. For more information, see Overview.

- Single ECS migration

  If your applications are deployed on an ECS instance and restarting the instance does not affect your system, we recommend that you use the single ECS migration solution.

Hybrid migration

The hybrid migration is a seamless migration solution that consists of hybrid access and hybrid attachment. This solution allows you to create cloud instances in a VPC, such as ECS instances, and migrate your applications to the VPC. After all your systems are migrated to the VPC, you can release the cloud resources in the classic network. For more information, see Hybrid migration.

- **Hybrid attachment**

  Hybrid attachment refers to attaching ECS instances in classic networks and VPCs to a Server Load Balancer (SLB) instance as backend servers to process forwarded requests. Hybrid attachment also allows you to add ECS instances in the classic networks and the VPC to a VServer group.

  Hybrid attachment is supported by public-facing and internal SLB instances.

> **Note** You can attach ECS instances in classic networks and VPCs to an internal network SLB instance. If you configure a Layer-4 (TCP and UDP) listener, you can obtain real client IP addresses from the ECS instances in the VPC. However, you cannot obtain IP addresses from ECS instances in the classic network. If you configure a Layer-7 (HTTP and HTTPs) listener, you can obtain the real client IP addresses from ECS instances in the VPC and the classic-network.

- **Hybrid access**

  Hybrid access allows ApsaraDB RDS, Object Storage Service (OSS), or other cloud services to be accessed by both the ECS instances in the classic network and the ECS instances in the VPC. Each service supports hybrid access and provides two types of endpoints. One type of endpoint is used to access the service over the classic network. The other type of endpoint is used to access the service within the VPC.

When you use the hybrid migration solution, take note of the following rules:

- This solution supports most migration scenarios. If the ECS instances in the classic network are required to communicate with the VPC, you can use the ClassicLink feature to enable internal connections among these ECS instances.
- This solution applies only to the migration of your system from a classic network to a VPC.

5.2. Hybrid access to ApsaraDB

5.2.1. Overview of the hybrid access mode of ApsaraDB

This topic provides an overview of the hybrid access mode of ApsaraDB. By using the hybrid access mode, you can access ApsaraDB from classic-network ECS instances and VPC ECS instances. The hybrid access mode of ApsaraDB reserves the classic network endpoint and the VPC endpoint at the same time. In this way, service disruptions can be avoided during the migration.

When you switch the network type of ApsaraDB instances from classic network to VPC, you can specify the retention period of the classic network endpoint. After the retention period expires, the classic network endpoint is automatically deleted.

Note the following when you use the hybrid access mode of ApsaraDB:

- The ApsaraDB types that support hybrid access are as follows:
  - ApsaraDB for RDS MySQL, SQL Server, PPAS, and PostgreSQL in the enhanced security mode
  - ApsaraDB for Redis/Redis cluster version
  - New ApsaraDB for Memcache (purchased after May 12, 2017)

- ApsaraDB for MongoDB replica set

  For MongoDB instances, RDS instances, and Redis instances, you can switch their network type from classic network to VPC through the console or the relevant API. After you switch the network type, the classic network endpoint remains unchanged and a VPC endpoint is created. You can view the classic network endpoint and the VPC endpoint in the console.

  For Memcache instances, you need to switch their network type from classic network to VPC through the relevant API. If you switch the network type through the console, the classic network endpoint cannot be reserved. After you switch the network type through the relevant API, the classic network endpoint remains unchanged and a VPC endpoint is created. The VPC network endpoint is displayed in the console. The classic network endpoint can only be viewed by calling the relevant API action.

- The ApsaraDB types that do not support hybrid access are as follows:
  - ApsaraDB for RDS in the standard network mode. To change the network type, switch to the enhanced security mode first.
  - ApsaraDB for MongoDB cluster version.
  - Earlier versions of ApsaraDB for Memcache (purchased before May 12, 2017). To change the network type, you must purchase an instance and migrate the instance to the new ApsaraDB for Memcache.

5.2.2. Switch the network type of an ApsaraDB for RDS instance

This topic describes how you can switch the network type of an ApsaraDB RDS instance from a classic network to a virtual private cloud (VPC) by using the RDS console or by calling the required API operation.

Prerequisites

Before you switch the network type, make sure that the following conditions are met:

- An Alibaba Cloud account is created. To create an Alibaba Cloud account, go to the Alibaba Cloud official website. For more information, seeCreate an Alibaba Cloud account.
- The network type of the RDS instance is the classic network.
- VPCs and VSwitches are available in the zone to which the RDS instance belongs. For more information, see Create a VPC.

