

# Alibaba Cloud Virtual Private Cloud

Best practices

Issue: 20190422

## 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 due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall 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 the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. 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 bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, 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 content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, 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 the Alibaba Cloud website, product programs, or content 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 contact Alibaba Cloud directly if you discover any errors in this document.



## Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 <b>Danger:</b> Resetting will result in the loss of user configuration data.
	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 <b>Warning:</b> Restarting will cause business interruption. About 10 minutes are required to restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 <b>Notice:</b> Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 <b>Note:</b> You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
<b>Bold</b>	It is used for buttons, menus, page names, and other UI elements.	Click OK.
Courier font	It is used for commands.	Run the <code>cd / d C :/ windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid Instance_ID</code>
[ ] or [a b]	It indicates that it is an optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>

Style	Description	Example
<code>{}</code> or <code>{a b}</code>	It indicates that it is a required value, and only one item can be selected.	<code>swich {stand   slave}</code>



# Contents

---

Legal disclaimer.....	I
Generic conventions.....	I
1 Plan and design VPC.....	1
2 How to choose a product to gain access to an intranet?.....	7
3 How to choose an Internet-facing product?.....	21
4 How to save the Internet cost?.....	26
5 How to use cloud products in a VPC?.....	31
6 Migrate from the classic network to VPC.....	33
6.1 Migration overview.....	33
6.2 Database hybrid access.....	35
6.2.1 Hybrid access of ApsaraDB.....	35
6.2.2 Change the network type of ApsaraDB for RDS.....	36
6.2.3 Change the network type of ApsaraDB for Redis.....	43
6.2.4 Change the network type of ApsaraDB for MongoDB.....	50
6.3 Hybrid access of other products.....	52
6.4 Example of hybrid access and hybrid adding migration.....	53



# 1 Plan and design VPC

---

Before creating VPCs and VSwitches, you must plan the quantity and CIDR blocks of VPCs and VSwitches according to specific business.

VPC (Virtual Private Cloud) is a private network dedicated to you in Alibaba Cloud. VPCs are logically isolated from other VPCs in Alibaba Cloud. More and more users use VPC because:

- Isolated network environment

Based on tunneling technology, VPC isolates the data link layer and provides an independent, isolated, and safe network for each user. Resources within a VPC can communicate with each other over the intranet, but cannot directly communicate with resources in other VPCs unless you have configured an EIP or a NAT IP.

- Controllable network configurations

You have full control over your VPC, such as specifying its IP address range and configuring route tables and network gateways, to securely and easily access resources. Additionally, you can connect a VPC to another VPC or to a local IDC network to form an on-demand network environment, which allows you to smoothly migrate applications to Alibaba Cloud and expand the network of your local IDC.

For more information, see [What is VPC](#).

To use a VPC, you must first plan a VPC network. You can start planning and designing your VPC by answering the following questions:

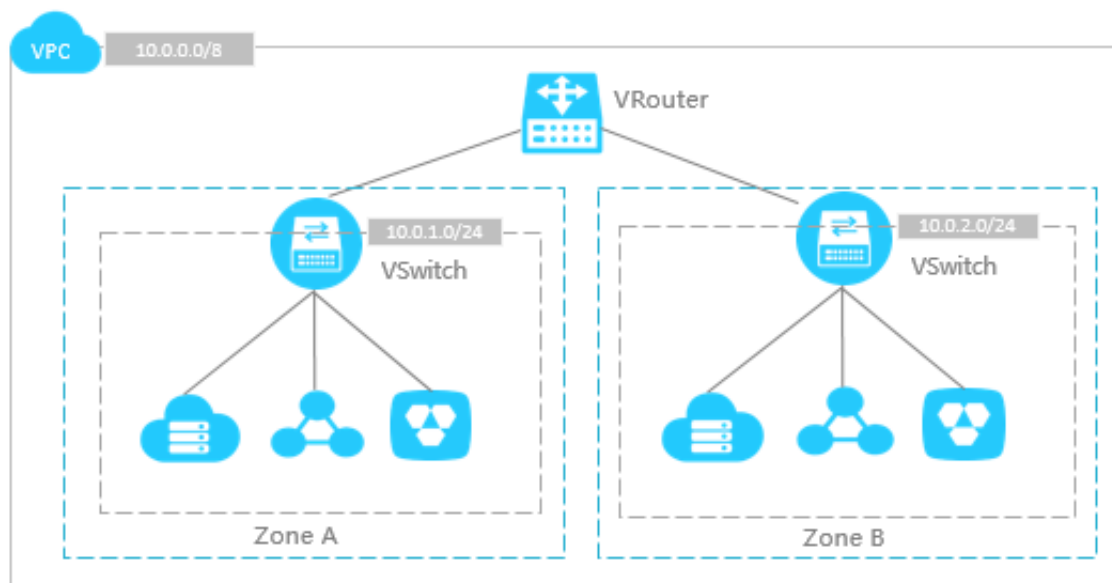
- [Q1: How many VPCs are required?](#)
- [Question 2: How many VSwitches are required?](#)
- [Question 3: How to specify the private IP address range?](#)
- [Question 4: How to specify the private IP address range when planning to connect a VPC to a local data centers or other VPCs?](#)

**Question 1: How many VPCs are required?**

- One VPC

We recommend that you create one VPC if you do not have requirements to deploy your system in multiple regions and the system is not required to be isolated by

the VPC. Currently, a VPC can accommodate up to 15,000 cloud product instances, which can basically meet your demands.



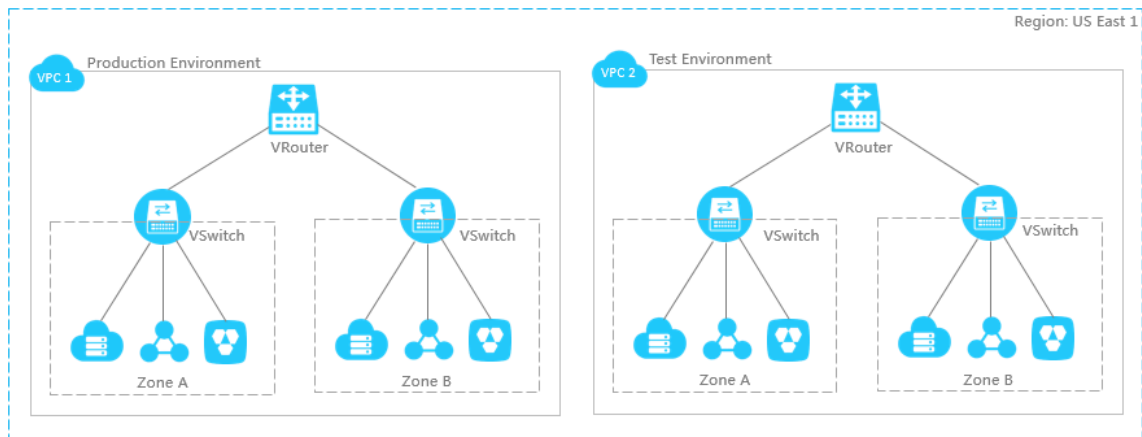
- **Multiple VPCs**

We recommend that you create multiple VPCs if you have the following requirements:

- Deploy cloud product resources in different regions

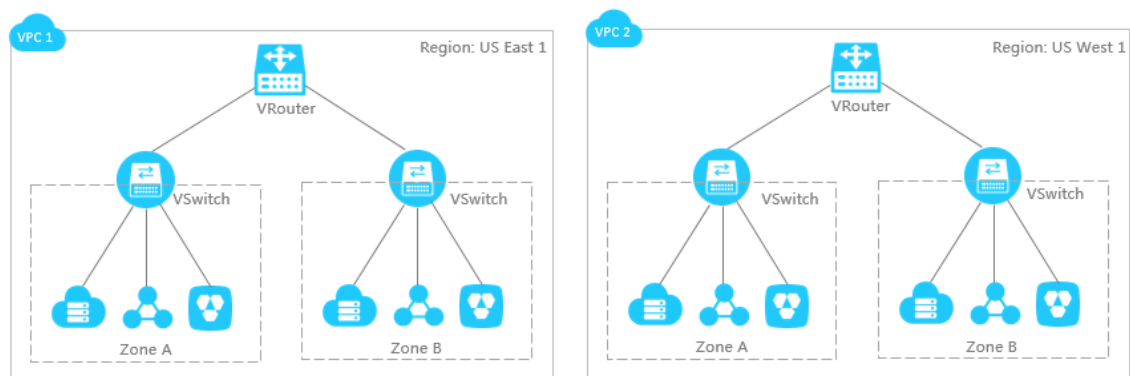
VPCs are region-specific resources that cannot be deployed across regions. If you have to deploy different systems in different regions, you have to create

multiple VPCs. You can use products such as Express Connect, VPN Gateway and CEN to connect VPCs.



- Isolate different systems

If you have to isolate your systems, such as isolate the production environment from the test environment, create multiple VPCs. Different VPCs are completely isolated.



**Question 2: How many VSwitches are required?**

In general, we recommend that you create at least two VSwitches for each VPC, and deploy these two VSwitches in two different zones (Zones are physical areas with independent power supplies and networks in a region. Zones within the same region are interconnected over the intranet). This achieves cross-region disaster tolerance.

Network latency between different zones in the same region is very small. You have to verify the network latency in your real business system. The network latency might be larger than expected due to complicated system calls or cross-zone calls. Optimize and adjust the system to find a balance between high availability and low latency.

The number of VSwitches used is related to the system size and planning. If the front-end system can be accessed by the Internet and wants to access the Internet, consider deploying different front-end systems under different VSwitches for better disaster tolerance. Then, deploy the backend system in other VSwitches.

#### Question 3: How to specify the private IP address range?

When creating VPCs and VSwitches, you have to specify the private IP address range for the VPC in the form of a Classless Inter-Domain Routing (CIDR) block.

- Private IP address range of VPC

Use 192.168.0.0/16, 172.16.0.0/12, and 10.0.0.0/8 or their subsets as the private IP address range for your VPC. Note the following when planning the private IP address range of VPC:

- If you have only one VPC and it does not have to communicate with a local data center, you are free to use any of the preceding IP address ranges or their subnets.
- If you have multiple VPCs, or you want to build a hybrid cloud composed of one or more VPCs and local data centers, we recommend that you use a subset of these standard IP address ranges as the IP address range for your VPC and make sure that the netmask is no larger than /16.
- You also need to consider whether the classic network is used when selecting a VPC CIDR block. If you plan to connect ECS instances in a classic network with a VPC, we recommend that you do not use the IP address range 10.0.0.0/8, which is also used by the classic network.

- Private IP address range of VSwitch

The IP address range of a VSwitch can be the same as the VPC that it belongs to, or a subset of the IP address range of the VPC. For example, if the IP address range of

a VPC is 192.168.0.0/16, then the IP address range of the VSwitch can be 192.168.0.0/16, or any IP address range between 192.168.0.0/17 and 192.168.0.0/29.

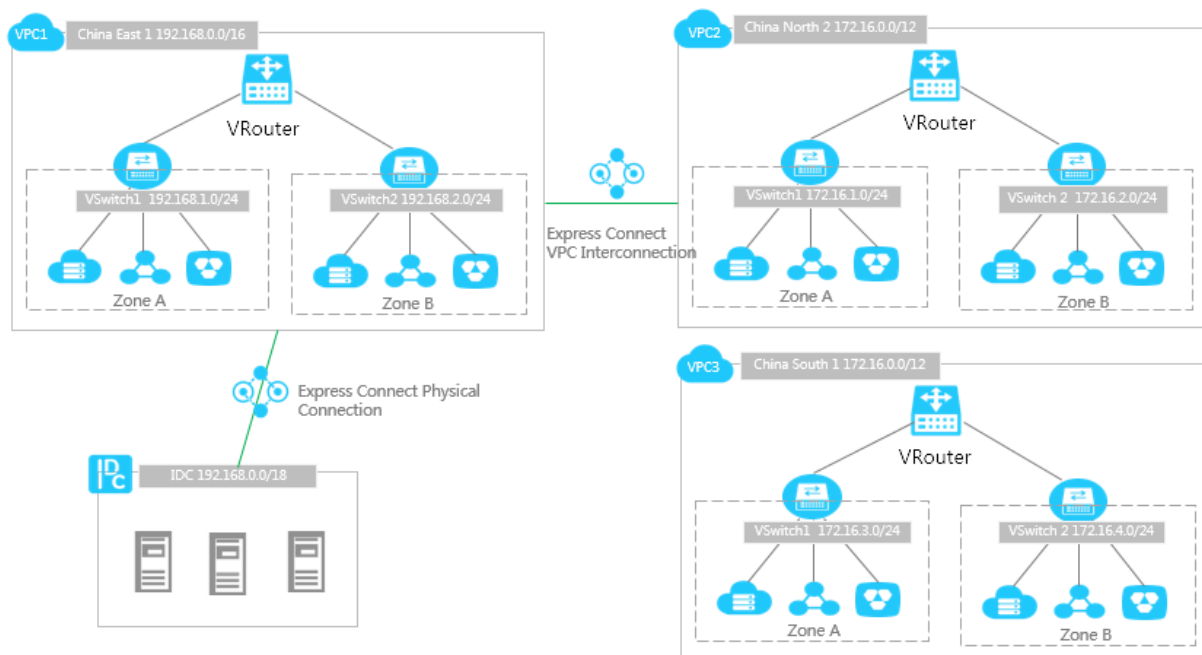
Note the following when planning the IP address range of a VSwitch:

- The allowed block size for a VSwitch is between a /16 netmask and /29 netmask, which can provide 8 to 65,536 IP addresses. Because the /16 netmask is larger enough to use with 65,532 IP addresses, while the /29 netmask is too small.
- The first and last three IP addresses of a VSwitch are reserved by the system. For example, if the CIDR block of a VSwitch is 192.168.1.0/24, IP addresses 192.168.1.0, 192.168.1.253, 192.168.1.254, and 192.168.1.255 are reserved.
- The ClassicLink function enables ECS instances in the classic network to communicate with ECS instances in VPC CIDR blocks of 192.168.0.0/16, 10.0.0.0/8, and 172.16.0.0/12. If you want to connect an ECS instance in the classic network to a VSwitch using the ClassicLink function, and the IP address range of the VPC is 10.0.0.0/8, make sure the IP address range of the VSwitch is 10.111.0.0/16. For more information, see [ClassicLink overview](#).
- Consider the number of ECS instances running in the VSwitch.

