ALIBABA CLOUD

Alibaba Cloud

Virtual Private Cloud

Best practices

Document Version: 20220402

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.

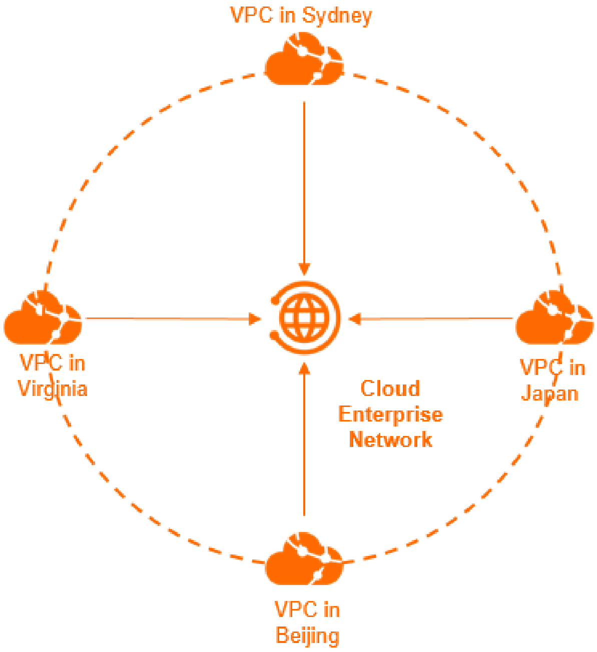
Connect VPCs

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.

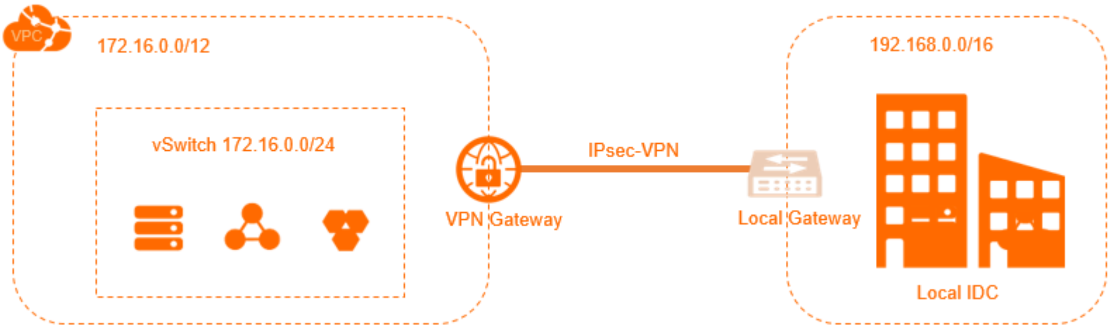
- CEN

  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

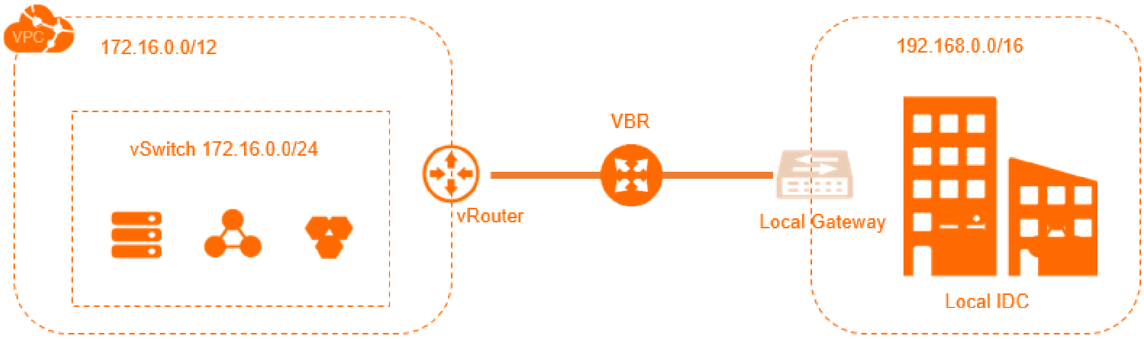
You can connect a VPC to an on-premises data center to build a hybrid cloud. You can establish secure and reliable connections between the VPC and the on-premises data center. This allows you to integrate the computing, storage, network, CDN and BGP resources of Alibaba Cloud with your IT infrastructure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

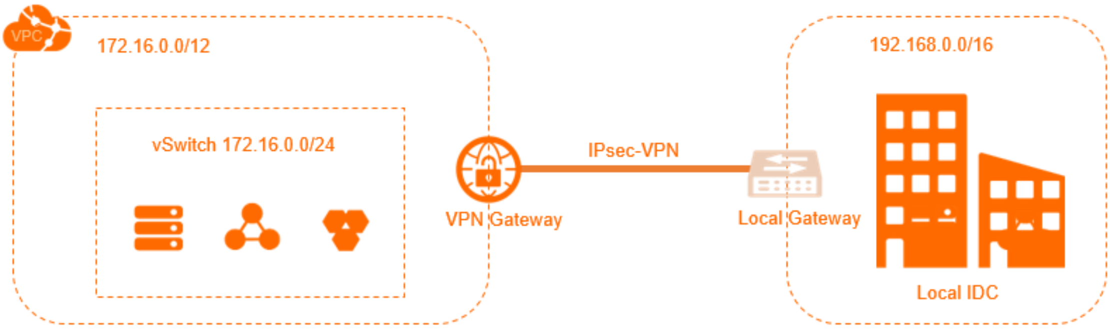
  Express Connect supports connections through leased lines. After a leased line has accessed an Alibaba cloud access point, you can create a VBR to connect your on-premises data center with Alibaba Cloud. This way, you can build a hybrid cloud to enable connections over a private network, instead of the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



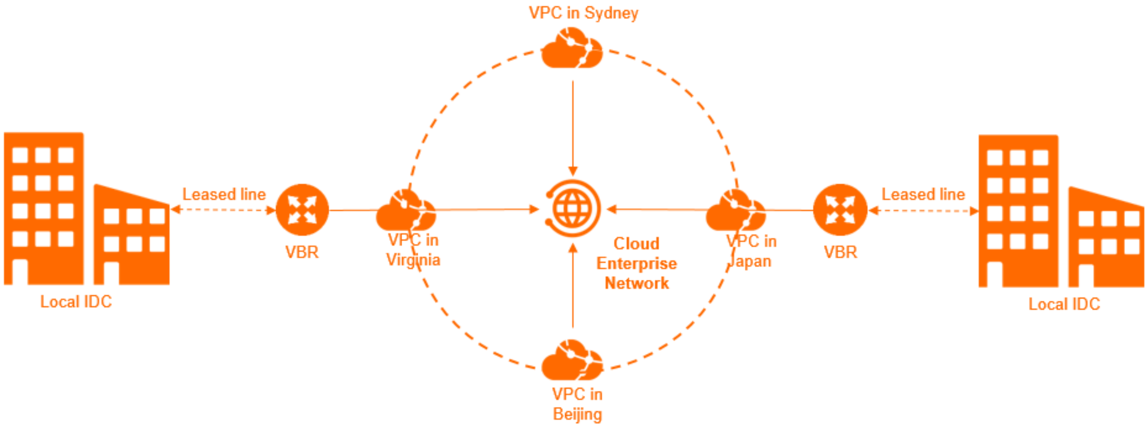
- VPN gateways

  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

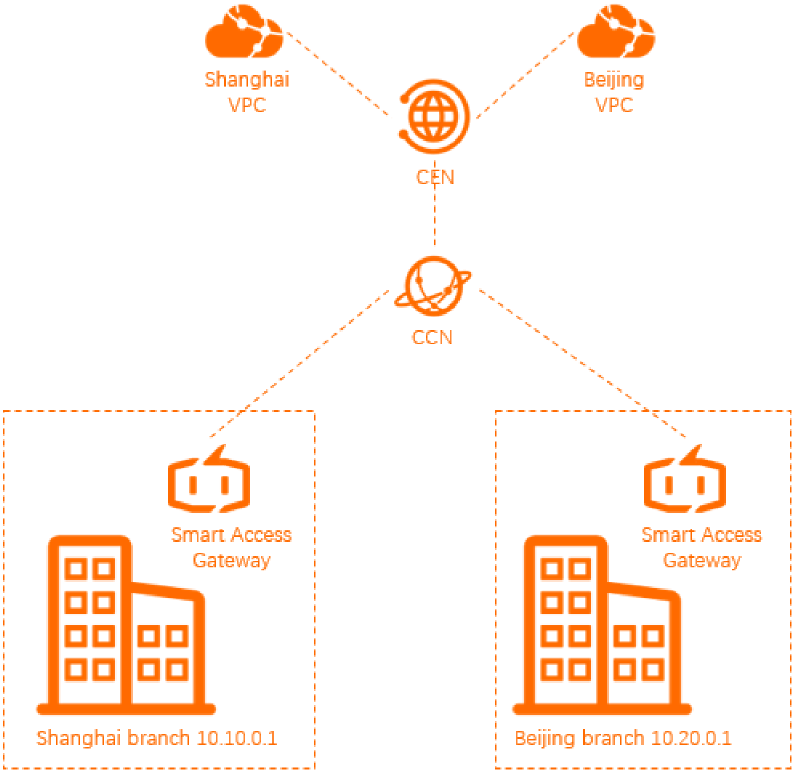
  CEN can be used to establish internal connections and connect resources within multiple VPCs based on automatic route distribution and learning. After you attach the VBR that is associated with an on-premises data center to a CEN instance, the on-premises data center can communicate with all cloud resources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



- SAG

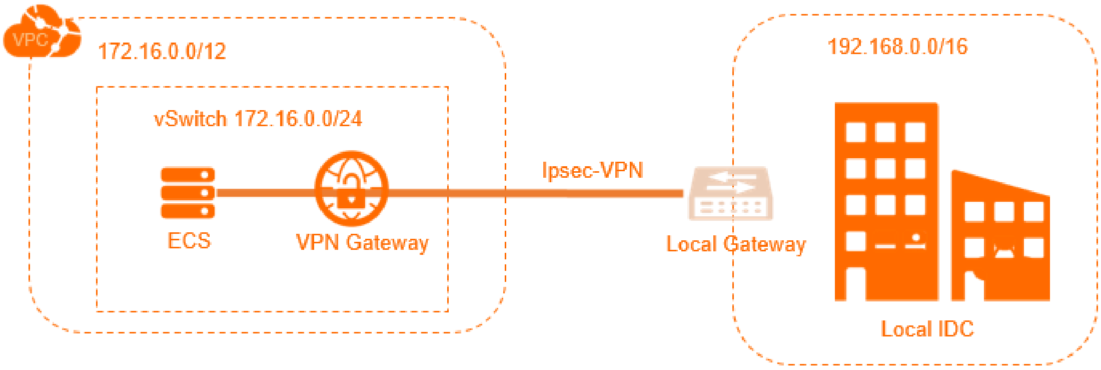
  Smart Access Gateway provides an end-to-end cloud deployment solution. SAG allows enterprises to connect to the nearest access points of VPC through encrypted connections over the Internet. SAG provides more intelligent, reliable, and secure connections to the cloud.

  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.



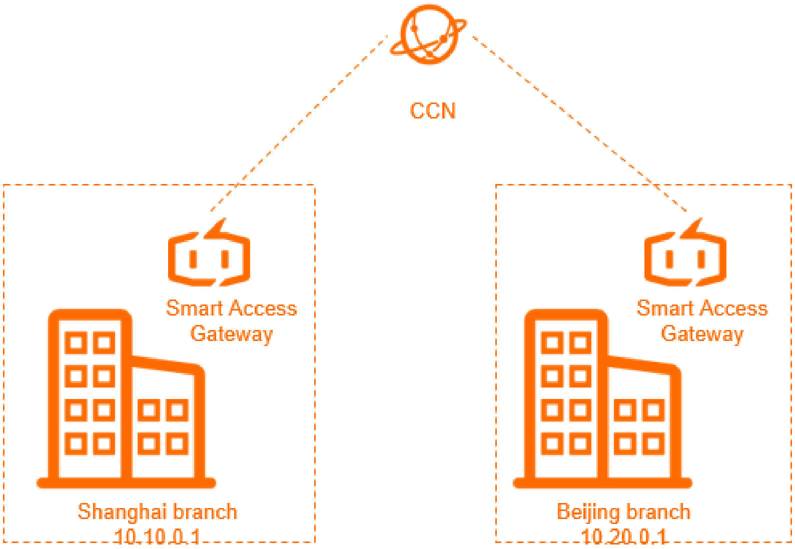
Connect multiple sites

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.