Background information

For more information about how you can switch the network type of an RDS instance from a classic network to a VPC, see Hybrid access solution for smooth migration from classic networks to VPCs.

> **Note**
>
> - When you switch the network type, you can specify a retention period for the classic network endpoint. After the retention period expires, the classic network endpoint is automatically deleted. Before the endpoint is deleted, you will receive SMS messages.
> - If the RDS instance is a subdatabase of a DRDS instance, the DRDS instance will be disconnected from the RDS instance after the network type is switched. You must manually reconnect both instances.

Switch the network type by using the RDS console

1. Log on to the ApsaraDB for RDS console.
2. On the top of the page, select the region where the RDS instance is deployed.
3. Click the ID of the RDS instance.
4. In the left-side navigation pane, click **Databases Connection**.
5. On the **Instance Connection** tab, click **Switch to VPC**.
6. On the **Switch to VPC** page, select the VPC and VSwitch that you want to switch.
7. Select **Reserve Original Classic Network Endpoint** and set **Expiration Time** for the classic network endpoint.
   - Seven days before the classic network endpoint expires, the system will send SMS messages to the mobile phone associated with your account once a day.
   - When the classic network endpoint expires, it is automatically deleted. You cannot access the database through the classic network endpoint. To avoid service disruptions, set the retention period based on your specific needs. After you configure the hybrid access mode, you can change the expiration time.
8. Click **OK**. An **original classic endpoint** is added in the console.

Modify the retention period of the classic network endpoint by using the console

After you set the retention period for the classic network endpoint, you can extend the retention period by using the console before the endpoint expires.

During the hybrid access period, you can modify the retention period of the classic network endpoint at any time. The expiration date is timed from the date when you modify the retention period. For example, if the classic network endpoint is set to expire on August 18, 2017 and you modify the expiration date to 14 days later on August 15, 2017, the endpoint will be deleted on August 29, 2017.

1. Log on to the ApsaraDB for RDS console.
2. In the top menu bar, select the region where the RDS instance is deployed.
3. Click the ID of the RDS instance.
4. In the left-side navigation pane, click **Databases Connection**.
5. On the **Instance Connection** tab, click **Change Expiration Time**.
6. Select the expiration time and click **OK**.

Switch the network type by calling the relevant API operation

1. Download relevant SDKs.
   - aliyun-java-sdk-rds-new.zip
   - aliyun-python-sdk-rds-new.zip
   - aliyun-php-sdk-rds-new.zip
2. Call the ModifyDBInstanceNetworkType operation to switch the network type.Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ModifyDBInstanceNetworkType*
DBInstanceId	String	Yes	The ID of an instance.
InstanceNetworkType	String	Yes	The network type of the instance. Valid values: - *VPC*: a VPC network. - *Classic*: a classic network
VPCId	String	No	The ID of the VPC.
VSwitchId	String	No	The ID of the VSwitch. This parameter is required if the VPC ID is specified.
PrivateIpAddress	String	No	An IP address in the CIDR block of the VSwitch. If no IP address is entered, the system assigns a private IP address based on the VPC ID and the VSwitch ID.
RetainClassic	String	No	Specifies whether to retain the classic network endpoint. Default value: *False*. - *True*: The classic network endpoint is retained. - *False*: The classic network endpoint is not retained.
ClassicExpiredDays	String	No	The retention period of the classic network endpoint in days. The shortest period is 1 day. The longest period is 180 days. The default period is 7 days. This parameter is required if RetainClassic is set to True.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TaskId	String	The ID of the task.

Examples

If you want to retain the classic network endpoint:

- Set the RetainClassic parameter to True. The classic network endpoint can be retained.
- Set the ClassicExpiredDays parameter for the retention period of a classic network endpoint. After the classic network endpoint expires, the endpoint will be deleted.

```
import com.aliyuncs.DefaultAcsClient;
import com.aliyuncs.IAcsClient;
import com.aliyuncs.exceptions.ClientException;
import com.aliyuncs.exceptions.ServerException;
import com.aliyuncs.profile.DefaultProfile;
import com.aliyuncs.profile.IClientProfile;
import com.aliyuncs.rds.model.v20140815.ModifyDBInstanceNetworkTypeRequest;
import com.aliyuncs.rds.model.v20140815.ModifyDBInstanceNetworkTypeResponse;
import org.junit.Test;
public class ModifyDBInstanceNetworkTypeTest {
  @Test
  public  void switchNetwork_success() {
  ModifyDBInstanceNetworkTypeRequest request=new ModifyDBInstanceNetworkTypeRequest ();
    request.setInstanceId("<Your instance ID>");
    request.setInstanceNetworkType ("VPC");
    request.setVpcId("<VpcId: This parameter is required when the TargetNetworkType is set to VPC.>"
);
    request.setVSwitchId("<VSwitchId: This parameter is required when the TargetNetworkType is set
to VPC.>");
    request.setRetainClassic("<Specifies whether to retain the classic network endpoint: Set the value
to True to retain and set the value to False not to retain.>");
    request.setClassicExpiredDays("set the retention period of the classic network endpoint");
    IClientProfile profile = DefaultProfile.getProfile("cn-hangzhou", "<Your AccessKey information>",
      "<Your AccessKey Secret>");
    IAcsClient client = new DefaultAcsClient(profile);
  try {
      ModifyDBInstanceNetworkTypeResponse response
        = client.getAcsResponse(request);
      System.out.println(response.getRequestId());
  }catch (ServerException e) {
      e.printStackTrace();
  }
    catch (ClientException e) {
      e.printStackTrace();
    }
  }
}
```

3. Call the DescribeDBInstanceNetInfo operation to view the classic network endpoint and the VPC endpoint.

   Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeDBInstanceNetInfo*
DBInstanceId	String	Yes	The ID of an instance.

Response parameters

Parameter	Type	Description
DBInstanceNetInfos	List	The connection information of the instance.
InstanceNetworkType	String	The network connection type of the instance. Valid values: ○ *VPC*: a VPC network. ○ *Classic*: a classic network

DBInstanceNetInfo

Parameter	Type	Description
ConnectionString	String	The connection string of DNS.
IPAddress	String	The IP address.
IPType	String	The IP address type of the classic-network instance: *Inner and Public*. The IP address type of the VPC instance: *Private and Public*.
Port	String	The port information.
VPCId	String	The ID of the VPC.
VSwitchId	String	The ID of a VSwitch.
ExpiredTime	String	The expiration time.

Examples

```
import com.aliyuncs.IAcsClient;
import com.aliyuncs.exceptions.ClientException;
import com.aliyuncs.exceptions.ServerException;
import com.aliyuncs.profile.DefaultProfile;
import com.aliyuncs.profile.IClientProfile;
import com.aliyuncs.rds.model.v20140815.DescribeDBInstanceNetInfoRequest;
import import com.aliyuncs.rds.model.v20140815.DescribeDBInstanceNetInfoResponse;
import org.junit.Test;
public class DescribeDBInstanceNetInfoTest {
  @Test
  public void describeDBInstanceNetInfo_success() {
    DescribeDBInstanceNetInfoRequest request=new DescribeDBInstanceNetInfoRequest();
    request.setInstanceId("<Your instance ID>");
    IClientProfile profile = DefaultProfile.getProfile("cn-hangzhou", "<Your AccessKey information>",
      "<Your AccessKey Secret>");
    IAcsClient client = new DefaultAcsClient(profile);
    try {
      DescribeDBInstanceNetInfoResponse response
        = client.getAcsResponse(request);
      System.out.println(response.getRequestId());
  }catch (ServerException e) {
      e.printStackTrace();
  }
    catch (ClientException e) {
      e.printStackTrace();
    }
  }
}
```

Modify the retention period of the classic network endpoint by using the relevant API operation

1. Download relevant SDKs.
   - aliyun-java-sdk-rds-new.zip
   - aliyun-python-sdk-rds-new.zip
   - aliyun-php-sdk-rds-new.zip
2. Call the ModifyDBInstanceNetworkExpireTime operation to modify the retention period of the classic network endpoint.

   Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ModifyDBInstanceNetworkExpireTime*.
DBInstanceId	String	Yes	The ID of an instance.
ConnectionString	String	Yes	The classic network endpoint for which retention period you want to extend. Classic network endpoints are divided into the classic network endpoint of the current instance and the classic network endpoint with read/write splitting.
ClassicExpiredDays	Integer	Yes	The retention period of the classic network endpoint. Value range: 1 to 120 days.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

```
public static void main(String[] args) {
    ModifyDBInstanceNetExpireTimeRequest request = new ModifyDBInstanceNetExpireTimeRequest();
    request.setClassicExpiredDays(3);
    request.setConnectionString("<Connection string>");
    request.setInstanceId("<Instance ID>");
    IClientProfile profile
        = DefaultProfile.getProfile("cn-qingdao", "<Your AccessKey information>",
        "<Your AccessKey Secret>");
    IAcsClient client = new DefaultAcsClient(profile);
    try {
      ModifyDBInstanceNetExpireTimeResponse response
          = client.getAcsResponse(request);
      System.out.println(response.getRequestId());
    }catch (ServerException e) {
      e.printStackTrace();
    }
    catch (ClientException e) {
      e.printStackTrace();
    }
}
```

5.2.3. Switch the network type of a Redis instance

This topic describes how to switch the network type of a Redis instance from a classic network to a virtual private cloud (VPC) network by using the console or by calling the relevant API operation. When you switch the network type, you can specify a retention period for the classic network endpoint. After the retention period expires, the classic network endpoint is automatically deleted.

Prerequisites

Before you can switch the network type, the following conditions must be met:

- An Alibaba Cloud account is created. If you do not have an Alibaba Cloud account, create one. For more information,Create an Alibaba Cloud account.
- The network type of the Redis instance is the classic network.
- VPCs and VSwitches are available in the zone to which the Redis instance belongs. For more information, see Create a VPC.

Switch the network type in the console

1. Log on to the ApsaraDB for Redis console.
2. Select the region where the instance is located.
3. Click the ID of the instance.

4. On the **Instance Information** page, click **Switch to VPC Network**.
5. In the dialog box that appears, perform the following steps:
   i. Select the VPC network and VSwitch that you want to use.
   ii. You can choose to retain a classic network endpoint and specify a retention period.

   > **Note** After you select to retain the classic network endpoint, the classic network endpoint and the VPC endpoint remain two different endpoints. ECS instances in the classic network can still access the database as normal and services are not affected. When the classic network endpoint expires, it is automatically deleted and you cannot access the database through the classic network endpoint.

   iii. Click **OK**.
6. You can click **Refresh** on the **Instance Information** page to view the endpoints of the classic network and VPC network.

Modify the retention period of the classic network endpoint by using the console

After you set the retention period for the connection address of a classic network, you can change the expiration date in the console to extend the retention period before the address expires.

During the period in which your instance can be connected over the classic network or VPCs, you can specify the expiration date for the endpoint of the classic network. The changes immediately take effect. For example, if the connection address of the classic network is about to expire on August 18, 2017 and you change the expiration date to 14 days later on August 15, 2017, the connection address of the classic network is released on August 29, 2017.

1. Log on to the ApsaraDB for Redis console.
2. Select the region where the instance is located.
3. Click the ID of the instance.
4. In the **Retained Classic Network IP Address** section, click **Change Expiration Date**.
5. In the dialog box that appears, select a new expiration time and click **OK**.

Switch the network type by calling the relevant API operation

1. Download relevant SDKs. (The SDK of ApsaraDB for Memcache is the same as that of ApsaraDB for Redis.)
   - aliyun-java-sdk- r-kvstore.zip
   - aliyun-python-sdk- r-kvstore.zip
   - aliyun-php-sdk-r-kvstore.zip
2. Call the SwitchNetwork API operation to switch the network type.

   Request parameters

Parameter	Type	Required	Description

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *SwitchNetwork*
InstanceId	String	Yes	The ID of the instance.
TargetNetworkType	String	Yes	The network type of the instance. Valid values: ○ *VPC*: a VPC network ○ *Classic*: a classic network
VPCId	String	No	The ID of the VPC network.
VSwitchId	String	No	The ID of the VSwitch. This parameter is required if the VPC ID is specified.
RetainClassic	String	No	Specifies whether to retain the classic network endpoint. Default: *False*: ○ *True*: The classic network endpoint is retained ○ *False*: The classic network endpoint is not retained
ClassicExpiredDays	String	No	The retention period of the classic network endpoint in days. Unit: days. Minimum value: 1. Maximum value: 120. Default value: 7. This parameter is required if RetainClassic is set to True.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TaskId	String	The ID of the task.