Question 4: How to specify the private IP address range when planning to connect a VPC to a local data centers or other VPCs?

If you have to connect a VPC with other VPCs or local data centers, make sure that the CIDR blocks for networks to be connect do not conflict with each other.

As shown in the following figure, you have VPC1 in China (Hangzhou), VPC2 in China (Shanghai) and VPC3 in China (Beijing). VPC1 and VPC2 can communicate with each other over the intranet through Express Connect. VPC3 has no requirements to communicate with other VPCs, but might need to communicate with VPC2 in the future. Additionally, you have a local data center in Shanghai, which is connected to VPC1 by using the physical connection of Express Connect.



When you have to connect a VPC with other VPCs or local data centers, make sure that the CIDR block for each VPC is not the same. Therefore, in this example, the CIDR blocks of VPC1 and VPC2 are different, while the CIDR block of VPC3 is the same as VPC2 because VPC3 does not need to communicate with other VPCs. However, the VSwitches in these two VPCs use completely different CIDR blocks to meet future demands for communication with each other. For communication among VPCs, the CIDR blocks of VSwitches to communicate with each other cannot be the same, but the CIDR blocks of the VPCs can be the same.

When specifying IP address ranges for VPCs requiring communication with other VPCs or local data centers, follow these rules:

- Use different IP address ranges for different VPCs. You can use the subsets of the standard IP address ranges to increase the number of available VPC CIDR blocks.
- If the first principle is not feasible, use different CIDR blocks for VSwitches of different VPCs.
- If neither of the previous conditions is met, make sure that the CIDR blocks of VSwitches requiring communications are different.

## 2 How to choose a product to gain access to an intranet?

Virtual Private Cloud (VPC) is a private network dedicated to you on Alibaba Cloud. Alibaba Cloud provides various products and services to access VPC, such as Express Connect, VPN Gateway, CEN, and Smart Access Gateway.

The following table describes various scenarios where different Alibaba Cloud products are used to establish an intranet environment connected to VPC.

<i>Connect VPCs</i>			
Product	Scenario	Benefits	Limits
<i>Cloud Enterprise Network (CEN)</i>	Connect one or more VPC networks located in different regions and under different accounts.	Easy configurations , and automatic route learning and distribution functions. Low latency and high speed. The networks (VPC /VBR) attached to a CEN instance are all connected with each other. The connection between networks in the same region is free of charge.	None
<i>Express Connect</i>	Establish a peering connection between two VPCs.	The connection between two VPCs in the same region is free of charge.	None
<i>Connect to an on-premises data center</i>			
Product	Scenario	Benefits	Limits

<a href="#">VPN Gateway</a>	Connect an on-premises data center and a VPC through an Internet-based and encrypted IPsec-VPN tunnel.	Low cost. Secure. Configurations take effect immediately.	The network latency and availability is dependent on the quality of the Internet connection .
<a href="#">Cloud Enterprise Network (CEN)</a>	Through automatic route learning and distribution, CEN can connect resources in the whole network. You only need to attach the VBR associated with the local data center to the CEN instance.	Easy configurations , and automatic route learning and distribution functions. Low latency and high speed. The networks (VPC /VBR) attached to a CEN instance are all connected with one other. Connecting networks in the same region is free of charge.	None



<a href="#">Smart Access Gateway</a>	Connect a local data center to Alibaba Cloud.	Automatic features with out-of-the-box functionality. The connection between local branches and Alibaba Cloud is through an encrypted private network and encryption authentication is implemented during the Internet transmission. Nearby access within the city through the Internet is supported. Additionally, multiple local branches can access Alibaba Cloud using the Smart Access Gateway devices with active/standby links.	None
<a href="#">Express Connect</a>	Connect an on-premises data center and a VPC through the physical connection of Express Connect .	High network quality. Large bandwidth.	Initial setup costs are high. The service activation takes a long time.

VPN software in the Alibaba Cloud Marketplace	You can buy a VPN Gateway in the Alibaba Cloud Marketplace and deploy it in the VPC so that you can connect a local data center to the VPC through an Internet-based and encrypted IPsec-VPN tunnel.	Secure. Multiple types of VPN software available to meet different network architectures. Configurations take effect immediately.	You need to manually deploy and maintain the VPN Gateway. The network latency and availability is dependent on the quality of the Internet connection .
<a href="#">Connect multiple sites</a>			
Product	Scenario	Benefits	Limits
<a href="#">VPN Gateway</a>	Establish secure communication between multiple sites through the VPN Gateway . The VPN-Hub function provides communication between sites, and between the sites and the VPC.	Low cost. Zero touch provisioning (ZTP ), and configurations take effect immediately.	None

<a href="#">Smart Access Gateway</a> + <a href="#">Express Connect</a>	After you purchase and configure Smart Access Gateway for the local branches, you can add the Smart Access Gateways to a Cloud Connect Network (CCN). Then, you can attach the CCN to a Cloud Enterprise Network (CEN) instance to enable intranet communication between the local branches.	Zero touch provisioning (ZTP). The local branches and the Alibaba Cloud are connected through an encrypted private network and encryption authentication is implemented during the Internet transmission. Nearby access within the city through the Internet is supported. Additionally, multiple local branches can access Alibaba Cloud using the Smart Access Gateway devices with active/standby links.	None
<a href="#">VPN Gateway</a>	You can use VPN Gateway and Express Connect to connect application systems and office sites around the world.	High network quality.	The network latency and availability depends on the quality of the Internet connection.
<a href="#">Remote access to a VPC</a>			
Product	Scenario	Benefits	Limits
<a href="#">VPN Gateway</a> (SSL-VPN function)	Use the SSL-VPN function to securely and quickly access a VPC from a remote client.	Low cost. Reliable. Easy to configure and deploy.	None

<b>SSL-VPN software in Alibaba Cloud Marketplace</b>	<b>After you purchase SSL-VPN software from the Alibaba Cloud Marketplace, you can deploy it in a VPC so that you can access the VPN server from a remote client.</b>	<b>Multiple types of SSL-VPN software are available.</b>	<b>High cost. Low reliability. You need to deploy and maintain the SSL-VPN software by yourself.</b>
--	---	--	--

## Connect VPCs

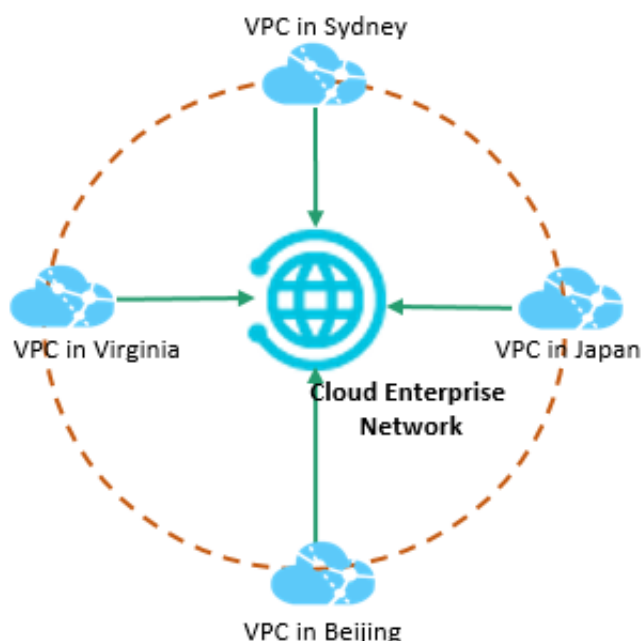
You can deploy different applications in different VPC networks to build a service network across regions. This architecture helps provide services from nearby locations, reduce network latency, achieve mutual backup and improve the reliability of the whole system.

Both Express Connect and VPN Gateway can connect VPCs in the same region or in different regions.

- CEN

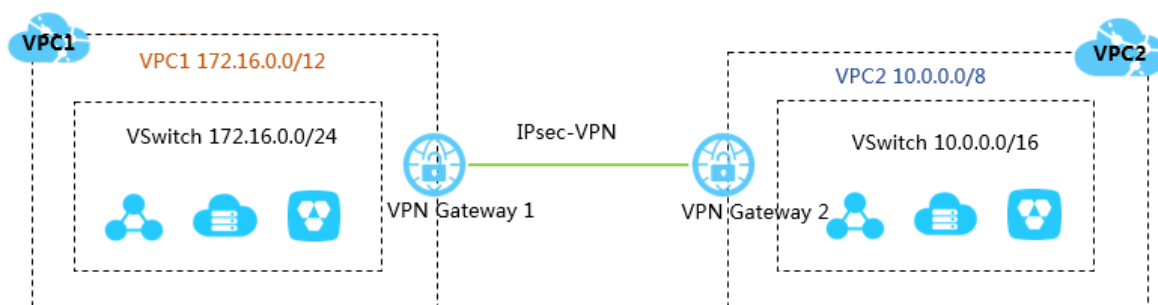
Cloud Enterprise Network (CEN) allows you to build an intranet-based communication channel between one or more VPCs. By using automatic route distribution and learning functions, CEN accelerates network convergence, improves the quality and security of cross-network communication, and interconnects resources

within the whole network, helping you achieve an interconnected network with enterprise-level scale and communication capabilities.



- VPN Gateway

VPN Gateway can connect a local data center, a local office network, or an Internet terminal to a VPC through an Internet-based, encrypted channel. You can connect VPCs located in different regions and under different accounts through VPN Gateway. By default, a VPN Gateway contains two gateway instances that form active/standby backup, so that if the active instance fails, the traffic is immediately directed to the standby instance. You can also use VPN Gateway to implement an IPsec-VPN connection between an on-premises data center and a VPC..



### Connect to an on-premises data center

You can connect a VPC to an on-premises data center to build a hybrid cloud. By using the secure and reliable connection between the VPC and the on-premises data center, and by integrating the computing, storage, network, CDN and BGP resources of

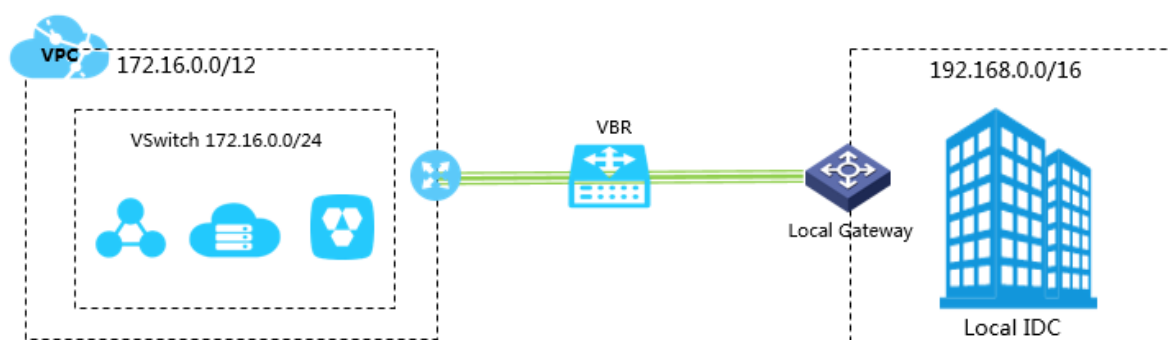
Alibaba Cloud, you can easily expand your local IT infrastructure to Alibaba Cloud to cope with changing service demands.

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

- Express Connect

Express Connect helps establish physical access. After a leased line is connected to an Alibaba Cloud access point, you can create a peer connection between a VBR and a VPC to build a hybrid cloud.

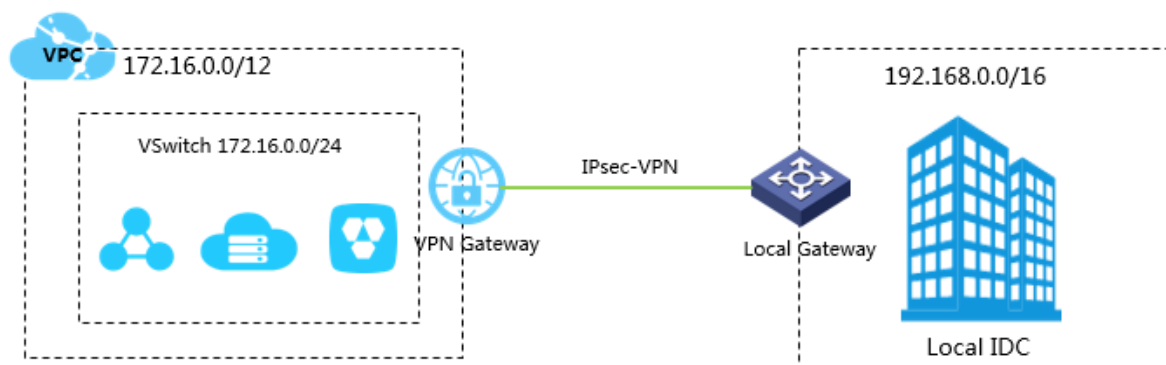
With Express Connect, the intranet connection of the leased line does not use the Internet. Therefore, compared with a traditional Internet connection, the physical connection features higher security, reliability, and speed while also providing lower network latency.