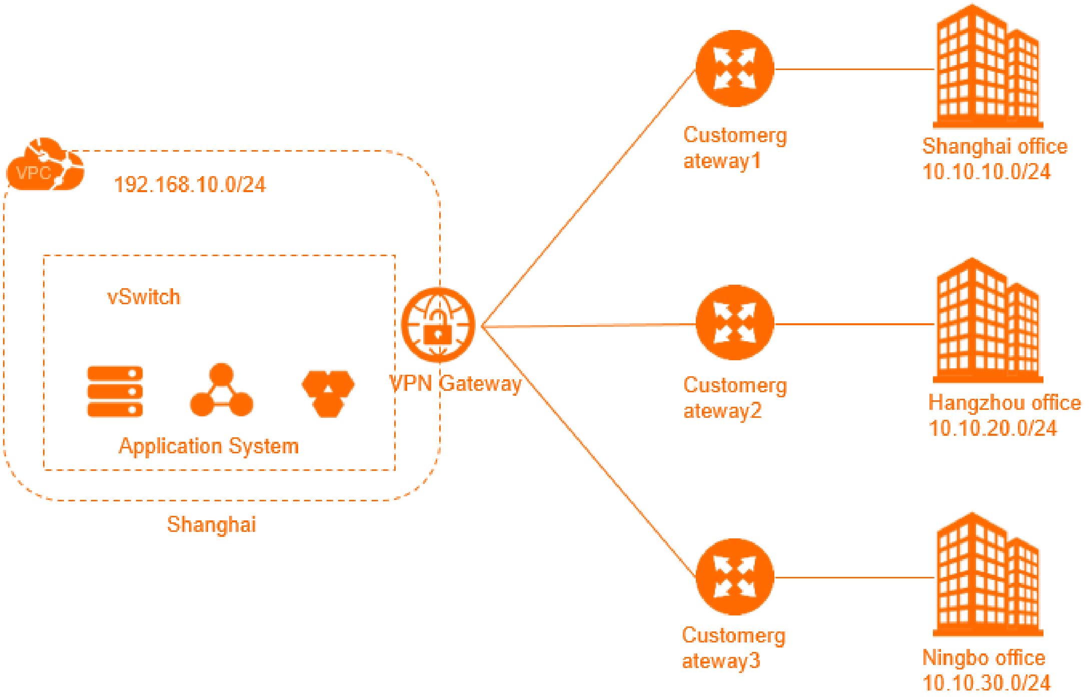


- VPN Gateway

  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.

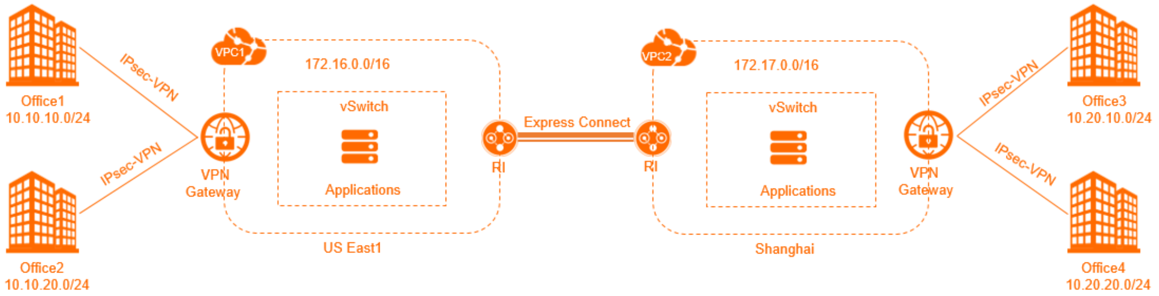
By default, the VPN-Hub function is enabled. You must configure the IPsec-VPN connection between each office site and Alibaba Cloud. No additional configurations or payments are required. A VPN gateway supports up to 10 IPsec connections. You can connect 10 office sites in different areas by using one 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.



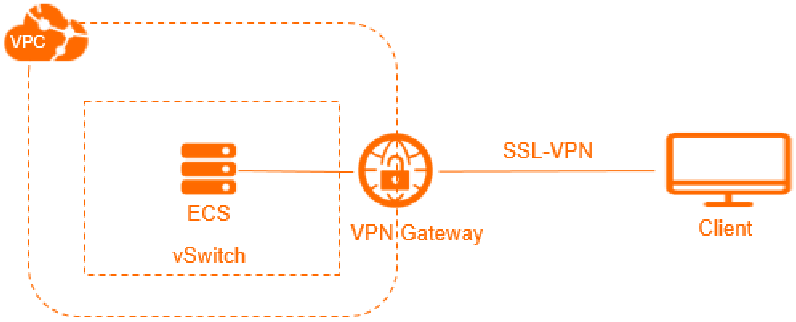
Remote access to a VPC

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

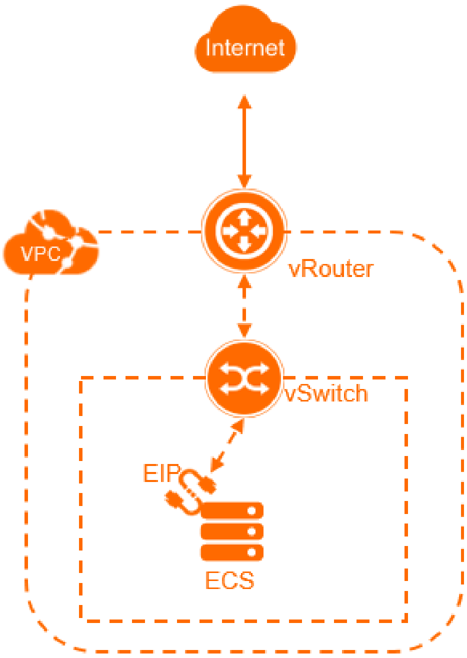
The following table lists the features of Alibaba Cloud products that have access to the Internet.

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.

Scenario 1: Provide external services

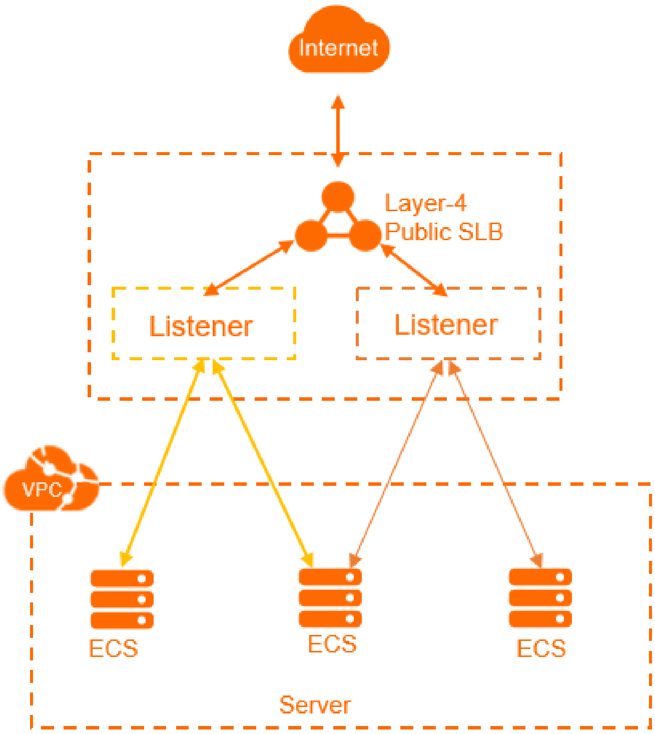
- Provide external services by using a single ECS instance

  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.



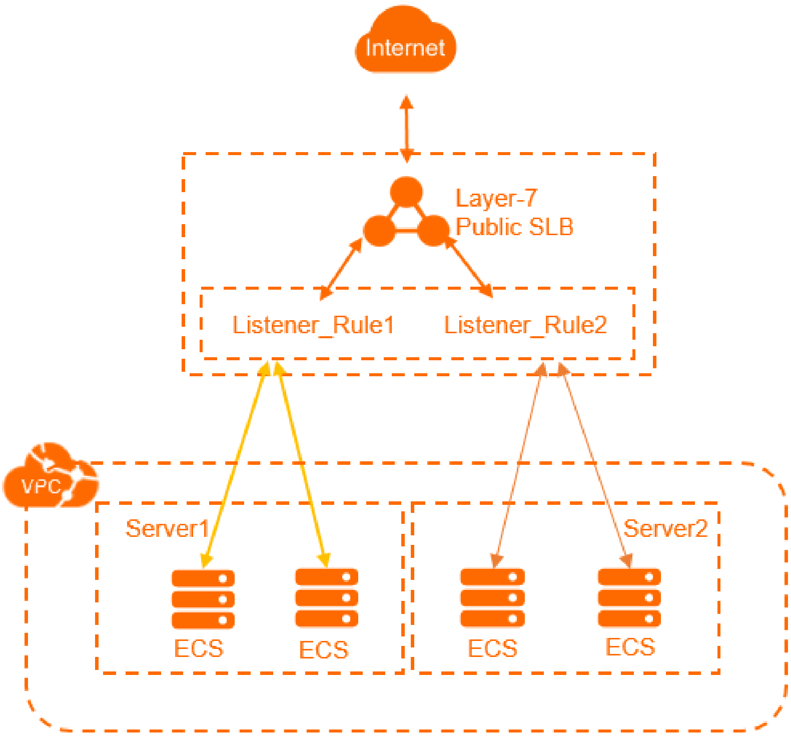
- Provide external services by using the Layer-4 load balancing function

  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

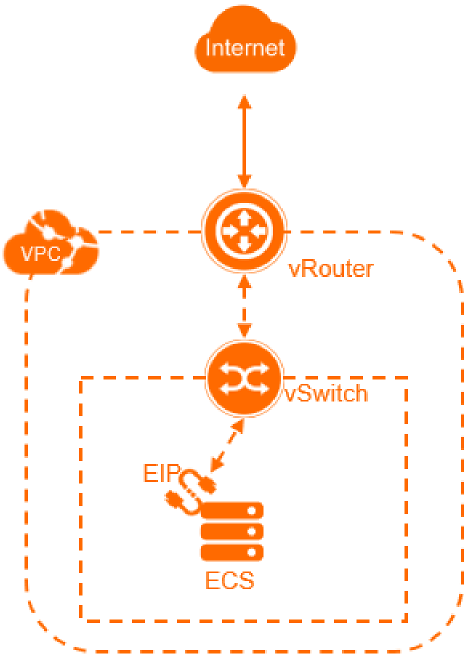
If you want to distribute different requests to different backend servers, you can add domain name-based or URL-based forwarding rules to a Layer-7 listener. Specifically, you can create an Internet SLB instance with a Layer-7 listener and add the ECS instances as backend servers.



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

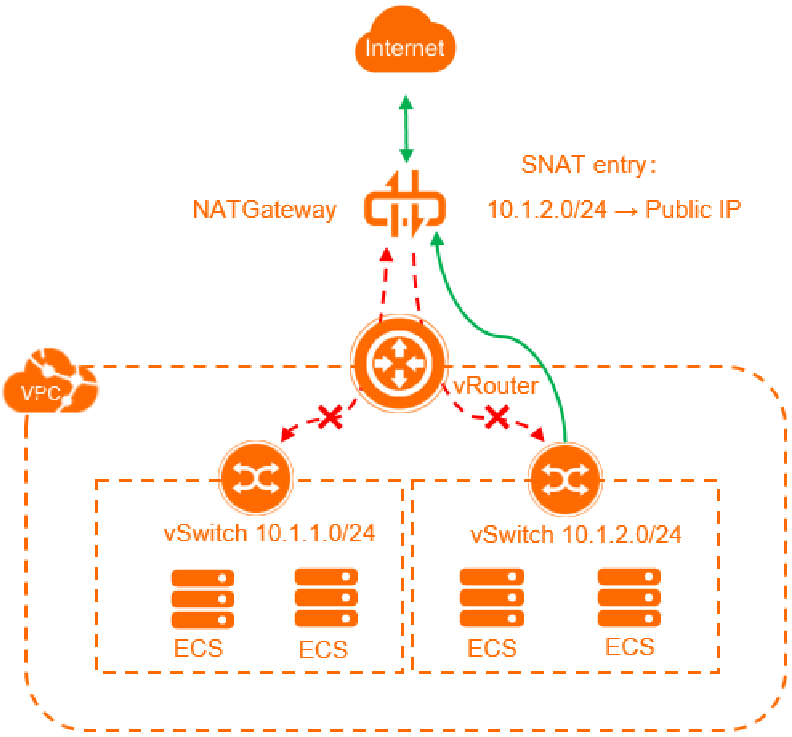
- Associate an EIP

  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

This topic describes how to reduce the costs of data transfer over the Internet by using data transfer plans and elastic IP address (EIP) bandwidth plans.