Sample requests

```
import com.aliyuncs.DefaultAcsClient;
import com.aliyuncs.IAcsClient;
import com.aliyuncs.exceptions.ClientException;
import com.aliyuncs.exceptions.ServerException;
import com.aliyuncs.profile.DefaultProfile;
import com.aliyuncs.profile.IClientProfile;
import com.aliyuncs.r_kvstore.model.v20150101.SwitchNetworkRequest;
import com.aliyuncs.r_kvstore.model.v20150101.SwitchNetworkResponse;
import org.junit.Test;
/**
 * Created by wb259286 on 2017/6/9.
 */
public class SwitchNetworkTest {
  @Test
  public  void switchNetwork_success() {
    SwitchNetworkRequest request=new SwitchNetworkRequest();
    request.setInstanceId("<<Your instance ID>");
    request.setTargetNetworkType("VPC");
    request.setVpcId("<VpcId: This parameter is required when TargetNetworkType is set to VPC.>");
    request.setVSwitchId("<VSwitchId: This parameter is required when the TargetNetworkType is VPC
>");
    request.setRetainClassic("<Whether to retain the classic network endpoint>");
    request.setClassicExpiredDays("The retention period of the classic network endpoint");
    IClientProfile profile = DefaultProfile.getProfile("cn-hangzhou", "<Your AccessKey information>",
      "<<Your AccessKey Secret>>");
    IAcsClient client = new DefaultAcsClient(profile);
    try {
      SwitchNetworkResponse response
        = client.getAcsResponse(request);
      System.out.println(response.getRequestId());
  }catch (ServerException e) {
      e.printStackTrace();
  }
    catch (ClientException e) {
      e.printStackTrace();
    }
  }
}
```

3. Call the DescribeDBInstanceNetInfo API operation to view the classic network endpoint and the VPC endpoint.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeDBInstanceNetInfo*
InstanceId	String	Yes	The ID of the instance.

Response parameters

Parameter	Type	Description
NetInfoItems	List	The connection information of the instance.
InstanceNetworkType	String	The network connection type of the instance. Valid values: - *VPC*: the VPC network type. - *Classic*: the classic network type.

InstanceNetInfo

Parameter	Type	Description
ConnectionString	String	The DNS connection string.
IPAddress	String	The IP address.
IPType	String	The following IP address types of the classic network are supported: *Inner and Public*. The IP address type of the VPC network: *Private and Public*.
Port	String	The port information.
VPCId	String	The ID of the VPC to which the instances belong.
VSwitchId	String	The ID of the VSwitch.
ExpiredTime	String	The expiration date.

Example code

```
import com.aliyuncs.DefaultAcsClient;
import com.aliyuncs.IAcsClient;
import com.aliyuncs.exceptions.ClientException;
import com.aliyuncs.exceptions.ServerException;
import com.aliyuncs.profile.DefaultProfile;
import com.aliyuncs.profile.IClientProfile;
import com.aliyuncs.r_kvstore.model.v20150101.DescribeDBInstanceNetInfoRequest;
import com.aliyuncs.r_kvstore.model.v20150101.DescribeDBInstanceNetInfoResponse;
import org.junit.Test;
/**
 *
 */
public class DescribeDBInstanceNetInfoTest {
@Test
  public  void describeDBInstanceNetInfo_success() {
    DescribeDBInstanceNetInfoRequest request=new    DescribeDBInstanceNetInfoRequest();
    request.setInstanceId("<Your instance ID>");
    IClientProfile profile = DefaultProfile.getProfile("cn-hangzhou", "<Your AccessKey information>",
      "<Your AccessKey Secret>");
    IAcsClient client = new DefaultAcsClient(profile);
    try {
      DescribeDBInstanceNetInfoResponse response
        = client.getAcsResponse(request);
      System.out.println(response.getRequestId());
  }catch (ServerException e) {
      e.printStackTrace();
    }
    catch (ClientException e) {
    e.printStackTrace();
    }
  }
}
```

Modify the retention period of the classic network endpoint by using the relevant API operation

1. Download relevant SDKs. (The SDK of ApsaraDB for Memcache is the same as that of ApsaraDB for Redis.)
   - aliyun-java-sdk- r-kvstore.zip
   - aliyun-python-sdk- r-kvstore.zip
   - aliyun-php-sdk-r-kvstore.zip

2. Call the ModifyInstanceNetExpireTime API operation to switch the network type.

   Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ModifyInstanceNetExpireTime*.
InstanceId	String	Yes	The ID of the instance.
ConnectionString	String	Yes	The endpoint of the classic network.
ClassicExpiredDays	Integer	Yes	Specifies the number of days the classic network endpoint is retained. Valid values: 14, 30, 60, and 120.