- VPN Gateway

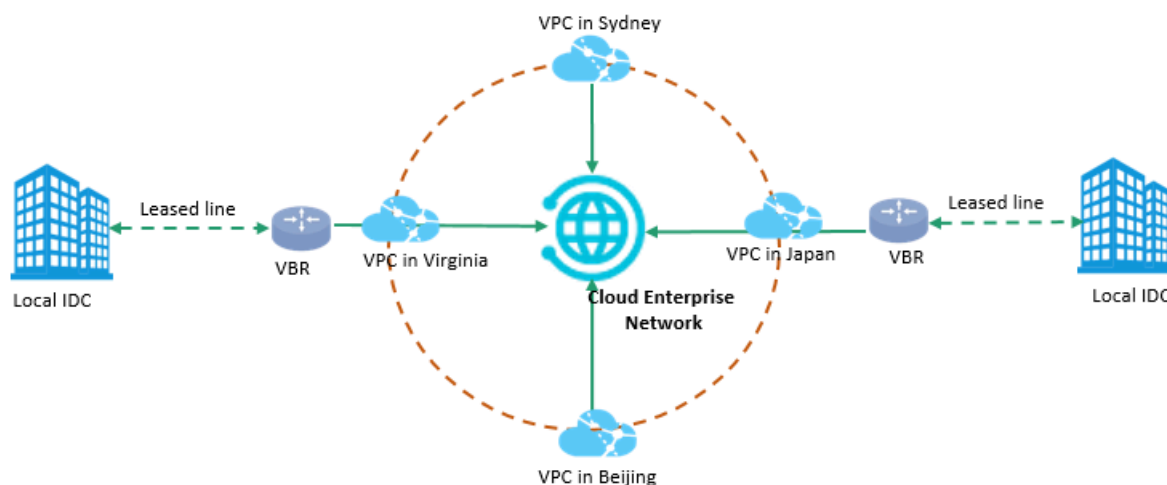
VPN Gateway can connect a local data center, a local site, an Internet terminal to a VPC in a secure and reliable way through an Internet-based and encrypted channel. VPN Gateway contains two different gateway instances which provide active/standby hot backup. The traffic is automatically distributed to the standby

node when the active node fails. You can use IPsec-VPN to connect a local data center to a VPC.



- CEN

Through automatic route distribution and learning, CEN enables you to build a secure, private, and enterprise-class interconnected network between VPCs in different regions and your local data centers. You only need to attach the VBR associated with the on-premises data center to a CEN instance, then the on-premises data center can communicate with all networks (VPCs or VBRs) attached to the CEN instance.

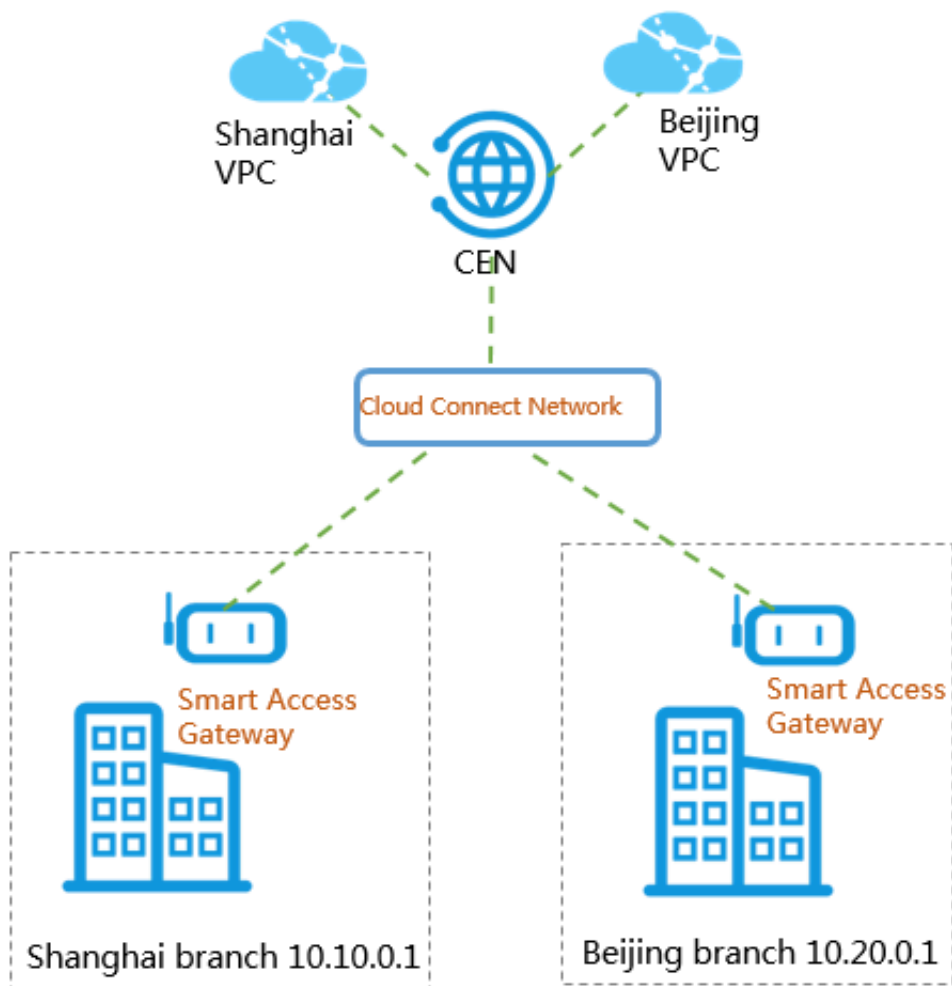


- Smart Access Gateway

Smart Access Gateway Smart Access Gateway is a device-based solution that enables the connection of on-premises data centers to Alibaba Cloud. With Smart Access Gateway, enterprises can access Alibaba Cloud through the Internet in an

encrypted manner, and experience a more intelligent, more reliable, and more secure mechanism in which to access the Alibaba Cloud ecosystem.

You can buy a Smart Access Gateway device for the local data center, and attach the CCN instance associated with the device to the CEN instance so as to connect the on-premises data center to Alibaba Cloud.

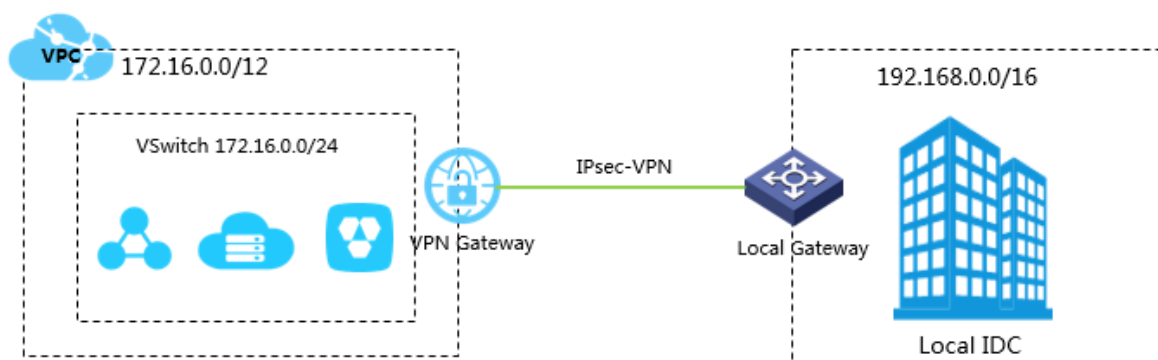


- VPN software in the Alibaba Cloud Marketplace

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 EIP to connect the VPC to the customer gateway of your on-premises data center through the Internet.



### Connect multiple sites

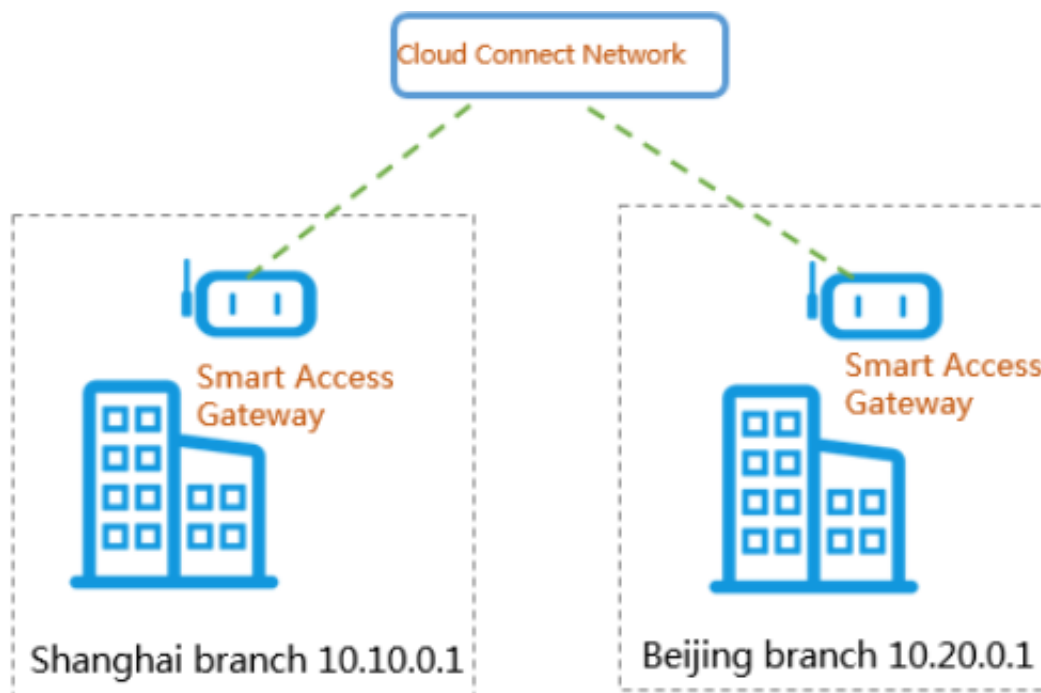
You can connect multiple sites through Smart Access Gateway or the VPN-Hub function of VPN Gateway.

- Smart Access Gateway

Smart Access Gateway is a device-based solution that enables the connection of on-premises data centers to Alibaba Cloud. With Smart Access Gateway, enterprises can access Alibaba Cloud through the Internet in an encrypted manner, and

experience a more intelligent, more reliable, and more secure mechanism in accessing the Alibaba Cloud ecosystem.

You can purchase Smart Access Gateway devices for local branches and connect the devices through CEN so that the local branches can communicate with one another.



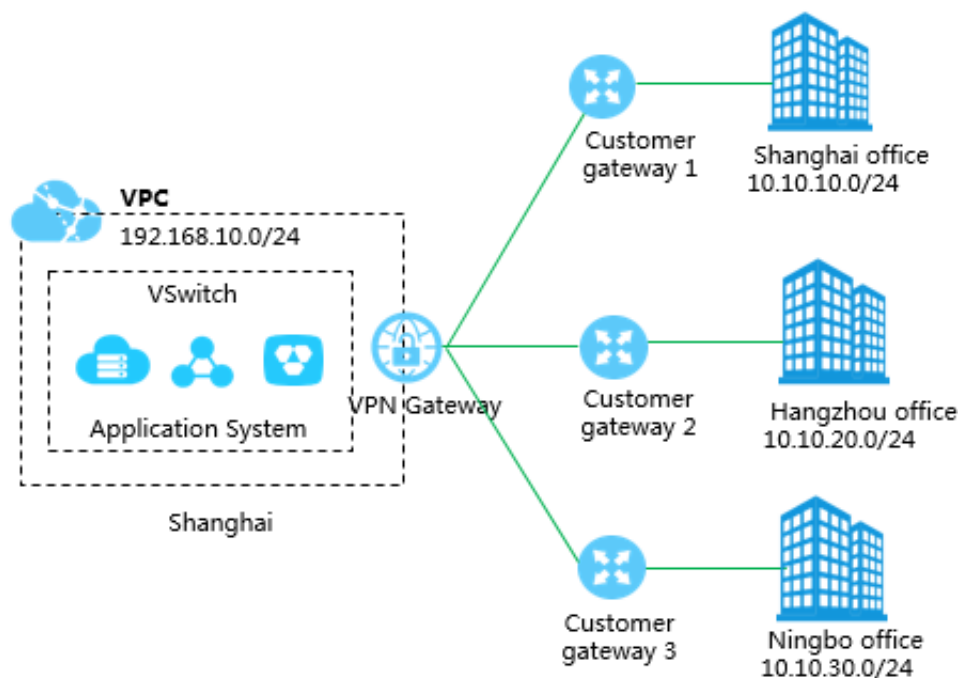
- VPN Gateway

The IPsec-VPN function of VPN Gateway provides site-to-site VPN connection. Each VPN Gateway supports 10 IPsec-VPN connections. Therefore, you can buy a VPN Gateway to connect 10 on-premises data centers or local sites in different areas.

You can establish secure communication between multiple sites through the VPN -Hub function. The sites cannot communicate with the connected VPC, but can communicate with each another. VPN-Hub allows large enterprises to establish intranet communication across different sites.

The VPN-Hub function is enabled by default. You only need to configure the IPsec-VPN connection between each office site and Alibaba Cloud. No additional configurations or payments required. A VPN Gateway supports up to 10 IPsec connections. The following figure shows an example of how to connect three office

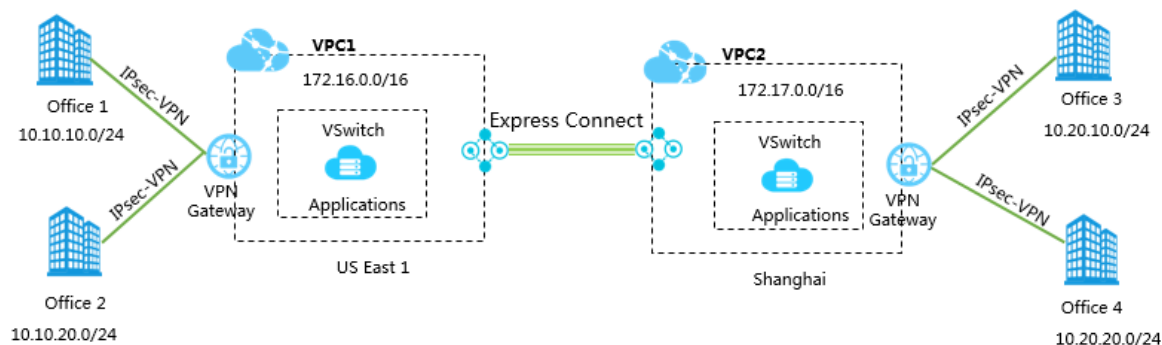
sites (Shanghai, Hangzhou, and Ningbo). In this example, you only need to create a VPN Gateway and three customer gateways, and establish three IPsec connections.