Data transfer plans

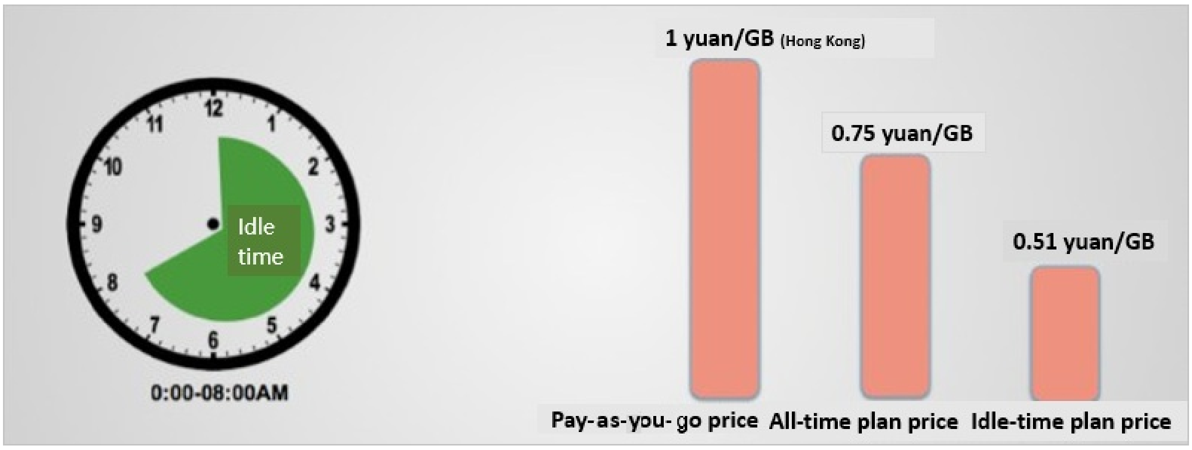
You can use data transfer plans to deduct the costs of data transfer over the Internet. Data transfer plans are billed on a subscription basis, which is more cost-effective than pay-as-you-go. In addition, you can use off-peak data transfer plans to reduce expenses on data transfer over the Internet. Data transfer plans are automatically applied to Elastic Cloud Service (ECS) instances, EIPs, and Server Load Balancer (SLB) instances that are billed by data transfer.

Data transfer plans are easy to use. After you purchase a data transfer plan, it is automatically applied. You can view the usage of data transfer plan on the Billing Management page.

The following section describes the benefits of data transfer plans:

- Reduce the costs of data transfer

  Off-peak data transfer plans are offered at a lower price. In the following table, the China (Hong Kong) region is used as an example to compare the costs of data transfer when the pay-as-you-go billing method, a full-time data transfer plan, and an off-peak data transfer plan are used.



  Assume that your cloud resources consume a total of 5 TB data in the China (Hong Kong) region. The statistics in the following table show that using data transfer plans can greatly reduce the costs of data transfer.

Billing of 5 TB of data transferred in the China (Hong Kong) region	Unit price (CNY/GB)	Total amount (CNY)	Saves (CNY)	Saves (%)
Pay-as-you-go	1	5120	0	0
Full-time data transfer plan	0.75	3727	1393	27.2%

Billing of 5 TB of data transferred in the China (Hong Kong) region	Unit price (CNY/GB)	Total amount (CNY)	Saves (CNY)	Saves (%)
Off-peak data transfer plan	0.51	2609	2511	49%

- Supports multiple scenarios

  All ECS instances, EIPs, and SLB instances that are paid 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 data transfer plan has a validity period. After a data transfer plan expires, the remaining quota of the plan becomes invalid. We recommend that you purchase a proper number of data transfer plans based on the historical data usage of your workloads. You can first purchase data transfer plans to meet the lowest data transfer requirement. Then, purchase more data transfer plans in the future when the need in data transfer grows.
  - When your data transfer plans are exhausted, the system automatically switches to the pay-as-you-go billing method. This ensures business continuity.
  - If you have purchased multiple data transfer plans, the system preferably applies the data transfer plan whichever will expire first.

EIP bandwidth plans

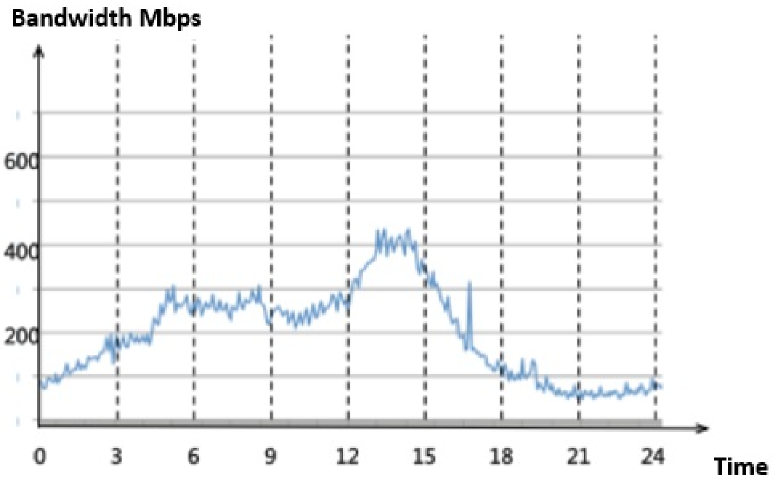
EIP bandwidth plans are offered as an independent bandwidth service. EIP bandwidth plans provide high-quality multi-line Border Gateway Protocol (BGP) bandwidth and support multiple billing methods. You can add EIPs to an EIP bandwidth plan. This allows the EIPs to share the bandwidth that is supported by the EIP bandwidth plan. You can associate the EIPs with ECS instances, NAT gateways, or SLB instances in a virtual private cloud (VPC). This way, these services can share the bandwidth of your EIP bandwidth plan.

EIP bandwidth plans support multiple billing methods, includingpay-by-bandwidth. You can purchase EIP bandwidth plans and choose different billing methods to reduce your expenses on bandwidth resources. In addition, this improves the elasticity of your services.

Note EIP bandwidth plans are provided as an independent bandwidth service. EIP bandwidth plans are not bundled with public IP addresses. You must manually add EIPs to EIP bandwidth plans.

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 is suitable for scenarios in which network traffic severely fluctuates. For example, you have deployed 10 ECS instances in the China (Hong Kong) region. EIPs are associated with these ECS instances. The EIPs are paid by bandwidth and the maximum bandwidth of each EIP is 100 Mbit/s. You must pay for the 10 EIPs with the maximum bandwidth of 100 Mbit/s. Therefore, you are charged CNY 3,253 per day.

However, the analytic results of network traffic on the 10 EIPs indicate that user traffic destined for different ECS instances fluctuate 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 plans. You can purchase an EIP bandwidth plan of 500 Mbit/s in size for the 10 ECS instances. Each ECS instance can use a peak bandwidth five times that of the EIP, and you are charged only CNY 1,680 per day for the 500 Mbit/s EIP bandwidth plan. The daily bandwidth cost is reduced to CNY 1,573, which is 50% off.

Therefore, if you have purchased multiple EIPs and you experience severe workload fluctuations, you can purchase EIP bandwidth plans to reduce costs.

Note We recommend that you analyze the data transfer model of your system and select an appropriate billing method:

If the data transfer is stable, you can choose the subscription billing method. This saves 20% to 30% of the costs compared with the pay-as-you-go billing method.

4.Deploy cloud services in a VPC

Most Alibaba Cloud services support virtual private clouds (VPCs). You can choose to use a VPC when you create a cloud resource. You can also create a VPC, and then create cloud resources in the VPC.

Use a VPC

A VPC is an isolated private network. By default, VPCs cannot communicate with each other. Elastic Compute Service (ECS) instances in a VPC cannot access the Internet or be accessed over the Internet. A VPC cannot communicate with a classic network over a private network. However, most Alibaba Cloud services can be accessed over the Internet or a private network. More than 95% of Alibaba Cloud services support VPCs.

> **Note** Cloud resources that need to communicate with each other over a private network must be of the same network type. For example, if an ECS instance in a VPC needs to access a Classic Load Balancer (CLB) instance or an ApsaraDB RDS instance over a private network, the CLB instance or the ApsaraDB RDS instance must be deployed in a VPC.

How you use a VPC varies based on the service:

- Select VPC as the network type on the buy page

  You can use this method for services that allow you to create instances, such as ECS, ApsaraDB RDS, and CLB. You can select VPC as the network type on the buy page of these services. This way, the instance that you purchase is created in a VPC or a VPC endpoint is provided for the instance. The endpoint is resolved to an IP address that falls within the CIDR block of the VPC.

- Configure VPC access in the console

  You can use this method for services such as Tablestore (OTS), Container Service for Kubernetes (ACK), E-MapReduce (EMR), and Apsara File Storage NAS (NAS).

  For OTS, you can configure a VPC endpoint for an OTS instance in the console. For ACK or EMR, you can select VPC as the network type when you create an ACK cluster or an EMR cluster in the console. For NAS, you can add a VPC as a mount target in the console.

- View the VPC endpoints of different services

  The following topics describe how to view the VPC endpoints of Log Service, Object Storage Service (OSS), and ECS:

  - VPC endpoints of Log Service
  - VPC endpoints of OSS
  - VPC endpoints of ECS

  To query the VPC endpoints of other services, you can use Alibaba Cloud DNS PrivateZone to call API operations. For more information, see Activate Alibaba Cloud DNS PrivateZone.

Change the network type

- For some cloud services that allow you to create instances, such as ApsaraDB RDS, you can change the network type from classic network to VPC in the console.

- For CLB instances, you cannot change the network type from classic network to VPC. You can create a new CLB instance that uses VPC and associate ECS instances in a VPC with the CLB instance.

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 Migrate cloud resources from a classic network to a VPC.

- **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. Change the network type of an ApsaraDB RDS instance

This topic describes how to change the network type of an ApsaraDB RDS instance from classic network to Virtual Private Cloud (VPC) by using the ApsaraDB RDS console or by calling the relevant API operation. You can choose to retain the classic network endpoint when you change the network type.

Prerequisites

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

- The ApsaraDB RDS instance is deployed in a classic network.
- VPCs and vSwitches are available in the zone to which the ApsaraDB RDS instance belongs. For more information, see Create an IPv4 VPC.

Background information

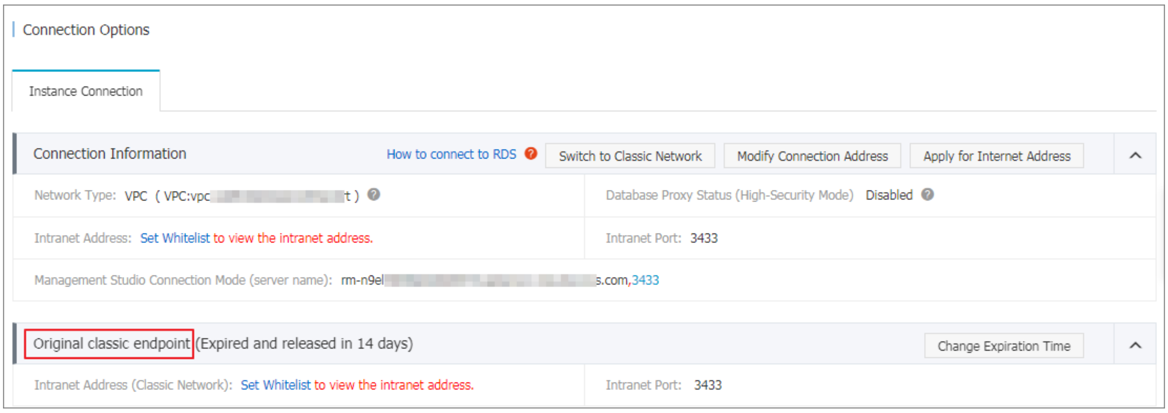
For more information about how the system seamlessly migrates an ApsaraDB RDS instance from a classic network to a VPC, see Hybrid access solution for smooth migration from classic networks to VPCs.