   Response parameters

Parameter	Type	Description
RequestId	String	The ID of the instance.

   Example code

```
public static void main(String[] args) {
  ModifyInstanceNetExpireTimeRequest request = new ModifyInstanceNetExpireTimeRequest();
  request.setClassicExpiredDays(3);
  request.setConnectionString("<The connection string>");
  request.setInstanceId("<The ID of the instance>");
  IClientProfile profile
      = DefaultProfile.getProfile("cn-hangzhou", "<Your AccessKey information>",
      "<Your AccessKey Secret>");
  IAcsClient client = new DefaultAcsClient(profile);
  try {
    ModifyInstanceNetExpireTimeResponse response
        = client.getAcsResponse(request);
    for (NetInfoItem item:response.getNetInfoItems()) {
      System.out.println(item.getConnectionString());
      System.out.println(item.getPort());
      System.out.println(item.getDBInstanceNetType());
      System.out.println(item.getIPAddress());
      System.out.println(item.getExpiredTime());
    }
  }catch (ServerException e) {
    e.printStackTrace();
  }
  catch (ClientException e) {
    e.printStackTrace();
  }
}
```

5.2.4. Switch the network type of an ApsaraDB for MongoDB instance

This topic describes how you can switch the network type of an ApsaraDB for MongoDB instance from a classic network to a virtual private cloud (VPC) by using the console or by calling the relevant API operation. When you switch the network type, you can specify a period for which you want to retain the classic network endpoint of the instance. After the retention period expires, the classic network endpoint is automatically deleted.

Prerequisites

Before you switch the network type, make sure that the following requirements are met:

- An Alibaba Cloud account is created. If you do not have an Alibaba Cloud account, create one. For more information, seeCreate an Alibaba Cloud account.
- The network type is the classic network.

- The instance must be an ApsaraDB for MongoDB replica set instance.
- VPCs and VSwitches are available in the zone to which the ApsaraDB for MongoDB instance belongs. For more information, see Create a VPC.

Switch the network type by using the console

1. Log on to the ApsaraDB for MongoDB console.
2. Find the instance that you want to manage, and click the instance ID or click **Manage** in the **Actions** column.
3. In the left-side navigation pane, click **Database Connection**, and click **Switch to VPC**.
4. In the dialog box that appears, perform the following steps:
   i. Select the VPC and VSwitch that you want to use.
   ii. You can choose to retain a classic network endpoint and specify a retention period.

   > **Note** After you select to retain the classic network endpoint, classic-network ECS instances can access the database. When the classic network endpoint expires, it is automatically deleted and you cannot access the database through the classic network endpoint.

   iii. Click **OK**.
5. You can click **Refresh** on the **Database Connection** page to view the endpoints of the classic network and VPC.

Switch the network type by calling the required API operation

1. Download an SDK that meets your business requirements. The following SDKs are available:
   - aliyun-python-sdk-dds.zip
   - aliyun-java-sdk-dds.zip
   - aliyun-php-sdk-dds.zip
2. Call the ModifyDBInstanceNetworkType operation to switch the network type.

   Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ModifyDBInstanceNetworkType*
DBInstanceId	String	Yes	The ID of the instance.
NetworkType	String	Yes	The network type of the instance. Valid values: - *VPC*: The instance runs in a VPC. - *Classic*: a classic network.
VPCId	String	No	The ID of the VPC.

Parameter	Type	Required	Description
VSwitchId	String	No	The ID of the VSwitch. This parameter is required if the VPC ID is specified.
RetainClassic	String	No	Specifies whether to retain the classic network endpoint. Default value: *False*: ○ *True*: The classic network endpoint is retained. ○ *False*: The classic network endpoint is not retained.
ClassicExpiredDays	String	No	The retention period of the classic network endpoint in days. The retention period of the classic network endpoint in days. Unit: days. Minimum value: 1. Maximum value: 120. Default value: 7. This parameter is required if RetainClassic is set to True.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TaskId	String	The ID of the task.

3. You can call the DescribeReplicaSetRole operation to view the classic network endpoint and the VPC endpoint.

   Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeReplicaSetRole*
DBInstanceId	String	Yes	The ID of an instance.