- Build a high-speed global network

You can connect application systems and office sites located around the world through VPN Gateway and Express Connect. This method features high security, high network quality and low cost.

As shown in the following figure, to connect office sites in US (Virginia) and office sites in Shanghai, you can deploy application systems in the VPC in US (Virginia) and the VPC in Shanghai, connect the VPCs through Express Connect and then connect the office sites in the two regions to the two VPCs through IPsec-VPN.



## Remote access to a VPC

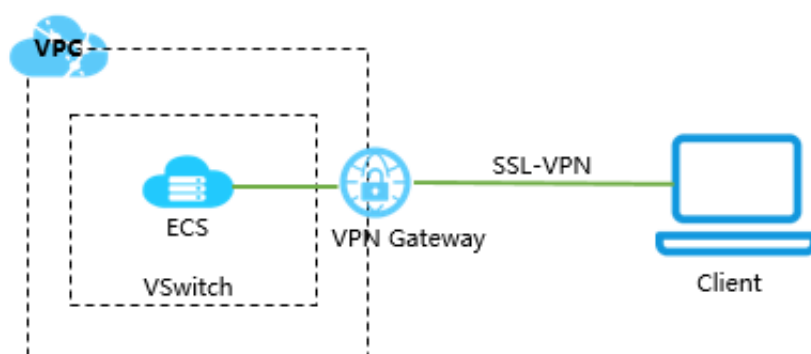
The SSL-VPN function of VPN Gateway provides site-to-site VPN connection.

Terminals can directly access a VPC without the need to configure customer gateways. You can deploy local internal applications in a VPC, and staff based in office can access the internal system through SSL-VPN. For example, local IT staff can access the VPC through the intranet, while staff that are based out of the office can access local applications in the VPC from remote sites.

Both VPN Gateway or VPN software/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 deployed in a VPC. When the deployment is complete, you only need to load the certificate in the client to initiate the connection. VPN Gateway contains two different gateway instances which provide active-standby hot backup. The traffic is automatically distributed to the standby node when the active node fails.



- SSL-VPN software from the Alibaba Cloud Marketplace

After you purchase SSL-VPN software from the Alibaba Cloud Marketplace, you can deploy it in a VPC so that you can access the VPN server from a remote client. Multiple types of SSL-VPN software are available.

## 3 How to choose an Internet-facing product?

In the VPC network, you can use EIP, NAT Gateway, Internet SLB instance and the public IP 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 of an ECS instance of the VPC network, the public IP of a NAT bandwidth package, the public IP of an Internet SLB instance, and the public IP of a VPN Gateway. To facilitate the unified management of the public IP addresses, ECS instances of the VPC network, NAT Gateways, and intranet SLB instances have supported binding EIP.



You can add EIPs to [Internet Shared Bandwidth](#) and [Data Transfer Plan](#) to flexibly cope with traffic and bandwidth fluctuation and reduce the Internet cost.

### Internet-facing products

The following table lists available Internet-facing products and the corresponding features.

Besides, to reduce the cost of Internet bandwidth and traffic, Alibaba Cloud provides [Internet Shared Bandwidth](#) and [Data Transfer Plan](#) for VPCs. You can choose different products based on your service model to reduce cost.

Product	Features	Benefits
The public IP of an ECS instance of the VPC network	The public IP allocated by Alibaba Cloud when creating an ECS instance of the VPC network. With this public IP, the ECS instance can access the Internet (SNAT) and also can be accessed from the Internet (DNAT).	You can use <a href="#">Data Transfer Plan</a> . After changing a public IP to an EIP, you can also use <a href="#">Internet Shared Bandwidth</a> .
Elastic IP Address (EIP)	With an EIP, the ECS instance can access the Internet (SNAT) and also can be accessed from the Internet (DNAT).	You can bind and unbind an EIP from an ECS instance at any time. You can use <a href="#">Internet Shared Bandwidth</a> and <a href="#">Data Transfer Plan</a> to reduce Internet cost.

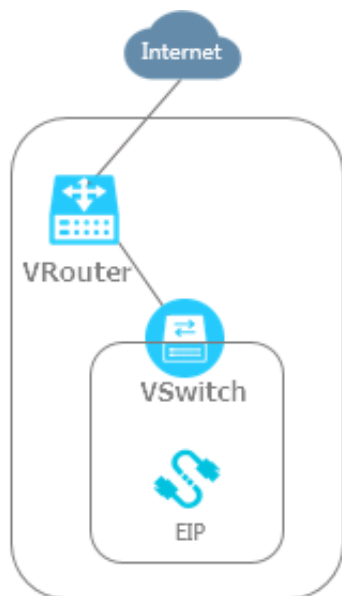
Product	Features	Benefits
NAT Gateway	<p>NAT Gateway is an enterprise-class Internet gateway, supporting multiple ECS instances accessing the Internet with one EIP (SNAT) and being accessed from the Internet (DNAT).</p> <div>  <b>Note:</b>            Compared to Server Load Balancer, NAT Gateway itself does not provide traffic balancing.         </div>	<p>Internet access for multiple ECS instances is supported. (Note that EIP does not provide this support.)</p>
Server Load Balancer	<p>Port-based load balancing, Server Load Balancer provides Layer-4 (TCP and UDP protocols) and Layer-7 (HTTP and HTTPS protocols) load balancing. Server Load Balancer can forward the client requests from the Internet to the backend ECS instances.</p> <div>  <b>Note:</b>            ECS instances without a public IP address cannot access the Internet (SNAT) through Server Load Balancer.         </div>	<p>In DNAT, Server Load Balancer supports forwarding an Internet request to multiple ECS instances.</p> <p>Server Load Balancer can increase your service capability and enhance overall availability. After binding with an EIP, you can use <a href="#">Internet Shared Bandwidth</a> and <a href="#">Data Transfer Plan</a> to reduce the Internet cost.</p>

#### Scenario 1: Provide external services

- Provide external services with a single ECS instance

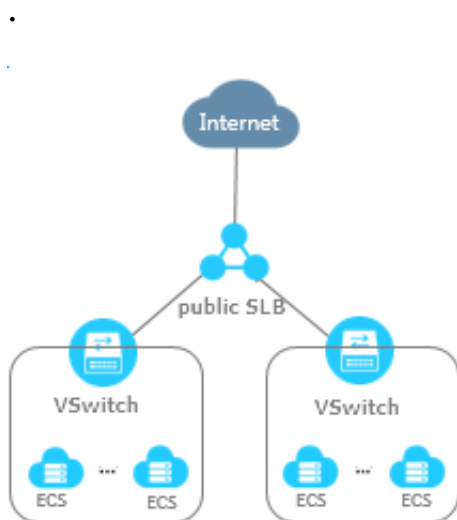
If you have only one application and the business is not large, a single ECS instance can meet your requirements. You can deploy applications, databases, and files

on this ECS instance. Then, bind an EIP to the ECS instance. Therefore, users can access the deployed application through the Internet.



- Provide external services with Layer-4

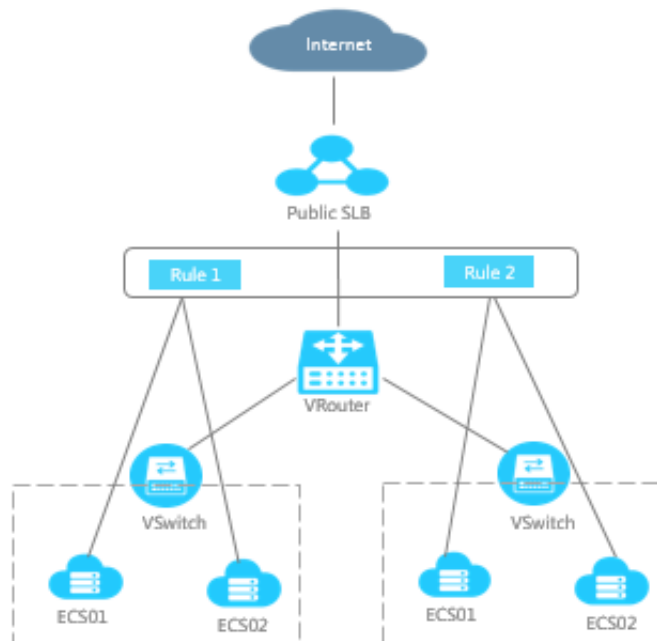
When the traffic is large, one ECS cannot support all access traffic. You must configure multiple ECS instances. In this case, you can configure an Internet SLB instance with a Layer-4 listener and add these ECS instances as the backend servers



- Provide external services with Layer-7 load balancing

In addition to the basic traffic distribution, if you want to distribute different requests to different backend servers, you can add URL forwarding rules to a Layer

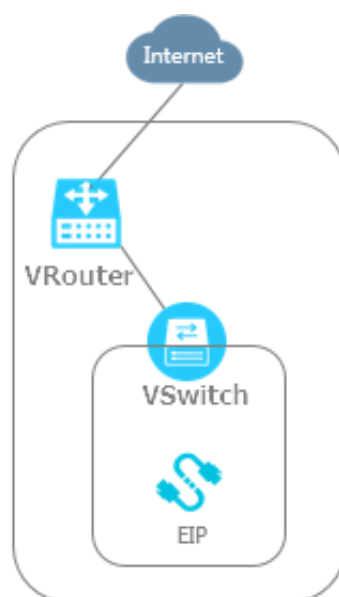
-7 listener. In this case, you can configure an Internet SLB instance with a Layer-7 listener and add these ECS instances as the backend servers.



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

- Bind an EIP

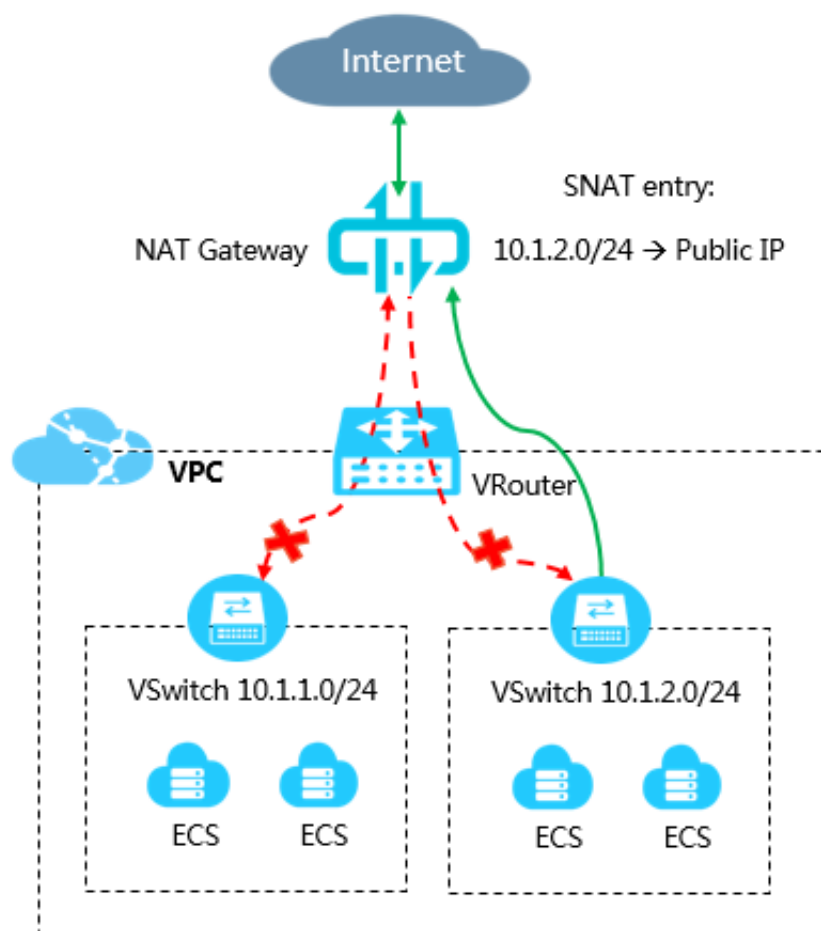
When you have fewer ECS instances, you can bind an EIP to each ECS instance. The ECS instance then can access the Internet using the EIP. Unbind the EIP from the ECS instance whenever the Internet access is not needed.





- Configure SNAT entries using NAT Gateway

If you bind an EIP to each ECS instance respectively, the management cost is high when you have many ECS instances. Additionally, users can access the ECS instance from the Internet through the EIP. In this case, you can configure an SNAT entry for the ECS instances in a VSwitch to access the Internet, but do not configure any DNAT entries. Therefore, the ECS instances can access the Internet, but users cannot access these ECS instances from the Internet, as shown in the following figure.



## 4 How to save the Internet cost?

---

You can use Internet Shared Bandwidth and Data Transfer Plan to save the Internet cost.

### Data Transfer Plan

Data Transfer Plan is a subscription Internet traffic package. It offers price lower than that of Pay-As-You-Go traffic scheme and also provides Idle-time Data Transfer Plan, greatly reducing the Internet traffic cost. Data Transfer Plan applies to ECS instances, EIPs and SLB instances that are billed by traffic.

After you purchase a Data Transfer Plan, traffic fee is automatically deducted from the plan and no additional operation is required. You can view the usage of Data Transfer Plan of different products in [Billing Management - Resource Packages](#).

This section analyzes Data Transfer Plan from the following aspects:

- How much can Data Transfer Plan save?