Note

- When you change the network type, you can specify an expiration date for the classic network endpoint. After the expiration date is reached, the classic network endpoint is automatically deleted. Before the classic network endpoint is deleted, you will receive text messages.
- If the ApsaraDB RDS instance is a shard of a DRDS instance, the DRDS instance will be disconnected from the ApsaraDB RDS instance after the network type is changed. You must manually reconnect both instances.

Change the network type by using the ApsaraDB RDS console

1. Log on to the ApsaraDB RDS console.
2. In the left-side navigation pane, click **Instances**.
3. Select the region where the ApsaraDB RDS instance is deployed.
4. Click the ID of the ApsaraDB RDS instance.
5. In the left-side navigation pane, click **Database Connection**.
6. On the **Database Connection** page, click **Switch to VPC**.
7. In the **Switch to VPC** dialog box, select the VPC and vSwitch that you want to use.
8. 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 a text message to the mobile number associated with your Alibaba Cloud account each day.
   - After the expiration date of the classic network endpoint is reached, the classic network endpoint is automatically deleted. Then, you can no longer access the ApsaraDB RDS instance through the classic network endpoint. To ensure that your services are not interrupted, set a proper expiration date. After you configure the hybrid access mode, you can change the expiration date.
9. Click **OK**.
   The **Database Connection** page displays **Reserve Original Classic Network Endpoint**.



Connection Information

Network Type: VPC (VPC:vpc[redacted]t)

Database Proxy Status (High-Security Mode) Disabled

Intranet Address: Set Whitelist to view the intranet address.

Intranet Port: 3433

Management Studio Connection Mode (server name): rm-n9el[redacted]s.com,3433

Original classic endpoint (Expired and released in 14 days)

Intranet Address (Classic Network): Set Whitelist to view the intranet address.

Intranet Port: 3433

Change the expiration date of the classic network endpoint by using the console

You can extend the expiration date of the classic network endpoint in the console before the classic network endpoint expires.

During the period in which your instance can be connected over a classic network or VPC, you can modify the expiration date of the classic network endpoint as needed. The change immediately takes effect. For example, if the classic network endpoint is set to expire on August 18, 2017 and you extend the expiration date by 14 days on August 15, 2017, the endpoint will be deleted on August 29, 2017.

1. Log on to the ApsaraDB RDS console.
2. In the left-side navigation pane, click **Instances**.
3. Select the region where the ApsaraDB RDS instance is deployed.
4. Click the ID of the ApsaraDB RDS instance.
5. In the left-side navigation pane, click **Database Connection**.
6. On the **Database Connection** page, click **Change Expiration Time**.
7. Set the expiration time and click **OK**.

Change the network type by calling the relevant API operation

For more information, see Change the network type of an ApsaraDB for RDS instance.

Change the expiration date of the classic network endpoint by calling the relevant API operation

For more information, see Change the expiration time of a classic network endpoint.

5.2.3. Change the network type of an ApsaraDB for Redis instance

This topic describes how to change the network type of an ApsaraDB for Redis instance from classic network to Virtual Private Cloud (VPC) in the console or by calling the relevant API operation. When you change the network type, you can choose to retain the classic network endpoint and specify an expiration date. After the expiration date is reached, the classic network endpoint is automatically deleted.

Prerequisites

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

- The ApsaraDB for Redis instance is deployed in a classic network.
- VPCs and vSwitches are available in the zone where the ApsaraDB for Redis instance is deployed. For more information, see Create an IPv4 VPC.

Change the network type in the console

1. Log on to the ApsaraDB for Redis console.
2. Select the region where the ApsaraDB for Redis instance is deployed.
3. Click the ID of the ApsaraDB for Redis instance.
4. On the **Instance Information** page, click **Switch to VPC**.
5. In the **Switch to VPC** panel, perform the following operations:
   i. Select the VPC and vSwitch that you want to use.

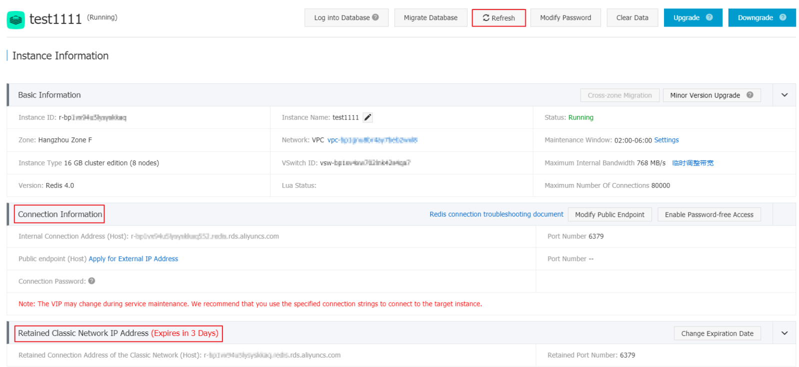
i. Select the VPC and vSwitch that you want to use.

ii. You can choose to retain the classic network endpoint and then specify an expiration date.

> **Note** After you select to retain the classic network endpoint, both the classic network endpoint and VPC endpoint are effective. ECS instances in the classic network can continue to access the ApsaraDB for Redis instance and services are not interrupted. When the classic network endpoint expires, it is automatically deleted and ECS instances can no longer access the ApsaraDB for Redis instance through the classic network endpoint.

iii. Click **OK**.

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



Instance Information

Basic Information

Instance ID: r-bp[redacted]	Instance Name: test1111	Status: Running
Zone: Hangzhou Zone F	Network: VPC vpc-[redacted]	Maintenance Window: 02:00-06:00 Settings
Instance Type 16 GB cluster edition (8 nodes)	VSwitch ID: vsw-[redacted]	Maximum Internal Bandwidth 768 MB/s 临时调整带宽
Version: Redis 4.0	Lua Status:	Maximum Number Of Connections 80000

Connection Information

Internal Connection Address (Host): r-[redacted].rds.aliyuncs.com	Port Number 6379
Public endpoint (Host) Apply for External IP Address	Port Number --
Connection Password:	

Note: The VIP may change during service maintenance. We recommend that you use the specified connection strings to connect to the target instance.

Retained Classic Network IP Address (Expires in 3 Days)

Retained Connection Address of the Classic Network (Host): r-[redacted].rds.aliyuncs.com	Retained Port Number: 6379

Modify the expiration date of the classic network endpoint in the console

After you retain the classic network endpoint, you can extend the retention period of the classic network endpoint by changing its expiration date in the console.

You can adjust the expiration date before the classic network endpoint expires. The new expiration date takes effect immediately. For example, if the classic network endpoint is about to expire on August 18, 2017 and you extend the expiration date by 14 days on August 15, 2017, the classic network endpoint is released on August 29, 2017.

1. Log on to the ApsaraDB for Redis console.
2. Select the region where the ApsaraDB for Redis instance is deployed.
3. Click the ID of the ApsaraDB for Redis instance.
4. In the **Connection Information** section, find **Retained Connection Address of the Classic Network (Host)** in the **Connection Type** column, and then click **Change Expiration Date** in the **Actions** column.
5. In the **Change Expiration Date** panel, select a new date and click **OK**.

Change the network type by calling the relevant API operation

For more information, see SwitchNetwork.

Modify the expiration date of the classic network endpoint by calling the relevant API operation

For more information, see ModifyInstanceNetExpireTime.

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

This topic describes how to switch the network type of an ApsaraDB for MongoDB instance from classic network to 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 during 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 can switch the network type, make sure that the following conditions are met:

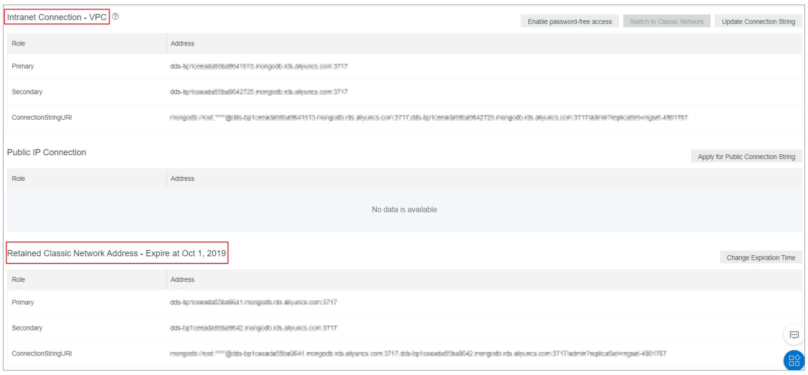
- The network type is classic network.
- The instance must be an ApsaraDB for MongoDB replica set instance.
- VPCs and vSwitches are available in the zone to which the ApsaraDB for MongoDB instance belongs. For more information, see Create an IPv4 VPC.

Switch the network type by using the console

1. Log on to the ApsaraDB for MongoDB console.
2. Find the ApsaraDB for MongoDB instance that you want to manage and click its ID.
3. In the left-side navigation pane, click **Database Connection**, and then click **Switch to VPC**.
4. In the **Create Alert** panel, perform the following steps:
   1. Select the VPC and vSwitch that you want to use.
   2. You can choose to retain the classic network endpoint and specify a retention period.

      > **Note** If you choose to retain the classic network endpoint, ECS instances in a classic network can still access the database. When the retention period expires, the classic endpoint is automatically deleted and you can no longer access the database through the classic network endpoint.

   3. Click **OK**.
5. On the Database Connection page, you can view the classic network and VPC endpoints.


Enable password-free access
Switch to Classic Network
Update Connection String
Apply for Public Connection String
Change Expiration Time

Intranet Connection - VPC

Role	Address
Primary	dds-[redacted]
Secondary	dds-[redacted]
ConnectionStringURI	[redacted]

Public IP Connection

Role	Address
No data is available	

Retained Classic Network Address - Expire at Oct 1, 2019

Role	Address
Primary	dds-[redacted]
Secondary	dds-[redacted]
ConnectionStringURI	[redacted]

Switch the network type by calling the relevant API operation

For more information about how to switch the network type by calling the relevant API operation, see

ModifyDBInstanceNetworkType.

5.3. Other services that support hybrid access

If a cloud service supports hybrid access, it can be accessed by Elastic Compute Service (ECS) instances in classic networks and ECS instances in virtual private clouds (VPCs). This topic lists the cloud services that support hybrid access in addition to ApsaraDB services. You can click the links provided in this topic to view the endpoints of different cloud services.

Storage services

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

Application services

Log Service:Obtain endpoints

Middleware

- Message Queue:Obtain endpoints

Big data

- MaxCompute: Obtain endpoints

5.4. Migrate cloud resources from a classic network to a VPC

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:

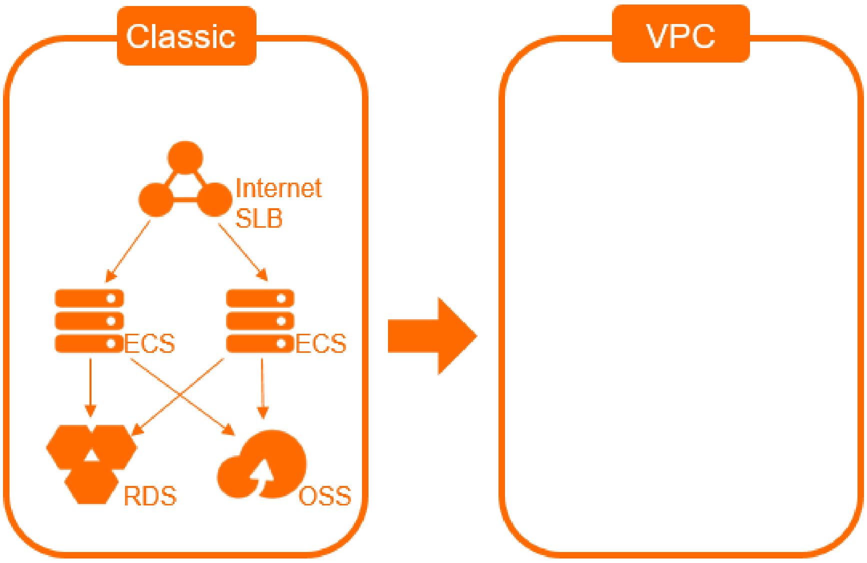
- An Alibaba Cloud account is created. If you do not have an Alibaba Cloud account, create one. For more information, see Create an Alibaba Cloud account.
- You understand the details and limits of the hybrid migration solution. For more information, see Overview.
- You are familiar with VPCs and relevant services. 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. The actual scenario may be more complex. You must assess the network architecture before you create a migration plan.