   Response parameters

Parameter	Type	Description
ReplicaSets	List	The list of replica set roles.
DBInstanceId	String	The ID of the instance.

ReplicaSetRole

Parameter	Type	Description
ReplicaSetRole	String	The replica set role. Valid values: *Primary and Secondary*.
ConnectionDomain	String	The domain name that is used to connect to the instance.
ConnectionPort	String	The port number that is used to connect to the instance.
ExpiredTime	String	The remaining period for the classic network endpoint. Unit: seconds.
NetworkType	String	The network type of the instance. Valid values: ○ *VPC*: a VPC network ○ *Classic*: a classic network

5.3. Other services that support hybrid access

This topic provides links to the documents that describe the endpoints of the cloud services that support hybrid access. In addition to ApsaraDB RDS, the following services support hybrid access. You can view the endpoints of different cloud services in the documents.

Storage services

- Object Storage Service: Obtain endpoints
- Tablestore: Obtain endpoints

Application services

- Log Service: Obtain endpoints

Middleware

- Message queue
  - Management and control: Obtain endpoints

Big data

- MaxCompute: Obtain endpoints

5.4. Hybrid migration

This topic describes how to use the hybrid migration solution to migrate cloud resources from a classic network to a virtual private cloud (VPC).

Prerequisites

Before you start the hybrid migration, make sure that the following requirements are met:

- An Alibaba Cloud account is created. If you do not have an Alibaba Cloud account, create one. To create an Alibaba Cloud account, clickCreate an Alibaba Cloud account.
- You are aware of the details and limits of the hybrid migration solution. For more information, see Overview.
- You are familiar with VPCs and the related products. VPCs are isolated private networks that allow you to manage your cloud resources by using relevant cloud services.
- The migration examples in this topic are for reference only. Systems in multiple use cases are more complex. You must assess the network architecture and system dependencies before you create a migration plan.

Systems to be migrated

The following two systems are used in the hybrid migration examples.

- System 1

  The following figure shows System 1. This system runs in a classic network system and integrates the Server Load Balancer (SLB), Elastic Compute Service (ECS), ApsaraDB RDS, and Object Storage Service (OSS) services. The Internet SLB instance uses two ECS instances as backend servers. The applications deployed on the two ECS instances are required to access the ApsaraDB RDS instance and the OSS bucket.

- System 2

  The following figure shows System 2. This system runs in a classic network. The architecture of System 2 is more complex than that of System 1. A public-facing SLB instance and an internal SLB instance are used. The ECS instances, ECS 1 and ECS 2, are specified as the backend servers of the public-facing SLB instance. Both ECS instances are required to access the internal SLB instance. Another two ECS instances, ECS 3 and ECS 4, are specified as the backend servers of the internal SLB instance. Both ECS instances are required to access the ApsaraDB RDS and the OSS.

Migrate System 1 to a VPC

To migrate **System 1** to a VPC, perform the following steps:

1. Prepare the network environment. Create a VPC to which the system is migrated and create a VSwitch for the VPC.

   For more information, see Create an IPv4 VPC network.

2. Obtain the internal endpoints of the ApsaraDB RDS instance and the OSS bucket that you want to access in the VPC.
   - You can use the RDS console or call the required API operation to switch the network type of the ApsaraDB RDS instance to VPC and reserve the classic network endpoint. For more information, see Switch the network type of an ApsaraDB for RDS instance.

     After System 1 is migrated, the classic network endpoint remains unchanged. An internal endpoint that can be accessed within the VPC is added. Therefore, the ECS instances in the classic network can still access can still access ApsaraDB RDS without service disruptions. After the classic network endpoint expires, it is automatically deleted. Then, ApsaraDB RDS can no longer be accessed through the classic network endpoint.
   - The OSS bucket provides a classic network endpoint and a VPC endpoint. You do not need to switch the network type. To obtain the VPC endpoint of the OSS bucket, see Regions and

endpoints.