Data Traffic Package supports Idle-time Data Transfer Plan with lower price. Take Hong Kong as an example. The prices of Pay-As-You-Go traffic, Full-time Data Transfer Plan and Idle-time Data Transfer Plan are as follows:



Take the 5-TB Data Transfer Plan in Hong Kong region as an example. The cost comparison is as follows. You can find that Data Transfer Plan saves a lot of traffic costs.

Hong Kong 5-TB traffic	Unit price (Yuan/GB)	Total price (Yuan)	Cost saved (Yuan)	Proportion of cost saved
Pay-As-You-Go traffic	1	5120	0	0
Full-time Data Transfer Plan	0.75	3727	1393	27.2%
Idle-time Data Transfer Plan	0.51	2609	2511	49%

- What are the usage scenarios of Data Transfer Plan?

All ECS instances, EIPs and SLB instances that are billed by traffic can use Data Transfer Plan. From the perspective of saving cost, Data Transfer plan saves more costs for resources with large traffic.

- Data Transfer Plan instructions

- Data Transfer Plan has a validity period. After a plan expires, the remaining traffic in the plan cannot be used. We recommend that you choose the specification of Data Transfer Plan according to the history usage of the service system.

You can purchase a small-specification plan first and buy more in the future to avoid wasting.

- After a Data Transfer Plan is used up, traffic further used by the service is billed as Pay-As-You-Go traffic and the service is not interrupted.
- If you have purchased multiple Data Transfer Plans, traffic in the Data Transfer Plan to expire first is deducted first.

### Internet Shared Bandwidth

Internet Shared Bandwidth is an independent bandwidth product that provides high-quality multi-line BGP bandwidth and various billing methods. You can add EIPs to Internet Shared Bandwidth so that the EIPs can share the bandwidth. You can bind EIPs to ECS instances of the VPC network, NAT Gateways, and SLB instances of the VPC network, so that these products can use Internet Shared Bandwidth.

Besides, Internet Shared Bandwidth provides rich billing methods, including 95 billing, billing by fixed bandwidth, and more. Using Internet Shared Bandwidth and the rich billing methods can effectively save bandwidth cost and provide strong elastic service capability. See [Understand Internet Shared Bandwidth through one figure](#) to quickly know about Internet Shared Bandwidth.

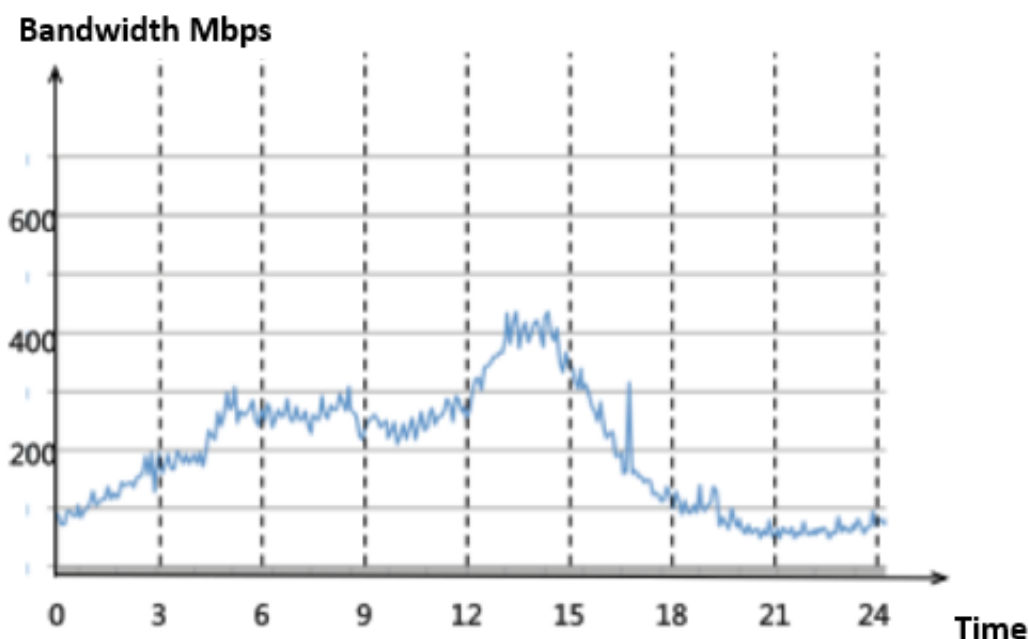


#### Note:

Internet Shared Bandwidth is an independent bandwidth product that does not contain any public IP by default. You can add EIPs to Internet Shared Bandwidth.

The bandwidth sharing function of Internet Shared Bandwidth helps you reduce Internet bandwidth cost, especially in the case of great bandwidth fluctuation. Suppose you have 10 ECS instances in Hong Kong and all the instances are bound to EIPs. If billing by bandwidth is adopted, the peak bandwidth is 100 Mbps. You must pay 3253 Yuan/day, which is the cost of 10 EIPs with the peak bandwidth of 100 Mbps, as shown in the following figure.

Traffic analysis of the 10 public IPs shows that the services differ in bandwidth fluctuation. The peak outbound bandwidth of the 10 servers is about 500 Mbps, as shown in the following figure.



Therefore, if you use Internet Shared Bandwidth, you only need to buy a 500-Mbps Internet Shared Bandwidth and the 10 ECS instances can use it. In this way, each ECS instance can use peak bandwidth five times that of the original one, and you only need to pay 1680 Yuan per day, the cost of the 500-Mbps bandwidth. Thus 1573 Yuan, that is, 50% bandwidth cost, is saved.

Basic Configuration		Current Selected																		
Region	<table border="1"> <tr> <td>China (Qingdao)</td> <td>China (Beijing)</td> <td>China (Zhangjiakou)</td> <td>China (Hohhot)</td> <td>China (Hangzhou)</td> <td>China (Shanghai)</td> </tr> <tr> <td>China (Shenzhen)</td> <td><b>Hong Kong</b></td> <td>Japan (Tokyo)</td> <td>Singapore</td> <td>Australia (Sydney)</td> <td>Malaysia (Kuala Lumpur)</td> </tr> <tr> <td>Indonesia (Jakarta)</td> <td>India (Mumbai)</td> <td>US (Virginia)</td> <td>US (Silicon Valley)</td> <td>UAE (Dubai)</td> <td>Germany (Frankfurt)</td> </tr> </table>	China (Qingdao)	China (Beijing)	China (Zhangjiakou)	China (Hohhot)	China (Hangzhou)	China (Shanghai)	China (Shenzhen)	<b>Hong Kong</b>	Japan (Tokyo)	Singapore	Australia (Sydney)	Malaysia (Kuala Lumpur)	Indonesia (Jakarta)	India (Mumbai)	US (Virginia)	US (Silicon Valley)	UAE (Dubai)	Germany (Frankfurt)	Region: Hong Kong ISP: BGP
China (Qingdao)	China (Beijing)	China (Zhangjiakou)	China (Hohhot)	China (Hangzhou)	China (Shanghai)															
China (Shenzhen)	<b>Hong Kong</b>	Japan (Tokyo)	Singapore	Australia (Sydney)	Malaysia (Kuala Lumpur)															
Indonesia (Jakarta)	India (Mumbai)	US (Virginia)	US (Silicon Valley)	UAE (Dubai)	Germany (Frankfurt)															
Billing Method	<input checked="" type="radio"/> Pay by Bandwidth	Billing Method: Pay by Bandwidth Billing Cycle: 1 hour(s)																		
Bandwidth	<input checked="" type="radio"/> 500 Mbps	Bandwidth: 500Mbps Name: - Purchase Quantity: 1 Fee: <b>CN¥70.000</b> / hour(s)																		
Name	<input type="text"/>	<input type="button" value="Buy Now"/> <input type="button" value="Add To Cart"/>																		

Internet Shared Bandwidth also provides 95 billing and "unlimited" peak bandwidth. The billing is based on the actual bandwidth usage minus the abrupt peak bandwidth. In this way, the bandwidth cost is saved and the impact of limited bandwidth on service is avoided. It is especially difficult for users with great bandwidth fluctuation to estimate a reasonable peak bandwidth. A high peak bandwidth will cause

wasting; and a low peak bandwidth will cause packet loss and further affect service development and user experience. In this case, you can choose 95 billing.

Therefore, if you have multiple EIPs and experience obvious bandwidth fluctuation, using Internet Shared Bandwidth can greatly save the cost. You can choose 95 billing for services frequently experiencing abrupt bandwidth peak, thus the impact of limited peak bandwidth on the service and the cost wasting caused by high peak bandwidth are avoided.



**Note:**

You must analyze the traffic model of the system to select an appropriate billing mode:

- For systems with stable traffic, you can choose the Subscription billing mode by bandwidth, which can save 20%-30% cost compared with Pay-As-You-Go billing by bandwidth.
- You can choose 95 billing for services frequently experiencing abrupt bandwidth peak.

## 5 How to use cloud products in a VPC?

---

Most cloud products have supported 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. ECS instances in a VPC cannot access the Internet or be accessed by the Internet, and cannot access the classic network through intranet. But Alibaba Cloud provides a lot 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 an SLB instance or 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 to use 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.

- Provide VPC endpoints

This applies to cloud products such as Log Service and Object Storage Service.

You can view help documents of the following products:

- [VPC endpoint of Log Service](#)
- [VPC endpoint of Object Storage Service](#)

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 changing the network type. 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 [Migration overview](#).



## 6 Migrate from the classic network to VPC

---

### 6.1 Migration overview

You can migrate resources deployed in the classic network to a VPC network. VPC is an isolated network environment.

#### Why migrate to VPC?

Virtual Private Cloud (VPC) is a private network dedicated to you on Alibaba Cloud. You can use Alibaba Cloud resources and products in your own VPC. The VPC network has the following advantages:

- Secure and isolated network environment

Based on tunneling technology, VPC isolates the data link layer and provides an independent, isolated, and safe network for each user. Different VPCs are completely isolated from each other.

- Controllable network configurations

You have full control over your own VPC network. You can select its IP address range, create subnets, and configure route tables and gateways. Additionally, you can connect a VPC to your local IDC network through leased lines or VPN to form an on-demand network environment, which allows you to smoothly migrate applications to Alibaba Cloud and expand the network topology of the local IDC.

#### How to migrate?

You can use the following two methods to migrate your system to a VPC network. You can use these methods independently or together to meet the demands of different scenarios:

- Hybrid addition and hybrid access migration

If your system is deployed on RDS, SLB, or other cloud products, it is recommended using this solution. It is a seamless migration solution, allowing you to migrate your system to a VPC network without interrupting your services.

With the ClassicLink function, ECS instances in the classic network can access resources in the VPC network. For more information, see [ClassicLink overview](#).

- Single ECS migration

If your application is deployed on the ECS instance, and restarting the ECS instance does not affect your system, it is recommended using this method.

#### Hybrid access and hybrid addition

The hybrid access and hybrid addition solution is a seamless migration solution. Firstly, you must create the required cloud resources (such as ECS) in the VPC network to be migrated to, and then use this method to smoothly migrate your system to the VPC. After all the resources have been migrated to VPC, release the cloud resources in the classic network to complete the whole migration process. For more information, see [Example of hybrid access and hybrid adding migration](#).

- Hybrid addition

Hybrid addition means that Server Load Balancer supports adding ECS instances of both the classic and VPC networks as backend servers to handle forwarded requests. Hybrid addition is also supported by VServer groups.

Both Internet and intranet SLB support hybrid addition.



**Note:**

If you add both classic ECS instances and VPC ECS instances to an intranet SLB instance, and configure a Layer-4 (TCP and UDP protocols) listener, you can obtain the real IP address of the client on the ECS instances of the VPC network but cannot obtain it on the classic ECS instances. There is no impact on Layer-7 listeners. You can obtain the real IP address no matter the network type of backend servers.

- Hybrid access

Cloud products like RDS and OSS support hybrid access, that is, they can be accessed by an ECS instance of the classic network and an ECS instance of the VPC network at the same time. In general, these products have two endpoints, one is used for accessing the classic network access and the other one is used for accessing the VPC network.

Note the following when using this method:

- This solution meets the migration requirements of most systems. If the ECS instances in the classic network has to communicate with the cloud resources in the VPC network, use the ClassicLink function.
- This method can only be used to migrate a system from the classic network to the VPC network.

## 6.2 Database hybrid access

### 6.2.1 Hybrid access of ApsaraDB

Hybrid access means that a database can be accessed by both an ECS instance of the classic network and an ECS instance of the VPC network. To use the hybrid access/adding method to migrate your ApsaraDB from a classic network to a VPC network, you need to change ApsaraDB to the hybrid access mode (the classic network endpoint and the VPC endpoint are reserved at the same time), thus service interruption during the migration can be avoided.

When migrating ApsaraDB to VPC, you can specify the expiration time of the classic network endpoint. The classic network endpoint is automatically released when the time is reached.

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

- Currently, the following databases support hybrid access:
  - 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 change the network type either on the console or through API. The classic network endpoint stays unchanged and a VPC endpoint will be added after the switchover. You can view the classic network endpoint and the VPC network endpoint on the console.

For the new Memcache instances, you have to do the migration using the API. Currently, after you change the network type on the console, the classic network endpoint cannot be reserved. The classic network endpoint stays unchanged

and a VPC endpoint will be added after the switchover. The console only displays the VPC network endpoint. You need to use API to view the classic network endpoint.

- Currently, the following databases have not support hybrid access:
  - 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, purchase a new instance and migrate to the new ApsaraDB for Memcache.

## 6.2.2 Change the network type of ApsaraDB for RDS

This document describes how to switch the network type of an ApsaraDB for RDS instance to VPC through the console or API while retaining the classic network endpoint.

For more information, see [Hybrid access solution for smooth migration from classic networks to VPCs](#).



### Note:

- The classic network endpoint has an expiration time. You can specify the period as needed. When the expiration time is reached, the classic network endpoint is automatically deleted by the system. Before the endpoint is deleted, you will receive a message.
- If the RDS instance is a branch database of a DRDS instance, the network connection between the DRDS and the RDS instances will be interrupted after the network type is changed and you must reconnect them.