Systems to be migrated

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

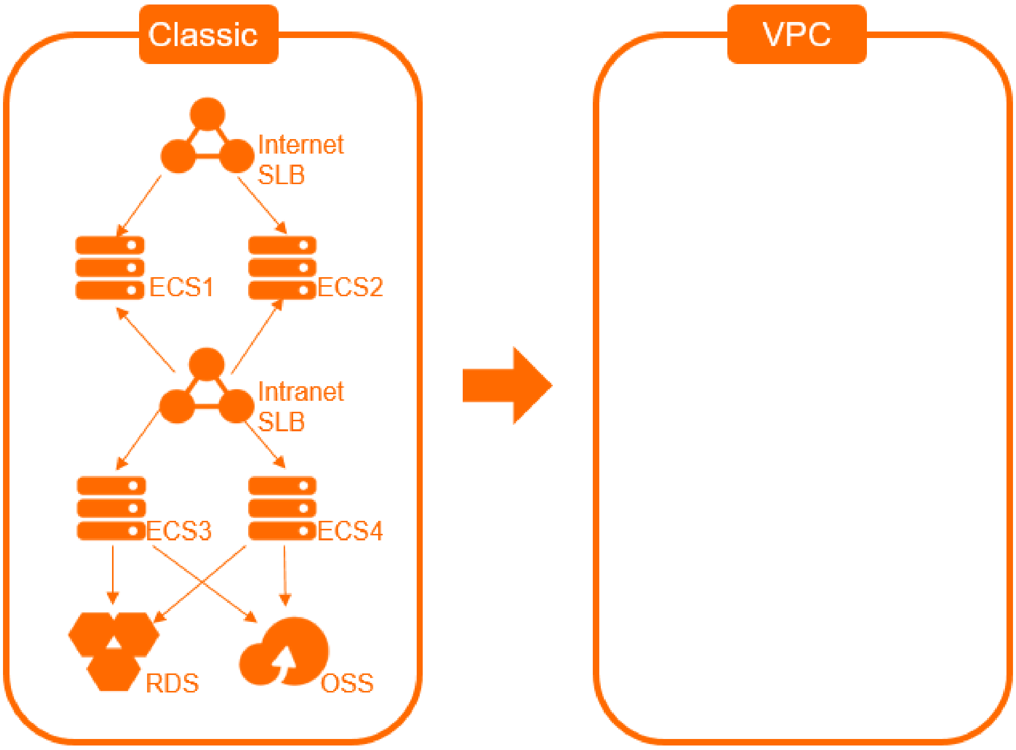
- System 1

The following figure shows System 1. This system runs in a classic network and uses Server Load Balancer (SLB), Elastic Compute Service (ECS), ApsaraDB RDS, and Object Storage Service (OSS). The Internet-facing SLB instance has 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. System 2 runs in a classic network and is more complex than system 1. The Internet-facing SLB instance is associated with ECS 1 and ECS 2. Both ECS instances are required to access an internal-facing SLB instance. The internal-facing SLB instance is associated with ECS 3 and ECS 4. Both ECS instances are required to access the ApsaraDB RDS instance and the OSS bucket.



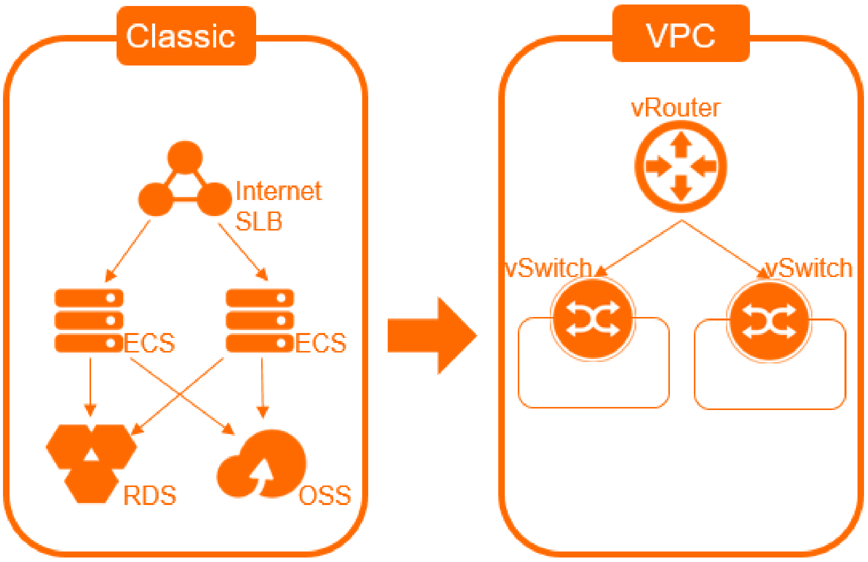
Example 1: Migrate System 1 to a VPC

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.



2. Obtain the internal endpoints of the ApsaraDB RDS instance and the OSS bucket that you want to access in the VPC.

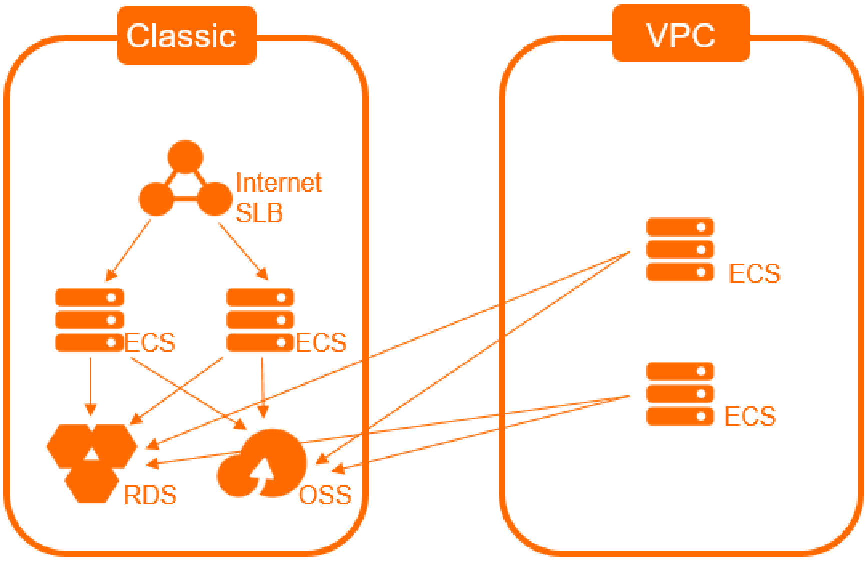
   - You can use the ApsaraDB RDS console or call an API operation to switch the network type of the ApsaraDB RDS instance to VPC and reserve the classic network endpoint. For more information, see Change the network type of an ApsaraDB RDS instance.

     After System 1 is migrated, the classic network endpoint remains unchanged. An internal endpoint that can be accessed within the VPC is added. This way, the ECS instances in the classic network can still access ApsaraDB RDS without service disruptions. When the classic network endpoint expires, it is automatically deleted and ECS instances can no longer access ApsaraDB RDS 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.

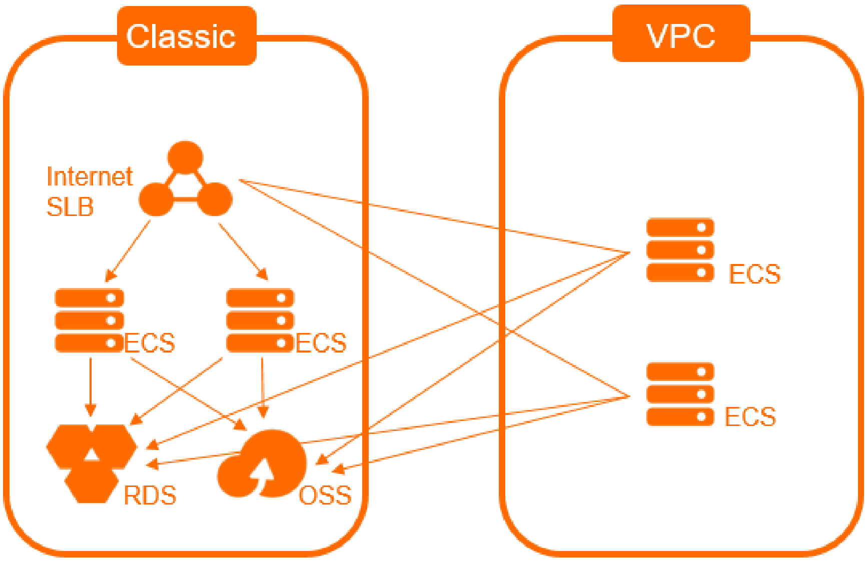
3. Create and configure two ECS instances in the VPC.

   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, test whether the ECS instances can access the OSS bucket and the ApsaraDB RDS instance.



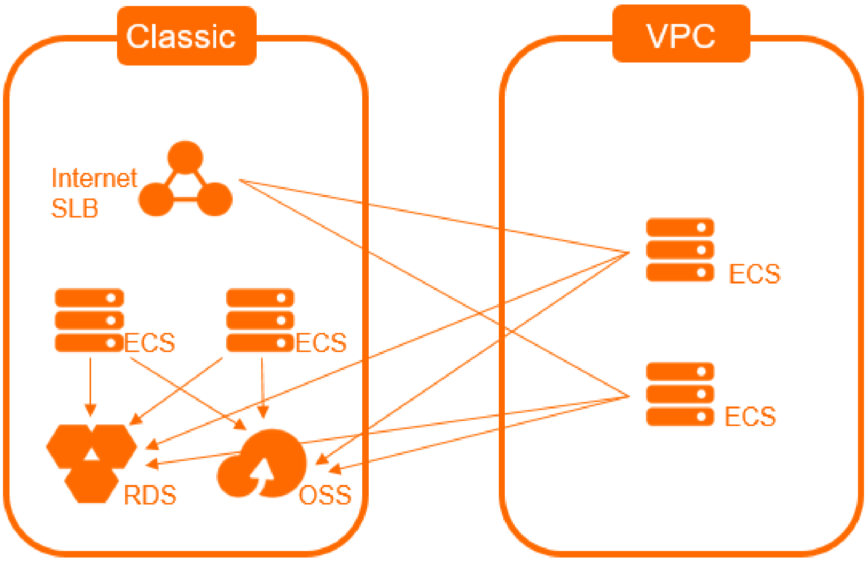
4. Specify the ECS instances in the VPC as the backend servers of the Internet-facing SLB instance.

   Add the two ECS instances in the VPC as the backend servers of the Internet-facing SLB instance. Check the health status of the ECS instances. We recommend that you set lower weights for the ECS instances. This reduces the impacts 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 Internet-facing SLB instance.

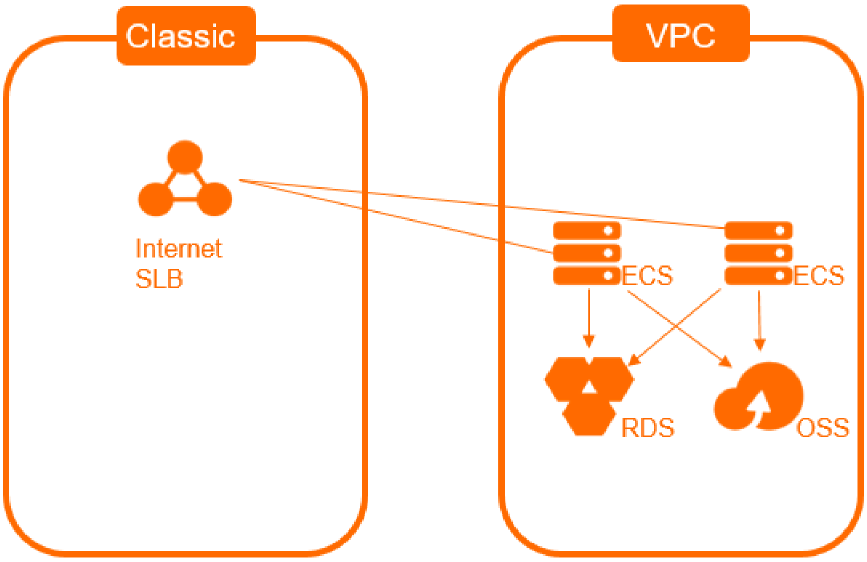
   The following figure shows how to remove the classic-network ECS instances from the backend servers of the Internet-facing SLB instance. We recommend that you set the weight of the classic-network ECS instances to 0. After the ECS instances no longer receive requests, remove them from the backend servers of the SLB instance.