3. Create and configure two ECS instances in the VPC. Create two ECS instances in the VPC, deploy applications on the ECS instances, and then change the endpoints of the ApsaraDB RDS instance and OSS bucket to the endpoints that can be accessed within the VPC. After you complete the configuration, you must conduct a test to verify that the ECS instances can access the OSS bucket and the ApsaraDB RDS instance.
4. Specify the ECS instances in the VPC as the backend servers of the public-facing SLB instance. Add the two ECS instances in the VPC as the backend servers of the public-facing SLB instance. Check the health status of the ECS instances. We recommend that you set a lower weight for the ECS instances. This can reduce the impact of unexpected faults on the system. Check the system status, traffic monitoring, and health check logs.
5. Remove the classic-network ECS instances from the backend servers of the public-facing SLB instance. The following figure shows how to remove the classic-network ECS instances from the backend servers of the public-facing SLB instance. We recommend that you set the weight of the classic-network ECS instances to 0. After these ECS instance no longer receive requests, remove them from the backend servers of the SLB instance.
6. Release the classic-network ECS instances. Release the classic-network ECS instances after the system runs as expected for a specific period. The public-facing SLB instance supports the ECS instances in the VPC and it is not required to be migrated. Your migration is complete.

   > **Note** The classic network endpoint of the ApsaraDB RDS instance will be automatically deleted after it expires.

Migrate System 2 to a VPC

When you migrate System 2 to a VPC, the preceding procedure does not apply. If you use the preceding procedure, the ECS instances in the VPC cannot access the ECS instances in the classic network. This is because the SLB instances that use these ECS instances as backend servers do not support hybrid access.

To migrate System 2 to a VPC, perform the following steps:

1. Create two ECS instances in the VPC to migrate ECS 3 and ECS 4 in the classic network to these ECS instances in the VPC. ECS 3 and ECS 4 are specified as the backend servers of the internal SLB instance.
2. Configure the ECS instances in the VPC, and change the endpoints of the ApsaraDB RDS instance and the OSS bucket to the endpoints that can be accessed within the VPC.
3. Create an internal SLB instance in the VPC to replace the internal SLB instance in the classic network.
4. Configure the internal SLB instance in the VPC. Add the two ECS instances that are created in Step 1 as backend servers.
5. Create another two ECS instances in the VPC as the migration destinations of ECS 1 and ECS 2 that are specified as the backend servers of the public-facing SLB instance.
6. Configure the ECS instances that are created in Step 5. Change the classic network endpoint of the internal SLB instance to the endpoint that is used in the VPC.
7. Repeat Steps 4 to 6 that are described in the migration solution of System 1 to migrate System 2.

5.5. Migrate ECS instances

This topic describes how to migrate one or more ECS instances from a classic network to a VPC.

Limits

Take note of the following requirements before you migrate ECS instances:

- During the migration process, the ECS instances will restart. This may affect your system and services.
- After the migration, no special configuration is required and the public IP address of the ECS instance remains unchanged.
  - For each migrated ECS instance, the public IP remains unchanged. However, you cannot view this public IP address in the operating system of the ECS instance. This public IP address is automatically assigned to the ECS instance in the VPC. You can change the public IP address of a pay-by-data-transfer ECS instance to an elastic IP address (EIP).
  - If one of your applications depends on the visible public IP on the operating system of the ECS instance, evaluate the migration carefully because it will have some impacts on the service.
- The VSwitch of the VPC network and the ECS instances that you want to migrate must be in the same zone.
- The instance ID and logon information remain unchanged in the migration process.
- The migration of subscription instances is not charged. The migrated ECS instances are billed in a new billing cycle. The billing rate is the same as that of the VPC-facing instances with the same specifications.
- Renewal or configuration upgrading orders that have not taken effect or have not been paid will be canceled after the migration and cannot be restored. You must place renewal or scaling orders for the ECS instances again.

Step 1: Schedule the migration

1. Log on to the ECS console.
2. Find the instance that you want to manage, and choose **More > Network and Security Group > Schedule Migration to VPC**.
3. In the displayed dialog box, click **OK**.
4. Click **View Scheduled Tasks** or click **Pending Events** in the common settings in the upper-right corner of the **Overview** page.
5. On the **Pending Events** page, click the **Migrate to VPC** tab.
6. Select the instance that you want to migrate, and then click **Schedule Migration**.
7. In the displayed dialog box, select the VPC network, VSwitch and time of migration, and click **OK**.

Step 2: Start the migration

After you schedule the migration, Alibaba Cloud will migrate the ECS instances at the scheduled time. It takes about five minutes to complete the migration.

Step 3: View the migration result

You can use one of the following methods to view the migration result:

- View the event status on the All Events page. If the event status is in the **Complete** state, the

migration succeeded.

- Check whether you have received an SMS message that indicates that the migration succeeded.
- Log on to the ECS console and check whether the **Network Type** of the instance is **VPC**.