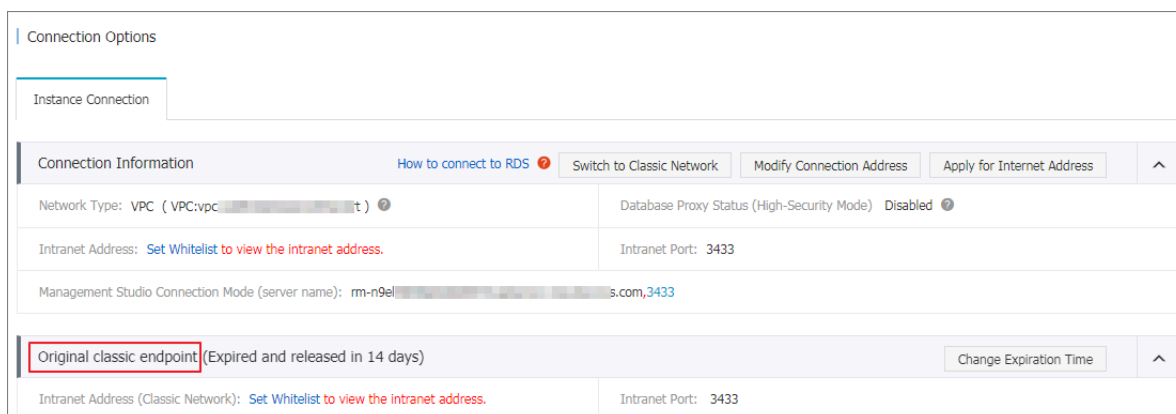
### Prerequisites

- The access mode of the instance is the enhanced security mode. For more information, see [Set access mode](#). MySQL 5.7, SQL Server 2012, and SQL Server 2016 version only supports the standard mode. This mode supports changing the network type through hybrid access.
- The network type is the classic network.

- There are available VPC and VSwitches in the zone where the RDS instance is located. For more information, see [Manage a VPC](#).

### Change the network type on the console

1. Log on to the RDS console.
2. Select the region of the target instance.
3. Click the ID of the target instance.
4. In the left-side navigation pane, select Connection Options.
5. In the Instance Connection tab, click Switch to VPC.
6. On the Switch to VPC page, select the target VPC and VSwitch.
7. Click Reserve original classic endpoint, and select the Expiration time.
  - From the 7th day before the classic network endpoint is deleted, the system will send a reminder message to the mobile phone bound to your account every day.
  - When the classic network endpoint expires, the classic network endpoint will be automatically released, and you cannot access the database through the classic network endpoint. To prevent service interruption, set the expiration time according to your needs. After the hybrid access configuration is complete, you can change the expiration time.
8. Click OK. An Original classic endpoint is added on the console.



### Modify the expiration time of the original classic endpoint on the console

After setting the expiration time for the classic network endpoint, you can extend the period on the console before the expiration time.

During the hybrid access period, you can change the expiration time of the classic network endpoint at any time as needed. The expiration time will be calculated from the date the change occurs. For example, if the classic network endpoint is set to

expire on August 18, 2017 and you change the expiration date to 14 days later on August 15, 2017, the endpoint will be released on August 29, 2017.

1. Log on to the RDS Console.
2. Select the region of the target instance.
3. Click the ID of the target instance.
4. In the left-side navigation pane, select Connection Options.
5. In the Instance Connection tab, click Change Expiration Time.
6. Select the expiration time and click OK.

#### Change the network type through API

1. Click the SDK link to download the SDK.
  - [aliyun-java-sdk-rds-new.zip](#)
  - [aliyun-python-sdk-rds-new.zip](#)
  - [aliyun-php-sdk-rds-new.zip](#)
2. Call the `ModifyDBInstanceNetworkType` API to change the network type.

#### Request parameters

Name	Type	Required	Description
Action	String	Yes	The action to perform. Valid value: <code>ModifyDBInstanceNetworkType</code>
DBInstanceId	String	Yes	The ID of the instance.
InstanceNetworkType	String	Yes	The network type of the instance: <ul style="list-style-type: none"><li>• <code>VPC</code> : An instance of the VPC network.</li><li>• <code>Classic</code> : An instance of the classic network.</li></ul>
VPCId	String	No	The ID of the VPC.
VSwitchId	String	No	The ID of the VSwitch. This parameter must be specified if the VPC ID is specified.

Name	Type	Required	Description
PrivateIpAddress	String	No	Enter an IP address in the VSwitch CIDR block. If no IP address is entered, the system allocates an intranet IP address according to the VPC ID and the VSwitch ID.
RetainClassic	String	No	Whether to retain the classic network endpoint. The default value is <code>False</code> : <ul style="list-style-type: none"> <li><code>True</code> : Retain</li> <li><code>False</code> : Do not retain</li> </ul>
ClassicExpiredDays	String	No	The expiration time of the classic network endpoint. The shortest time is 1 day, the longest time is 180 days, and the default value is 7 days. This parameter must be specified if <code>RetainClassic</code> is set to <code>True</code> .

### Response parameters

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

### Example code

If you want to retain the classic network endpoint:

- Set the `RetainClassic` parameter to `True`.
- Set the `ClassicExpiredDays` parameter to a value. The classic network endpoint will be deleted when it expires.

```
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_succeeds () {
```

```

ModifyDBIn stanceNetw orkTypeReq uest  request = new
ModifyDBIn stanceNetw orkTypeReq uest ();
    request . setInstanc eId ("< Your instance ID >");
    request . setInstanc eNetworkTy pe (" VPC ");
    request . setVPCId ("< VpcId : This parameter is
required when the TargetNetw orkType is VPC >");
    request . setVSwitch Id ("< VSwitchId : This parameter
is required when the TargetNetw orkType is VPC >");
    request . setRetainC lassic ("< Whether to retain
the classic network endpoint >");
    request . setClassic ExpiredDay s (" The expiration
time of the classic network endpoint ");
    IClientPro file profile = DefaultPro file .
getProfile (" cn - hangzhou ", "< Your AK >",
"< Your Security >");
    IAcsClient client = new DefaultAcs Client ( profile
);
    try {
        ModifyDBIn stanceNetw orkTypeRes ponse response
        response = client . getAcsResp onse ( request
);
        System . out . println ( response . getRequest Id
());
    } catch ( ServerExce ption e ) {
        e . printStack Trace ();
    }
    } catch ( ClientExce ption e ) {
        e . printStack Trace ();
    }
}
}

```

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

#### Request parameters

Name	Type	Required	Description
Action	String	Yes	The action to perform. Valid value: DescribeDB InstanceNe tInfo
DBInstance Id	String	Yes	The ID of the instance.

#### Response parameters

Name	Type	Description
DBInstance NetInfos	List	The connection information of the instance.



Name	Type	Description
InstanceNetworkType	String	<p>The network type of the instance:</p> <ul style="list-style-type: none"> <li>VPC : An instance of the VPC network.</li> <li>Classic : An instance of the classic network.</li> </ul>

### DBInstanceNetInfo

Name	Type	Description
ConnectionString	String	The DNS connection string.
IPAddress	String	The IP address.
IPType	String	<p>The IP type of an instance of the classic network: Inner   Public .</p> <p>The IP type of an instance of the VPC network: Private   Public .</p>
Port	String	The port information.
VPCId	String	The ID of the VPC.
VSwitchId	String	The ID of the VSwitch.
ExpiredTime	String	The expiration time.

### Reference code

```
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 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 AK >", "< Your Security >");
        IAcsClient client = new DefaultAcsClient(profile);
    }
}
```

```

        try {
            DescribeDBInstanceNetworkInfoResponse response
                = client.getAcsResponse(request);
            System.out.println(response.getRequestId());
        } catch (ServerException e) {
            e.printStackTrace();
        }
        } catch (ClientException e) {
            e.printStackTrace();
        }
    }
}

```

Modify the expiration time of the classic network endpoint through API

1. Click the SDK link to download the SDK.

- [aliyun-java-sdk-rds-new.zip](#)
- [aliyun-python-sdk-rds-new.zip](#)
- [aliyun-php-sdk-rds-new.zip](#)

2. Call the `ModifyDBInstanceNetworkExpireTime` API to modify the expiration time of the classic network endpoint.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The action to perform. Valid value: <code>ModifyDBInstanceNetworkExpireTime</code> .
DBInstanceId	String	Yes	The ID of the instance.
ConnectionString	String	Yes	The classic network connection string to be postponed. There are two string types: the classic network string of the current instance and the classic network string separating reading and writing.

Name	Type	Required	Description
ClassicExpiredDays	Integer	Yes	The expiration time of the classic network string is [1-120] days.

#### Response parameters

Name	Type	Description
RequestId	String	The ID of the request.

#### Reference code

```

public static void main ( String [] args ) {
    ModifyDBInstanceExpiredDaysRequest request = new
    ModifyDBInstanceExpiredDaysRequest ();
    request . setClassicExpiredDays ( 3 );
    request . setConnectionString ( "< The link string >" );
    request . setDBInstanceId ( "< The instance ID >" );
    IClientProfile profile
    = DefaultProfile . getProfile ( " cn - qingdao ", "<
Your ak >", "< Your sk >" );
    IAcsClient client = new DefaultAcsClient ( profile );
    try {
        ModifyDBInstanceExpiredDaysResponse response
        = client . getAcsResponse ( request );
        System . out . println ( response . getRequestId () );
    } catch ( ServerException e ) {
        e . printStackTrace ();
    }
    catch ( ClientException e ) {
        e . printStackTrace ();
    }
}

```

## 6.2.3 Change the network type of ApsaraDB for Redis

This document describes how to switch the network type of an ApsaraDB for Redis instance to a VPC network through the console and API while preserving the classic network endpoint. The classic network endpoint has a retention time limit. You can specify a retention period as needed. When the retention time is reached, the classic network endpoint is automatically deleted by the system. Before the endpoint is deleted, you will receive a message.

#### Prerequisites

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

- Make sure the network type of the instance is the classic network.

- There are available VPC and VSwitches in the zone where the Redis instance is located. For more information, see [Create a VPC and a VSwitch](#).

#### Change the network type on the console

1. Log on to the Redis Console.
2. Select the region where the target instance is located.
3. Click the ID of the target instance.
4. On the Instance Information page, click Switch to VPC.
5. In the displayed dialog box, complete these steps:
  - a. Select the target VPC and VSwitch.
  - b. Select to retain the classic network endpoint and select the retention time.



#### Note:

After you select to retain the classic network endpoint, the classic network endpoint and the VPC endpoint remain as two independent endpoints. As a result, ECS instances of the classic network can still access the database and the service is not affected. When the classic network endpoint expires, the system automatically deletes the classic network endpoint and you cannot access the database through the classic network endpoint.

- c. Click OK.
6. On the Instance Information page, click Refresh to view the VPC endpoint and classic network endpoint.

#### Modify the retention time

After setting the retention time for the classic network endpoint, you can extend its retention time through the console before it expires.

During the hybrid access period, you can change the retention time of the classic network endpoint at any time as needed. For example, if the classic network endpoint is set to expire on August 18, 2017 and you change the expiration date to 14 days later on August 15, 2017, the endpoint will be released on August 29, 2017.

1. Log on to the Redis Console.
2. Select the region where the target instance is located.
3. Click the ID of the target instance.

4. In the Retained Connection Address of the Classic Network area, click Modify Retention Period.
5. In the displayed dialog box, select a new expiration date and click OK.

#### Change the network type through API

1. Download the SDK. (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 to change the network type.

#### Request parameters

Name	Type	Required	Description
Action	String	Yes	The action to perform. Valid value: SwitchNetwork
InstanceId	String	Yes	The ID of the instance.
TargetNetworkType	String	Yes	The network type of the instance. <ul style="list-style-type: none"><li>• VPC : VPC</li><li>• Classic : Classic network</li></ul>
VPCId	String	No	The ID of the VPC.
VSwitchId	String	No	The ID of the VSwitch. This parameter must be specified if VPC ID is specified.
RetainClassic	String	No	Whether to retain the classic network endpoint. The default value is False : <ul style="list-style-type: none"><li>• True : Retain</li><li>• False : Do not retain</li></ul>

Name	Type	Required	Description
ClassicExpiredDays	String	No	The retention time of the classic network endpoint. The shortest time is 1 day, the longest time is 120 days, and the default value is 7 days. This parameter must be specified if RetainClassic is set to True.

### Response parameters

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

### 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.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 switchNetworkSuccess() {
        SwitchNetworkRequest request = new SwitchNetworkRequest();
        request.setInstanceId("< your instance ID >");
        request.setTargetNetworkType("VPC");
        request.setVpcId("< VpcId : This parameter is required when the TargetNetworkType is 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 time of the classic network endpoint");
        IClientProfile profile = DefaultProfile.getProfile("cn-hangzhou", "< Your AK >", "< Your Security >");
        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 to view the classic network endpoint and the VPC endpoint.

#### Request parameters

Name	Type	Required	Description
Action	String	Yes	The action to perform. Valid value: <code>DescribeDBInstanceNetInfo</code>
InstanceId	String	Yes	The ID of the instance.

#### Response parameters

Name	Type	Description
NetInfoItems	List	The connection information of the instance.
InstanceNetworkType	String	The network type of the instance. <ul style="list-style-type: none"> <li>• <code>VPC</code> : An instance of the VPC network.</li> <li>• <code>Classic</code> : An instance of the classic network.</li> </ul>

#### InstanceNetInfo

Name	Type	Description
ConnectionString	String	The connection string of DNS.
IPAddress	String	The IP address.
IPType	String	The IP type of an instance of the classic network: <code>Inner</code>   <code>Public</code> . The IP type of an instance of the VPC network: <code>Private</code>   <code>Public</code> .
Port	String	The port information.
VPCId	String	The ID of the VPC.

Name	Type	Description
VSwitchId	String	The ID of the VSwitch.
ExpiredTime	String	The time of expiration.