6. Release the classic-network ECS instances.

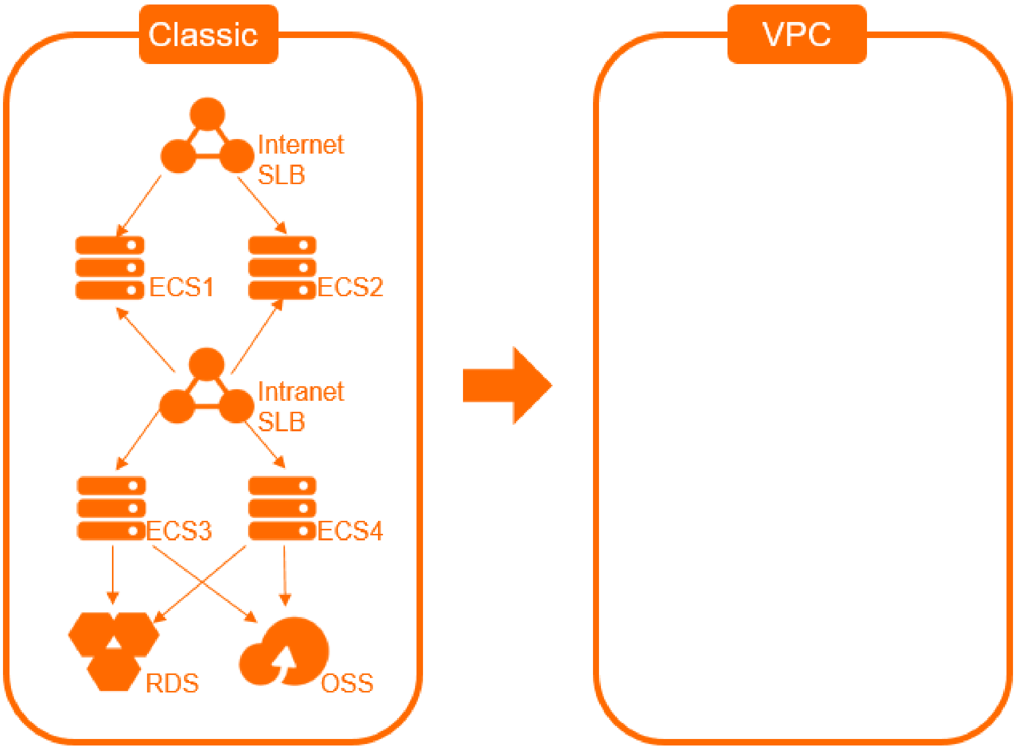
   Release the classic-network ECS instances after the system runs as expected for a specific period. The Internet-facing SLB instance supports the ECS instances in the VPC and it is not required to be migrated. Your migration is completed.

   > **Note** The classic network endpoint of the ApsaraDB RDS instance is automatically deleted when it expires.



Example 2: 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. 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.

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 ApsaraDB RDS console or call an API operation to switch the network type of the ApsaraDB RDS instance to VPC and reserve the classic network endpoint. For more information, see Change the network type of an ApsaraDB 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. This way, the ECS instances in the classic network can still access ApsaraDB RDS without service disruptions. When the classic network endpoint expires, it is automatically deleted and ECS instances can no longer access ApsaraDB RDS 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 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-facing SLB instance.

4. Configure the new 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.
5. Create an internal-facing SLB instance in the VPC to replace the internal-facing SLB instance in the classic network.
6. Configure the internal-facing SLB instance in the VPC. Specify the two ECS instances that are created in Step as backend servers.
7. Create two ECS instances in the VPC as the migration destinations of ECS 1 and ECS 2.
8. Configure the new ECS instances. Change the classic network endpoint of the internal SLB instance to the endpoint that is used in the VPC.
9. Perform Step to Step, as described in Example 1.

5.5. Migrate an ECS instance from a classic network to a VPC

ECS instances located in virtual private clouds (VPCs) are more secure and support more features, such as associating elastic IP addresses (EIPs), than those located in the classic network. This topic describes how to use a migration plan to migrate one or more ECS instances from the classic network to a VPC.

Prerequisites

The ECS instances that you want to migrate from the classic network to a VPC meet the following requirements:

- The instances do not have local disks attached. If the instances have local disks attached, submit a ticket to seek advice from Alibaba Cloud on how to migrate the instances.
- The instances have a public bandwidth higher than 0 Mbit/s. If an instance has a public IP address and a public bandwidth of 0 Mbit/s, you must upgrade the public bandwidth before you can migrate the instance. For more information, see Modify public bandwidth.
- The instances are located in one of the following regions that support the migration plan feature: China (Qingdao), China (Beijing), China (Hangzhou), China (Shanghai), China (Shenzhen), China (Hong Kong), US (Silicon Valley), and Singapore (Singapore).

> **Note** Some instances located in Hangzhou Zone C cannot be migrated from the classic network to VPCs.

Impacts of migrating an ECS instance from the classic network to a VPC

Item	Description

Item	Description
Amount of time required to migrate the instance	It takes about 15 minutes from the time the instance is stopped in the classic network until the instance is migrated and started in the VPC. **Note** After the computing and network resources of an instance are migrated, the instance is started in the VPC. If the instance is migrated across zones, the system continues to migrate disk data of the instance after the instance is started. Typically, it takes about 4 hours to migrate 100 GiB of disk data. During the migration, the I/O performance of disks degrades and snapshot- and disk-related features are not supported.
Instance state	During migration, the instance is stopped and then started again. We recommend that you schedule to migrate your instance during off-peak hours.
Network type	After the instance is migrated, its network type changes from classic network to VPC. For information about VPCs, see What is a VPC?.
Software authorization code	After the instance is migrated, its software authorization codes may change.
IP address	• The public IP address of the instance remains unchanged. **Notice** ECS instances located in VPCs do not have public network interface controllers (NICs), and use NAT devices to access the Internet. You can find only internal IP addresses inside the instances. If your applications require a public IP address visible in the instance operating system, reconsider whether to migrate your instance from the classic network to a VPC. • You can specify whether to retain the internal IP address of the instance when you create a migration plan to migrate the instance. You can also modify the internal IP address of the instance after the instance is migrated. For more information, see Modify a private IP address.
Disk name	Some ECS instances have their underlying virtualization technology upgraded when they are migrated from the classic network to VPCs. This may cause the disk names on the instances to change. On Linux instances, disks names follow a naming convention of vd?, such as vda, vdb, and vdc. • If a disk name is in the vd? format before the instance is migrated, the disk name remains unchanged after the instance is migrated. • If a disk name is in the xvd? format before the instance is migrated, the disk name is converted to the vd? format such as vda, vdb, or vdc after the instance is migrated. Alibaba Cloud updates the */etc/fstab* file for Linux instances. However, you must check whether applications are dependent on the original disk names.

Item	Description
Fee	- You are not charged for the migration. After a subscription instance is migrated from the classic network to a VPC, a new billing cycle immediately starts and the unit price of the instance type changes. An instance located in a VPC is more cost-effective than an instance with the same configurations located in the classic network. - Orders for instance renewal and configuration changes that do not take effect or are unpaid are canceled. You can renew the instance and change its configurations again.
Others	- The ID, username, and logon password of the instance remain unchanged. - If the ECS instance has been added to the vServer group of a Server Load Balancer (SLB) instance before the ECS instance is migrated, the ECS instance is not automatically associated with the SLB instance after the ECS instance is migrated. You must manually add the ECS instance to the vServer group of the SLB instance. For more information, see Modify a VServer group.

Preparations

1. Create snapshots for the disks on the ECS instances to be migrated to back up data.

   For more information, see Create a snapshot for a disk.

2. (Optional) If an ECS instance to be migrated is associated with an Alibaba Cloud database service, you must enable the hybrid access mode for the database service beforehand.

   In hybrid access mode, Alibaba Cloud database services are accessible to ECS instances regardless of whether the instances are located in the classic network or in VPCs. For more information, see Overview of the hybrid access mode of ApsaraDB.

3. (Optional) If an ECS instance to be migrated is associated with an Alibaba Cloud database service (such as ApsaraDB RDS) that provides the whitelist feature, you must add the CIDR block of the destination vSwitch to the corresponding whitelists of the database service beforehand.

   For more information, see Configure a whitelist.

4. (Optional) To ensure that services can be rapidly restored after the migration, we recommend that you configure application services to run on instance startup and monitor service availability.

5. Disable or uninstall server security software on the ECS instances to be migrated.

   > **Note** The device drivers of ECS instances are updated when the instances are migrated. You must disable or uninstall security software such as Safedog, Huweishen, and Yunsuo on the instances beforehand.

6. Reserve at least 500 MiB of free space on the system disk of each ECS instance to be migrated.

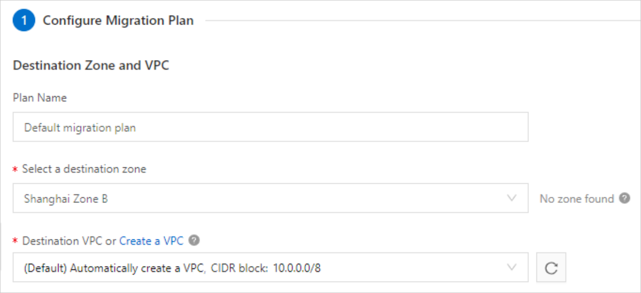
7. Make sure that the destination vSwitch has sufficient internal IP addresses available. The number of the available internal IP addresses must be greater than that of ECS instances to be migrated.

Step 1: Create a migration plan

1.
2.

3.
4. Click **Create Migration Plan**.
5. In the **Configure Migration Plan** step, configure parameters in different sections and then click **Next**.

   i. Configure parameters in the Destination Zone and VPC section.



1 Configure Migration Plan

Destination Zone and VPC

Plan Name

Default migration plan

* Select a destination zone

Shanghai Zone B

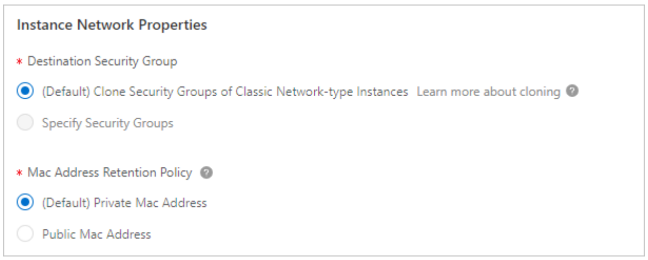
No zone found

* Destination VPC or Create a VPC

(Default) Automatically create a VPC, CIDR block: 10.0.0.0/8

Parameter	Description
Plan Name	Enter a name for the migration plan.
Select a destination zone	Select a destination zone from the drop-down list. The available zones are automatically planned based on resource availability. If you want to specify a zone that is not in the drop-down list, submit a ticket. **Note** Only a single zone can be specified in each migration plan. If you want to migrate multiple ECS instances to different zones, you must create multiple migration plans.
Destination VPC or Create a VPC	Select a destination VPC from the drop-down list. The CIDR block of the selected destination VPC determines whether to retain the internal IP addresses of the ECS instances from the classic network. ■ If you want to retain the internal IP addresses of the ECS instances, you must select a VPC that is associated with the 10.0.0.0/8 CIDR block. You can select the default option or a VPC that you created. ■ If you have not created VPCs that are associated with the 10.0.0.0/8 CIDR block, select **(Default) Automatically create a VPC, CIDR block: 10.0.0.0/8** for the system to create a VPC that is associated with the 10.0.0.0/8 CIDR block. ■ If you have created a VPC that is associated with the 10.0.0.0/8 CIDR block, select the VPC. ■ If you do not want to retain the internal IP addresses of the ECS instances, you must select a VPC that is associated with a CIDR block other than 10.0.0.0/8.

   ii. Configure parameters in the Instance Network Properties section.



Instance Network Properties

* Destination Security Group

● (Default) Clone Security Groups of Classic Network-type Instances Learn more about cloning

○ Specify Security Groups

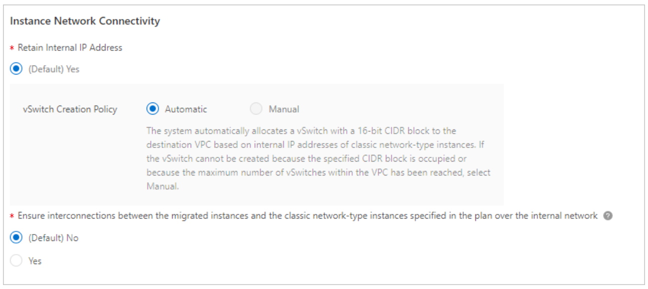
* Mac Address Retention Policy

● (Default) Private Mac Address

○ Public Mac Address

Parameter	Description
Destination Security Group	Specify destination security groups for the ECS instances from the classic network. Valid values: ■ **(Default) Clone Security Groups of Classic Network-type Instances**: The security groups of the ECS instances are automatically cloned from the classic network to the destination VPC. The rules in the new security groups (clone security groups) in the VPC are the same as those in the original security groups in the classic network. If you set **Destination VPC or Create a VPC** to **(Default) Automatically create a VPC, CIDR block: 10.0.0.0/8**, Destination Security Group is automatically set to (Default) Clone Security Groups of Classic Network-type Instances and cannot be modified. **Note** If a security group contains rules in which other security groups are configured as sources or destinations for traffic, the security group cannot be cloned. ■ **Specify Security Groups**: Select one or more existing security groups from the drop-down list. **Note** Improper security group settings affect the connectivity of your ECS instances. Make sure that your security group rules meet your connectivity requirements.
Mac Address Retention Policy	Specify which MAC address to retain for the ECS instances from the classic network. In the classic network, if an ECS instance is assigned a public IP address, the instance has a public MAC address and a private MAC address. In a VPC, each ECS instance has only a private MAC address and can have its internal IP address mapped by a NAT device to a public IP address for Internet access. You can select **(Default) Private Mac Address** or **Public Mac Address** based on your needs. ■ If your business system is associated with a MAC address, for example, if your software is associated with a MAC address for registration, retain the associated MAC address. ■ If your business system is not associated with a MAC address, select (Default) Private Mac Address or Public Mac Address.

iii. Configure parameters in the Instance Network Connectivity section.



Instance Network Connectivity

* Retain Internal IP Address

● (Default) Yes

vSwitch Creation Policy ● Automatic ○ Manual

The system automatically allocates a vSwitch with a 16-bit CIDR block to the destination VPC based on internal IP addresses of classic network-type instances. If the vSwitch cannot be created because the specified CIDR block is occupied or because the maximum number of vSwitches within the VPC has been reached, select Manual.

* Ensure interconnections between the migrated instances and the classic network-type instances specified in the plan over the internal network

● (Default) No

○ Yes

Parameter	Description

Parameter	Description
Retain Internal IP Address	Specify whether to retain the internal IP addresses of the ECS instances from the classic network. If you specify to retain the internal IP addresses of the ECS instances, you must specify how to create a vSwitch. If you specify not to retain the internal IP addresses of the ECS instances, you must select a vSwitch from the drop-down list. ■ **(Default) Yes**: retains the internal IP addresses of the ECS instances from the classic network. If (Default) Yes is selected, you must continue to specify **vSwitch Creation Policy**. 　■ If **vSwitch Creation Policy** is set to **Automatic**, a vSwitch is automatically created and associated with a CIDR block based on the internal IP addresses of the ECS instances. Make sure that the CIDR block that corresponds to the internal IP addresses of the ECS instances is not used. Otherwise, the vSwitch cannot be created. 　**Note** If you set **Destination VPC or Create a VPC** to **(Default) Automatically create a VPC, CIDR block: 10.0.0.0/8**, Retain Internal IP Address is automatically set to (Default) Yes, and **vSwitch Creation Policy** is automatically set to **Automatic** and cannot be modified. 　■ If **vSwitch Creation Policy** is set to **Manual**, you must manually create a vSwitch in the specified destination zone based on the internal IP addresses of the ECS instances from the classic network. 　**Note** You can set **vSwitch Creation Policy** to **Manual** only when you select a user-created VPC that is associated with the 10.0.0.0/8 CIDR block for **Destination VPC or Create a VPC**. ■ **No**: does not retain the internal IP addresses of the ECS instances. You must select a vSwitch from the drop-down list. **Note** If you cannot find the vSwitches that you created in the drop-down list, it may be because that the vSwitches are not located in the specified destination zone. Create a vSwitch in the destination zone. For more information, see Work with vSwitches.

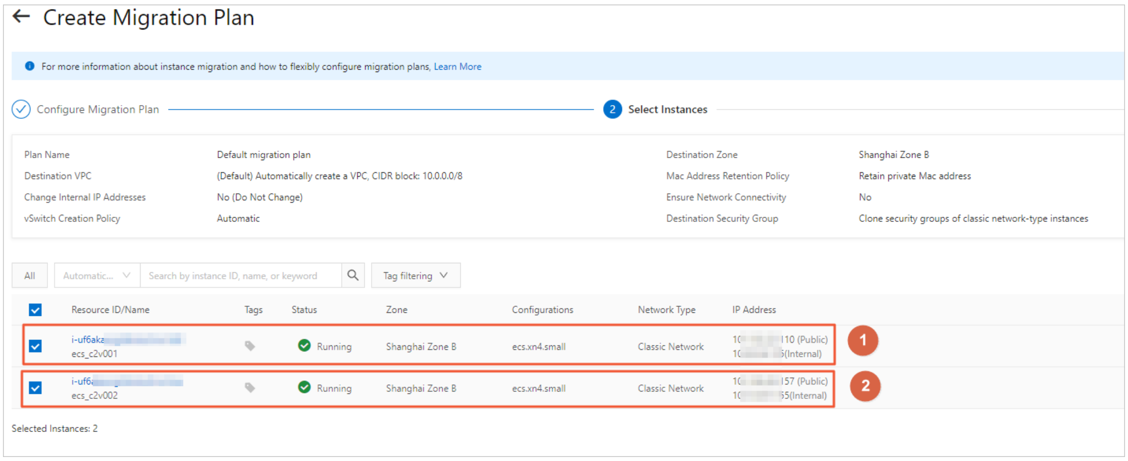
Parameter	Description
Ensure interconnections between the migrated instances and the classic network-type instances specified in the plan over the internal network	Specify whether to allow mutual access over the internal network between migrated and unmigrated instances that are included in this migration plan. Configure this parameter based on the value of Retain Internal IP Address: (Default) Yes or No. ■ (Default) Yes: 　■ If you do not want to allow mutual access over the internal network between migrated and unmigrated instances that are included in this migration plan, select **(Default) No**. 　■ If you want to allow mutual access over the internal network between migrated and unmigrated instances that are included in this migration plan, select **Yes**. Then, in the **Select Instances** step, select all ECS instances in the classic network that require mutual access over the internal network. You can schedule different migration times for these instances to control the order in which to migrate them. 　**Note** ECS instances in the classic network that are not included in this migration plan cannot communicate with the ECS instances that are migrated to the specified VPC. After this migration plan is created, ECS instances cannot be added to or removed from it. ■ No: 　■ If you do not want to allow mutual access over the internal network between migrated and unmigrated instances that are included in this migration plan, proceed to the Select Instances step. 　■ If you want to allow mutual access over the internal network between migrated and unmigrated instances that are included in this migration plan, configure ClassicLink to link these instances to the specified VPC before you migrate them. For more information, see Connect a classic network to a VPC.

6. In the **Select Instances** step, select ECS instance and click **Next**.

   If you set **Retain Internal IP Address** to **(Default) Yes** and specify to allow mutual access over the internal network between migrated and unmigrated instances that are included in the migration plan, you must select all ECS instances in the classic network that require mutual access over the internal network. You can schedule different migration times for these instances to control the order in which to migrate them.

   Note ECS instances in the classic network that are not included in this migration plan cannot communicate with the ECS instances that are migrated to the specified VPC. After this migration plan is created, ECS instances cannot be added to or removed from it.

In the following figure, the ① section shows the instances that you want to migrate first, and the ② section shows the instances that you want to migrate afterward.



← Create Migration Plan

For more information about instance migration and how to flexibly configure migration plans, Learn More

Configure Migration Plan — 2 Select Instances

Plan Name	Default migration plan	Destination Zone	Shanghai Zone B
Destination VPC	(Default) Automatically create a VPC, CIDR block: 10.0.0.0/8	Mac Address Retention Policy	Retain private Mac address
Change Internal IP Addresses	No (Do Not Change)	Ensure Network Connectivity	No
vSwitch Creation Policy	Automatic	Destination Security Group	Clone security groups of classic network-type instances

☑	Resource ID/Name	Tags	Status	Zone	Configurations	Network Type	IP Address	
☑	i-uf6aka[redacted] ecs_c2v001		✓ Running	Shanghai Zone B	ecs.xn4.small	Classic Network	10[redacted]10 (Public) 10[redacted]5(Internal)	1
☑	i-uf6[redacted] ecs_c2v002		✓ Running	Shanghai Zone B	ecs.xn4.small	Classic Network	10[redacted]157 (Public) 10[redacted]55(Internal)	2

Selected Instances: 2

7. In the **Scheduled Migration** step, set migration times for the instances and click **Verify**.

   The instances are stopped and then started again during the migration. We recommend that you schedule to migrate your instances during off-peak hours. An individual migration time can be specified for each instance.

   - To set a migration time for only a single instance at a time, click **Schedule Migration Time** in the **Actions** column.
   - To set a migration time for multiple instances at a time, select the instances and click **Batch Schedule Migration Time**.
   - To set the migration time for all of the instances at a time, click **Set Unified Migration Time**.

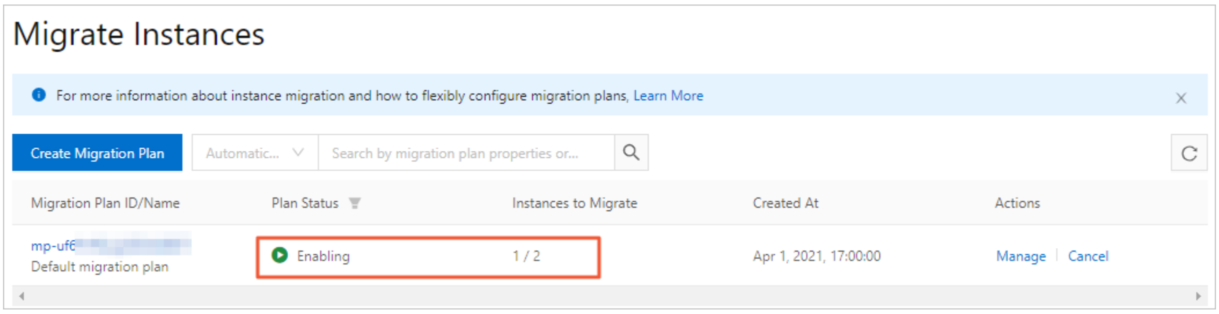
   > **Notice** Set a late migration time for ECS instances that need to remain in the classic network but require mutual access with migrated ECS instances over the internal network. Before the migration time arrives, determine whether to migrate the ECS instances from the classic network.

8. In the **Verify** dialog box, read the migration considerations and verify whether your migration plan meets the specified requirements.

   - If your migration plan meets the specified requirements, select the options and click **Confirm and Create**.
   - If your migration plan does not meet the requirements, an error message is displayed. You can perform troubleshooting based on the error message and create a migration plan again.

Step 2: Migrate the ECS instances

After the migration plan is created, the system migrates the specified ECS instances from the classic network to the destination VPC at the specified times.