### 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 AK >",
                "< Your Security >");
        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 time of the classic network endpoint through API

1. Click the SDK link to download the SDK. (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 to change the network type.

### Request parameters

Name	Type	Required	Description
Action	String	Yes	The action to perform. Valid value: ModifyInstanceNetExpireTime.
InstanceId	String	Yes	The ID of the instance.
ConnectionString	String	Yes	The classic network endpoint.
ClassicExpiredDays	Integer	Yes	Select the retention time. Valid values: 14, 30, 60, or 120.

### Response parameters

Name	Type	Description
RequestId	String	The ID of the request.

### Example code

```

public static void main ( String [] args ) {
    ModifyInstanceNetExpireTimeRequest request = new
    ModifyInstanceNetExpireTimeRequest ();
    request . setClassicExpiredDays ( 3 );
    request . setConnectionString ( "< link string >" );
    request . setInstanceId ( "< instance Id >" );
    IClientProfile profile
        = DefaultProfile . getProfile ( " cn - hangzhou ", "<
Your ak >",
        "< Your sk >" );
    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 . getIPAddresses ());
            System . out . println ( item . getExpiredTime ());
        }
    } catch ( ServerException e ) {
        e . printStackTrace ();
    }
    catch ( ClientException e ) {
        e . printStackTrace ();
    }
}

```

}

## 6.2.4 Change the network type of ApsaraDB for MongoDB

This document introduces how to change the network type of ApsaraDB for MongoDB to VPC on the console or through the API, and retain the classic network endpoint. The classic network endpoint will be reserved for a period of the time. You can specify the reservation time according to your needs. When the reservation time is reached, the classic network endpoint is automatically deleted by the system.

### Prerequisites

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

- Make sure the network type is the classic network.
- The instance type must be MongoDB replica set.
- Make sure there are available VPC and VSwitches in the zone of the database instance. For more information, see [Create a VPC and a VSwitch](#).

### Change the network type on the console

1. Log on to MongoDB console.
2. Find the target instance and click the instance ID or click Manage in the Actions column.
3. In the left-side navigation pane, click the Connection Options tab and then click Switch to VPC.
4. In the displayed dialog box, complete these steps:
  - a. Select the target VPC and VSwitches.
  - b. Select to retain the classic network endpoint and select the retention time.



#### Note:

After you select to retain the classic network endpoint, ECS instances of the classic network can still access data and there is no impact on the service. When the classic network endpoint expires, the system automatically deletes the classic network endpoint and you cannot access the database through the classic network endpoint.

- c. Click OK.
5. On the Connection Options page, Click Refresh to view the VPC endpoint and the classic network endpoint.

## Change the network type through API

### 1. Click the SDK link to download the SDK.

- [aliyun-python-sdk-dds.zip](#)
- [aliyun-java-sdk-dds.zip](#)
- [aliyun-php-sdk-dds.zip](#)

### 2. Call the ModifyDBInstanceNetworkType API to change the network type.

#### Request parameters

Name	Type	Required	Description
Action	String	Yes	The action to perform. Valid value: ModifyDBInstanceNetworkType
DBInstanceId	String	Yes	The ID of the instance.
NetworkType	String	Yes	The network type of the instance. <ul style="list-style-type: none"><li>• VPC : VPC</li><li>• Classic : Classic network</li></ul>
VPCId	String	No	The ID of the VPC.
VSwitchId	String	No	The ID of the VSwitch. This parameter must be specified if VPC ID is specified.
RetainClassic	String	No	Whether to retain the classic network endpoint. The default value is False : <ul style="list-style-type: none"><li>• True : Retain</li><li>• False : Do not retain</li></ul>
ClassicExpiredDays	String	No	The retention time of the classic network endpoint. The shortest time is 1 day, the longest time is 120 days, and the default value is 7 days. This parameter must be specified if RetainClassic is set to True.

#### Response parameters

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

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

#### Request parameters

Name	Type	Required	Description
Action	String	Yes	The action to perform. Valid value: DescribeReplicaSetRole
DBInstanceId	String	Yes	The ID of the instance.

#### Response parameters

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

#### ReplicaSetRole

Name	Type	Description
ReplicaSetRole	String	Replica set role: Primary   Secondary
ConnectionDomain	String	The connection information of the instance.
ConnectionPort	String	The connection port of the instance.
ExpiredTime	String	The remaining retention time in seconds of the classic network endpoint.
NetworkType	String	The network type of the instance. <ul style="list-style-type: none"><li>• VPC : VPC</li><li>• Classic : Classic network</li></ul>

## 6.3 Hybrid access of other products

Hybrid access means access to ApsaraDB from ECS instances in both the classic network and the VPC network. Besides ApsaraDB, the following products also

support hybrid access. You can view the endpoints of different cloud products in the documentation.

#### Storage

- Object Storage Service: [Obtain endpoints](#).
- Table Store: [Obtain endpoints](#).

#### Application service

- Log Service: [Obtain endpoints](#).

#### Middleware

- Message Queue
  - Management and control: [Obtain endpoints](#).

#### Big data

- MaxCompute: [Obtain endpoints](#).

## 6.4 Example of hybrid access and hybrid adding migration

This document provides an example of using the hybrid access and hybrid adding solution to migrate resources from the classic network to a VPC network.

#### Prerequisites

Before the migration, make sure that:

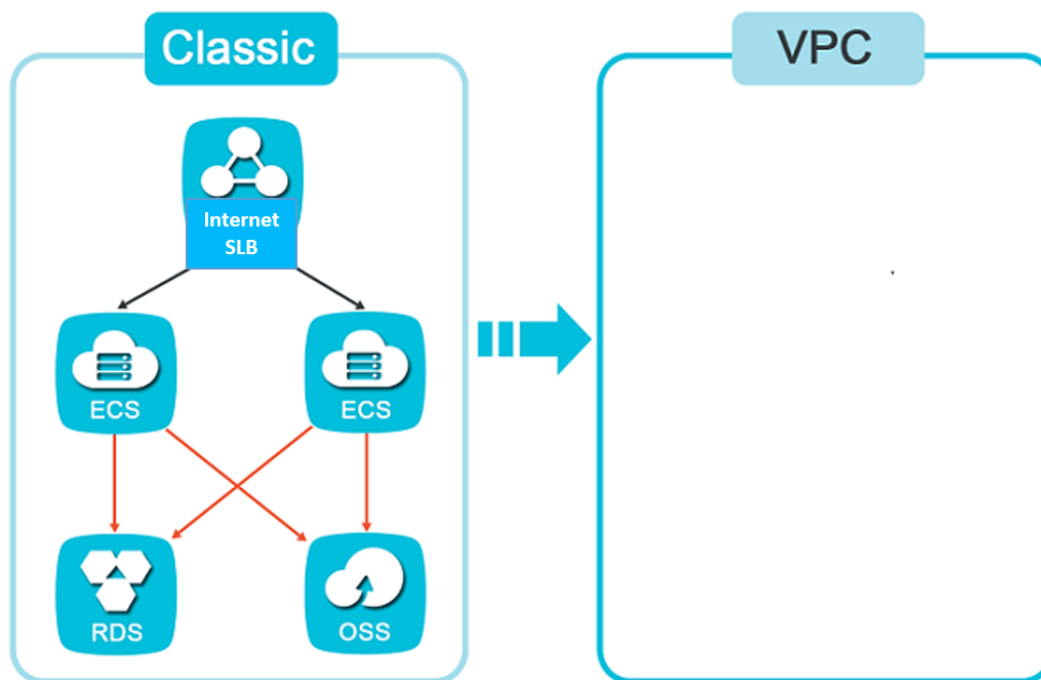
- You have known the details and limits of the migration. For more information, see [Migration overview](#).
- You are familiar with VPC and the related products. VPC and the classic network are very different. Apart from the network isolation, VPC enables you to control your private network by using other related products.
- The migration example in this document is only for reference. Many systems are more complex than that in the example. Before the migration, you need to make careful evaluation, find out system dependencies and work out a precise migration plan.

#### Example systems

This document provides two migration examples. One of the systems to be migrated is more complex than the other:

- System 1

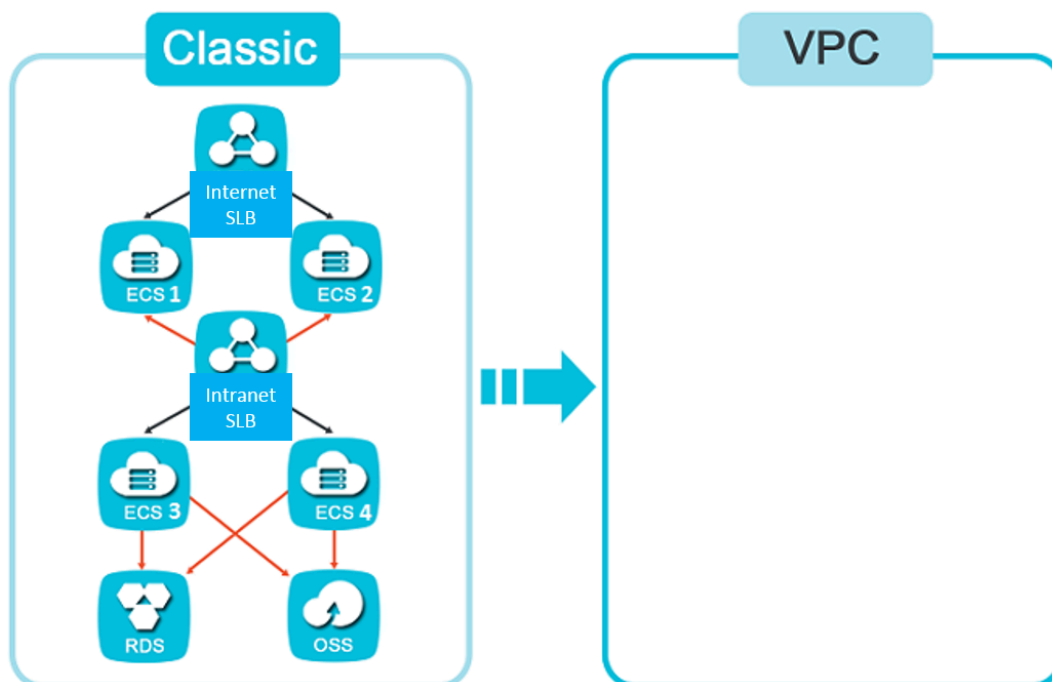
As shown in the following figure, the system to be migrated consists of SLB, ECS, RDS and OSS. The Internet SLB instance uses two ECS instances as the backend servers and the application deployed on the two ECS instances need to access RDS and OSS.



- System 2

As shown in the following figure, system 2 has a more complex architecture. As shown in the following figure, the Internet SLB instance uses two ECS instances (ECS 1 and ECS 2) as the backend servers. And these two ECS instances have to

access an intranet SLB instance. Similarly, the intranet SLB instance also uses two ECS instances (ECS 3 and ECS 4) which need to access RDS and OSS.



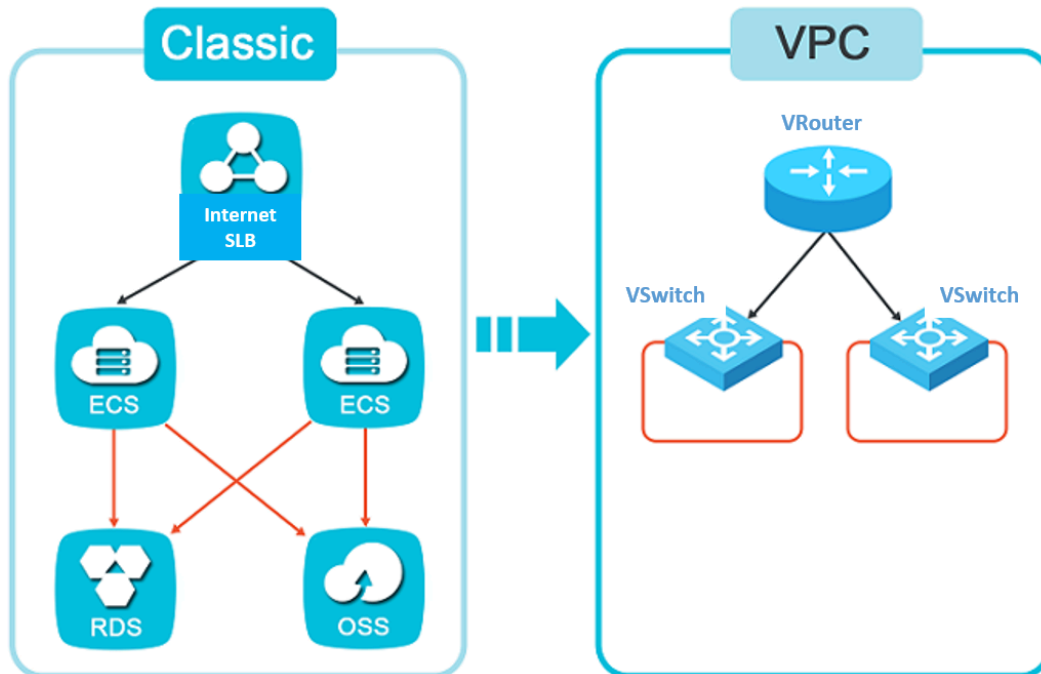
#### Migrate system 1 to VPC

To migrate *system 1* to a VPC, complete these steps:

### 1. Prepare the network environment.

Firstly, you have to create a VPC and VSwitch to which the system is migrated.

For more information, see [Create a VPC](#).



### 2. Obtain the VPC endpoints of RDS and OSS.

- You can migrate the RDS instance to the VPC either through the API or on the console and reserve its classic network endpoint at the same time. For more information, see [Change the network type of ApsaraDB for RDS](#).

After the migration, the classic network endpoint remains unchanged and a new VPC endpoint is added. Therefore, the ECS instances in the classic network can still access data and the service is not interrupted. When the classic network endpoint expires, the system automatically deletes it and you cannot access the database through the classic network endpoint.

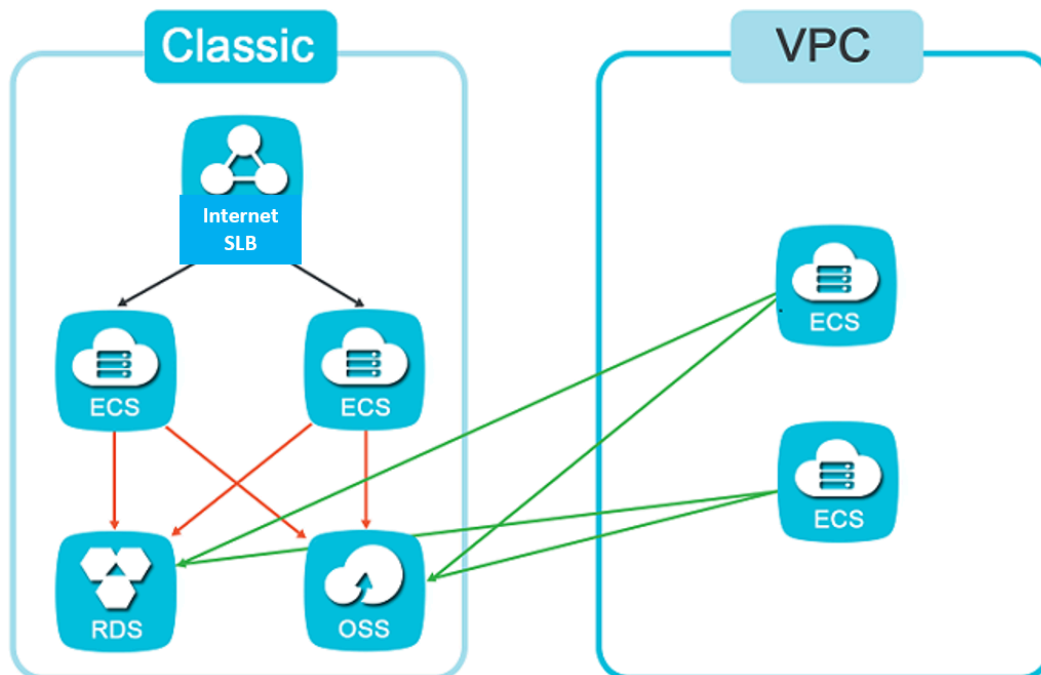
- OSS provides two endpoints itself and no switching is required. To obtain the VPC endpoint of OSS, see [Regions and endpoints](#).

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

As shown in the following figure, create two ECS instances in the VPC, deploy applications on these instances, and change the RDS and OSS endpoints to their



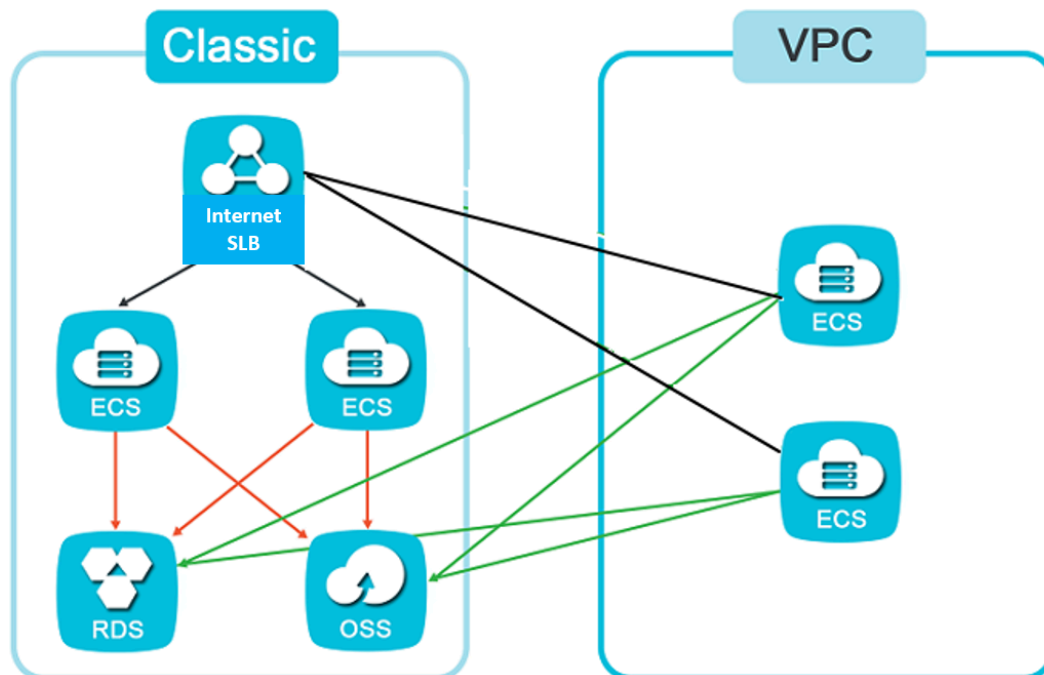
VPC endpoints. After the configuration is complete, you need to do test to verify that OSS and RDS are accessible.



4. Add the ECS instances in the VPC to the Internet SLB instance.

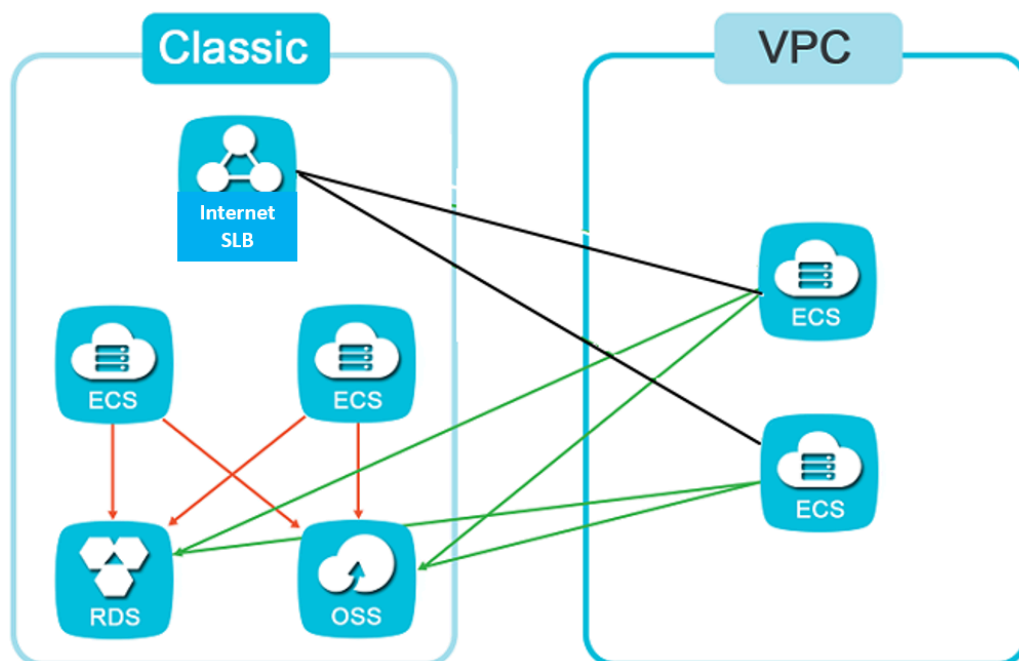
As shown in the following figure, add the ECS instances created and configured in the VPC to the Internet SLB instance. Then observe the health check status of the newly added ECS instances. You can set a smaller weight for the ECS instances . This helps reduce the impact on the system when the instances are declared as

healthy but other exceptions occur. Also, observe information like system status, traffic monitoring, and health check logs.



5. Remove ECS instances of the classic network from the Internet SLB instance.

As shown in the following figure, when the system is operating normally, remove the ECS instances of the classic network from the Internet SLB instance. You can set the weights of the ECS instances of the classic network to zero and then remove them when no more traffic is distributed to them.



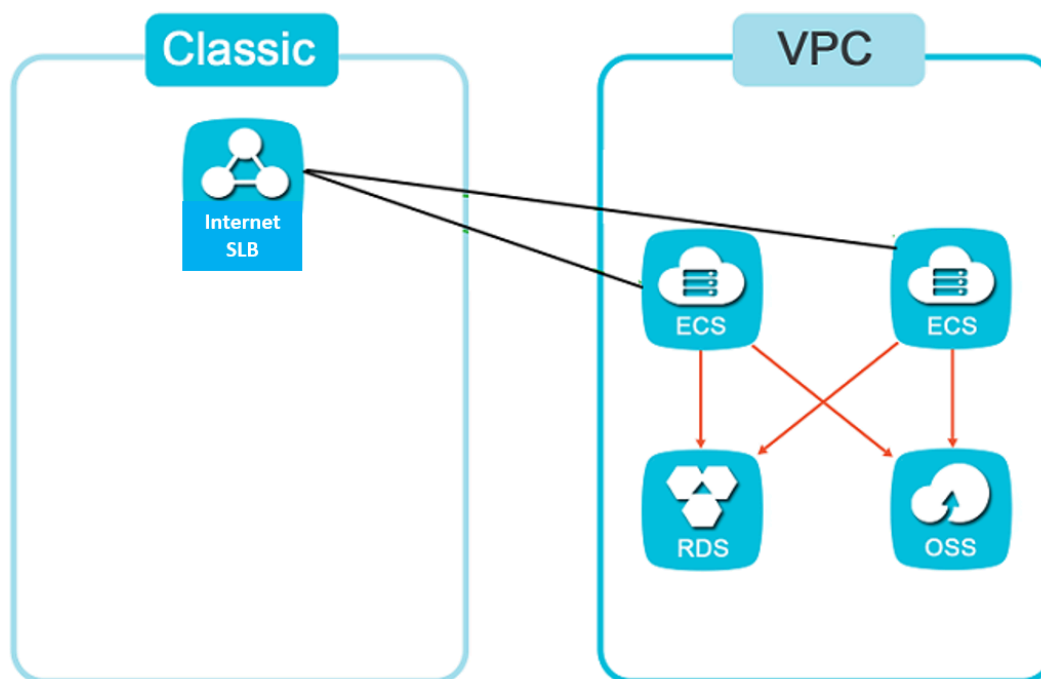
## 6. Release the ECS instances of the classic network.

As shown in the following figure, release the ECS instances of the classic network after the system has been running normally for a period of time. The Internet SLB instance supports adding ECS instances of the VPC network itself, so no migration is required. Till now, you have finished the migration.



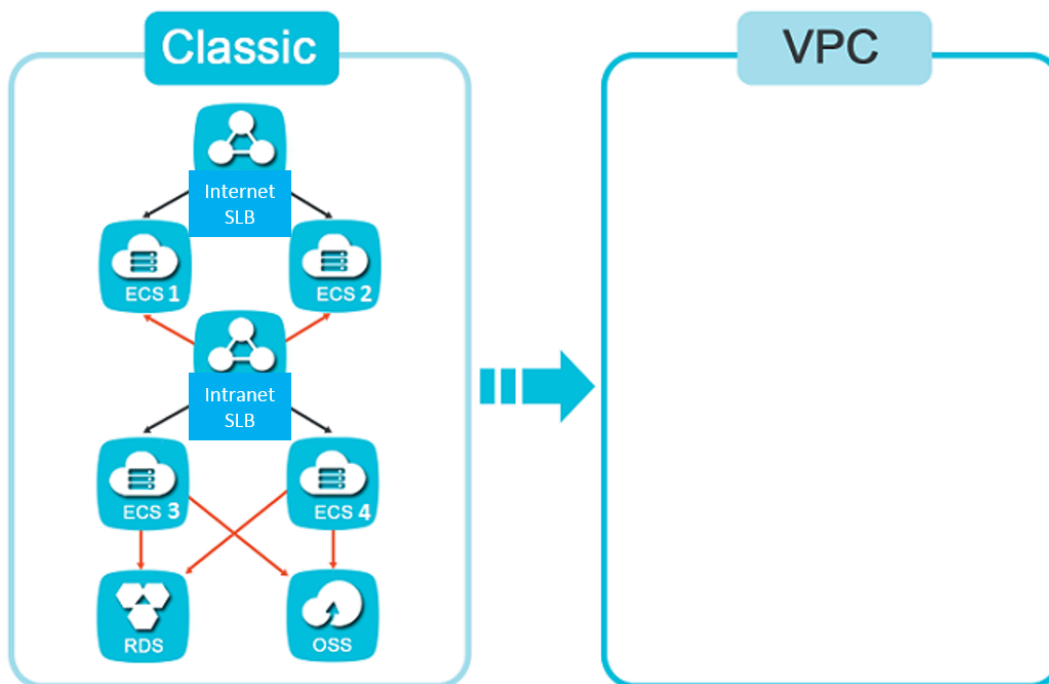
### Note:

The classic network endpoint of RDS will be automatically deleted once it expires.



## Migrate system 2 to VPC

When migrating a relative complex system as shown in the following figure, if the procedure for migrating system 1 is used, the ECS instances of the VPC network cannot access the ECS instances of the classic network because the SLB instance does not support hybrid access.



The basic steps for migrating this system are as follows:

1. Create two ECS instances in the VPC to migrate the ECS 3 and ECS 4 of the classic network added to the intranet SLB instance.
2. Configure the newly created ECS instances using the VPC endpoints of RDS and OSS.
3. Create an intranet SLB instance in the VPC to replace the intranet SLB instance in the classic network.
4. Configure the intranet SLB instance in the VPC. Add the two ECS instances created in step 1 as the backend servers.
5. Create two more ECS instances in the VPC to migrate the ECS 1 and ECS 2 of the classic network added to the Internet SLB instance.
6. Configure these two ECS instances. Change the classic network endpoint of the intranet SLB instance to the VPC endpoint of the instance.
7. The following steps are similar to the migration of system 1.