Migrate Instances

For more information about instance migration and how to flexibly configure migration plans, Learn More

Migration Plan ID/Name	Plan Status	Instances to Migrate	Created At	Actions
mp-uf6[redacted] Default migration plan	Enabling	1 / 2	Apr 1, 2021, 17:00:00	Manage | Cancel

During the migration, the system performs the following operations:

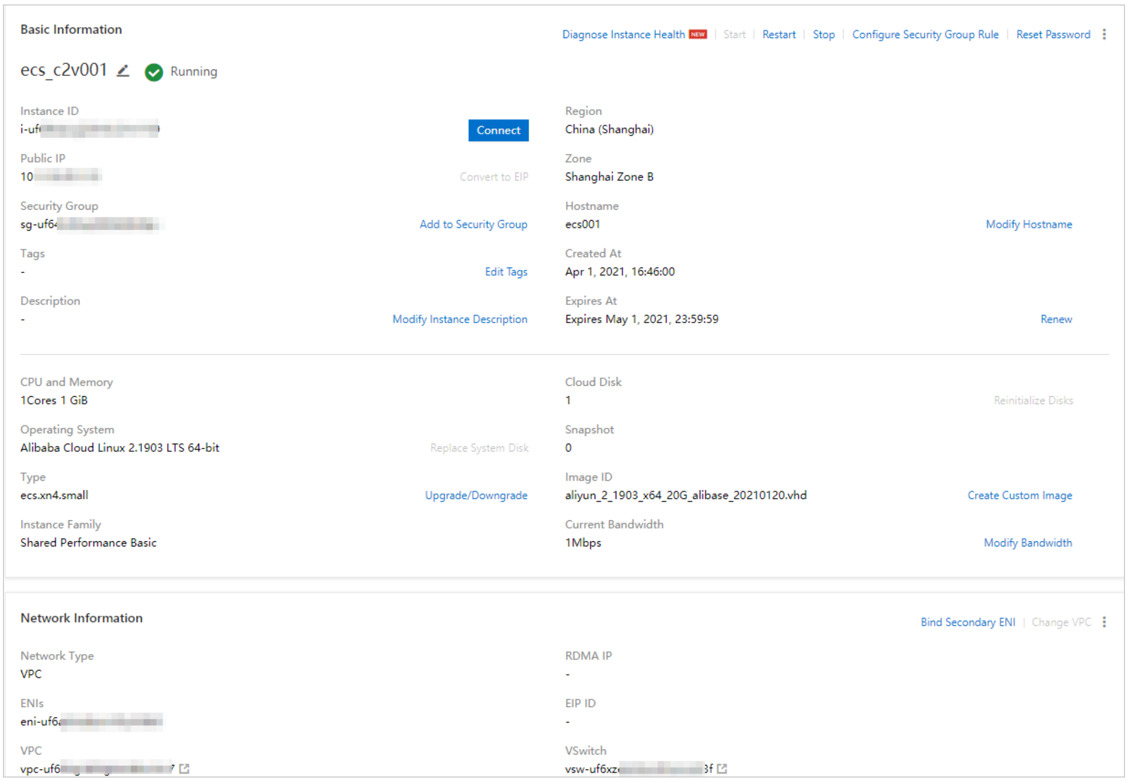
1. Stop the ECS instances to be migrated.
2. Migrate the computing and network resources of the ECS instances.
3. Start the migrated ECS instances.
4. Continue to migrate the disk data of the ECS instances.
5. Complete the migration.

> **Note** For a cross-zone migration, after the computing and network resources are migrated and the instances are started, the system continues to migrate disk data. Typically, it takes about 4 hours to migrate 100 GiB of disk data. During the migration, the I/O performance of disks degrades and snapshot- and disk-related features are not supported.

Step 3: Check the migration results

1.
2. Find the migrated ECS instances and click the ID of each of these instances.
3. On the **Instance Details** page, check whether the network type of the instance is VPC.

   If the instances are migrated to the specified VPC, their network type changes to **VPC**.



Basic Information

Diagnose Instance Health NEW | Start | Restart | Stop | Configure Security Group Rule | Reset Password

ecs_c2v001 Running

Instance ID
i-uf[redacted]

Region
China (Shanghai)

Public IP
10[redacted]

Zone
Shanghai Zone B

Security Group
sg-uf6[redacted]

Hostname
ecs001

Tags
-

Created At
Apr 1, 2021, 16:46:00

Description
-

Modify Instance Description

Expires At
Expires May 1, 2021, 23:59:59

CPU and Memory
1Cores 1 GiB

Cloud Disk
1

Operating System
Alibaba Cloud Linux 2.1903 LTS 64-bit

Snapshot
0

Type
ecs.xn4.small

Image ID
aliyun_2_1903_x64_20G_alibase_20210120.vhd

Instance Family
Shared Performance Basic

Current Bandwidth
1Mbps

Network Information

Network Type
VPC

RDMA IP
-

ENIs
eni-uf6[redacted]

EIP ID
-

VPC
vpc-uf6[redacted]

VSwitch
vsw-uf6x[redacted]3f

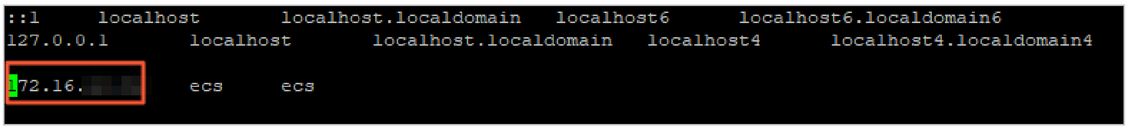
4. Check the internal network and business runtime environments.

Scenario	Migration plan	What to do next
Migrate all ECS instances from the classic network to a VPC	○ Set **Destination VPC or Create a VPC** to **(Default) Automatically create a VPC, CIDR block: 10.0.0.0/8**. ○ Set **Ensure interconnections between the migrated instances and the classic network-type instances specified in the plan over the internal network** to **Yes**.	Check whether your business system runs normally.
Migrate some ECS instances to a VPC and retain other ECS instances in the classic network	○ Set **Destination VPC or Create a VPC** to **(Default) Automatically create a VPC, CIDR block: 10.0.0.0/8**. ○ Set **Ensure interconnections between the migrated instances and the classic network-type instances specified in the plan over the internal network** to **Yes**.	Check whether your business system runs normally.

Scenario	Migration plan	What to do next
Other scenario	Set **Destination VPC or Create a VPC** to a VPC that is associated with a CIDR block other than 10.0.0.0/8.	i. Check network connectivity. ii. In this scenario, Retain Internal IP Address cannot be set to No. If your business is connected by using internal IP addresses, you must configure new internal IP addresses. iii. Check whether your business system runs normally.

Post-migration considerations

1. If an ECS instance runs a Linux operating system and is assigned a different internal IP address after the instance is migrated, you must modify the */etc/hosts* file of the instance.



```
::1     localhost       localhost.localdomain   localhost6      localhost6.localdomain6
127.0.0.1       localhost       localhost.localdomain   localhost4      localhost4.localdomain4

172.16.[redacted]       ecs     ecs
```

   i. Run the `vi /etc/hosts` command to open the hosts file.

   ii. Press the */*key to enter the edit mode.

   iii. Change the original internal IP address to the new internal IP address for the instance.

   iv. Press the *Esc* key to exit the edit mode.

   v. Enter *:wq* and press the Enter key.

2. If you have set Retain Internal IP Address to No in the migration plan, remove the internal IP addresses that are no longer used from the whitelists of other cloud services after the migration,

   such as AparaDB RDS, SLB, Object Storage Service (OSS), and Container Service for Kubernetes.

3. If an instance is migrated across zones, its connectivity with other Alibaba Cloud services such as ApsaraDB RDS, ApsaraDB for Redis, and ApsaraDB for MongoDB may be affected. Adjust application configurations in a timely manner. For example, migrate the corresponding RDS instances to the same zone as the ECS instance to ensure connectivity.

   For more information, see Migrate an ApsaraDB RDS for MySQL instance across zones in the same region.

4. If you have not restarted or upgraded the kernel of an instance for an extended period of time, problems may occur after the instance is migrated. For example, a file system check (fsck) may be performed, configuration changes may become invalid, and the instance may be unable to start.

5. (Optional) Software authorization codes change because NICs are deleted.

   If software is associated with a MAC address on your ECS instance and the software vendor approves the migration certificate issued by Alibaba Cloud, you can re-authorize the instance to use the software. If an error occurs, you must modify the configurations or roll back the instance.

6. (Optional) If you have not restarted an ECS instance for an extended period of time or if you have not restarted an instance after its kernel is upgraded, the system checks the file systems of the

instance and updates the configurations of the instance when the instance is restarted. If your ECS instance cannot be started, Submit a ticket in a timely manner to contact Alibaba Cloud.

FAQ

- Why am I unable to open websites, use services, or read data from or write data to databases on an instance after the instance is migrated from the classic network to a VPC?

  This may be because traffic is not allowed on the required communication ports in the new security groups of your instance. We recommend that you clone the original security groups. For more information, see Clone a security group.

- After an instance is migrated, some software cannot be used and I am prompted that the authorization code is expired or invalid or that no authorization code exists for the software. Why?

  This issue may occur due to one of the following reasons:

  - The software vendor has not approved the migration certificate issued by Alibaba Cloud. We recommend that you contact the software vendor or channel partner to submit a verification form for re-authorization.
  - The software was associated with a MAC address to register to your instance. Some software is registered to a valid environment by associating MAC addresses. After an ECS instance is migrated to a VPC, only the public or private MAC address of the instance is retained. If the MAC address with which a piece of software was associated to register is deleted, an authorization error occurs. We recommend that you contact the software vendor to check whether the software was associated with a MAC address to register to your instance. If yes, you must re-associate the MAC address of the instance with the software. For more information, see Overview.

- Why am I no longer able to use the FTP service on an instance after the instance is migrated?

  After your ECS instance is migrated, its public NIC is deleted and the FTP service becomes unavailable. We recommend that you perform the following operations:

  i. Convert the system-assigned public IP address of an instance that is located in a VPC to an EIP.

  ii. Associate an EIP with a secondary ENI in cut-through mode.

  > ? **Note** Some retired instance types and entry-level instance types of the previous generation do not support ENIs. If the instance type of your instance does not support ENIs, upgrade the instance to an instance type that supports ENIs before you perform the preceding operations. For more information, see Overview of instance configuration changes.

- I cannot find data disks on some Windows instances after the instances are migrated. What do I do?

  After some Windows instances are migrated, the disks attached to them go offline. We recommend that you perform the following steps to configure the disks to automatically go back online. For more information, see Methods for processing offline disks on Windows ECS instances.

  i. Log on to the ECS console.

  ii. In the left-side navigation pane, choose **Maintenance & Monitoring > ECS Cloud Assistant**.

  iii. Click **Create or Run Command** to create and run a Cloud Assistant command.

  In the Create Command panel, configure parameters described in the following table. For the parameters that are not described in the table, accept the default values. For more information, see Immediate execution.

Parameter	Description
Command Type	PowerShell
Command	`@("san policy=onlineall") |diskpart`
Select Instances	Select one or more Windows instances.

iv. Click **Execute and Save**.

- Why am I unable to transfer files to or from an instance over FTP after the instance is migrated from the classic network to a VPC?

  ECS instances in the classic network have both public and private NICs, whereas ECS instances in VPCs have only ENIs, which are private NICs. If your applications are configured to recognize only public IP addresses, you must reconfigure the applications.

  Most FTP clients access FTP servers in passive mode. In passive mode, FTP servers must communicate their IP addresses to FTP clients. In VPCs, public IP addresses cannot be recognized and FTP servers send their internal IP addresses to FTP clients. When the clients use the internal IP addresses to access the servers, errors occur.

  When you use an ECS instance located in a VPC as an FTP server, we recommend that you communicate the public IP address of the instance to the FTP server program. The procedures to communicate the public IP addresses of ECS instances vary based on the types of FTP server programs. Find a procedure that is suitable for your FTP server program. In the following example, vsftpd is used. Open the configuration file of vsftpd and add the following content to the file:

  ```
  listen_ipv6=NO pasv_address=<PublicIP>
  ```

  Note Replace *<PublicIP>* with the system-assigned public IP address or EIP of your instance. If an EIP is associated with the instance, we recommend that you use the EIP.

References

- Change the network type from classic network to VPC
- Change the network type of an ApsaraDB RDS for MySQL instance
- Configure the hybrid access solution for an ApsaraDB RDS for MySQL instance