

Alibaba Cloud Virtual Private Cloud

Best practices

Issue: 20180929

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.	 Danger: 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.	 Warning: 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.	 Note: 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.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus, page names, and other UI elements.	Click OK .
<i>Courier font</i>	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 a optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	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 private connectivity product?.....	6
3 How to choose an Internet-facing product?.....	18
4 How to use cloud products in a VPC ?	23
5 Migrate from the classic network to VPC.....	25
5.1 Migration overview.....	25
5.2 Database hybrid access.....	27
5.2.1 Hybrid access of ApsaraDB.....	27
5.2.2 Change the network type of ApsaraDB for RDS.....	28
5.2.3 Change the network type of ApsaraDB for Redis.....	35
5.2.4 Change the network type of ApsaraDB for MongoDB.....	41
5.3 Hybrid access of other products.....	44
5.4 Example of hybrid access and hybrid addition migration.....	45

1 Plan and design VPC

Before creating VPCs and VSwitches, you need to plan the number of VPCs to create and CIDR blocks of VPCs and VSwitches according to specific business.

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

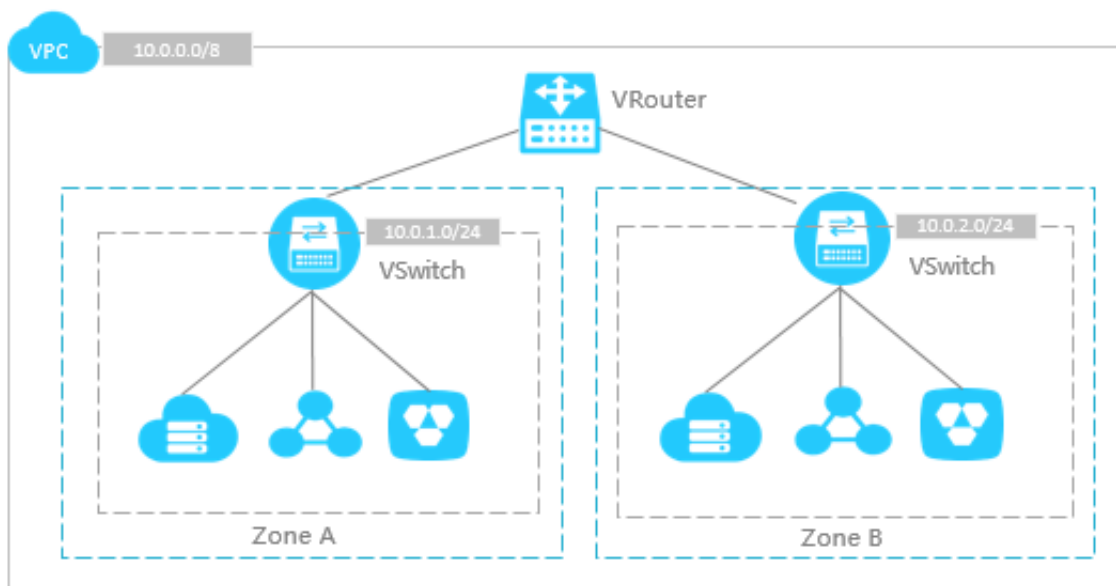
When using VPC, the first problem encountered is how to design your VPC network. You can start designing your VPC by answering the following questions:

- [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?](#)

Q1: How many VPCs are required?

- One VPC

If you do not have requirements to deploy your system in multiple regions and the system does need to be isolated by using VPC, one VPC is recommended. Currently, a VPC can host up to 15,000 cloud product instances.

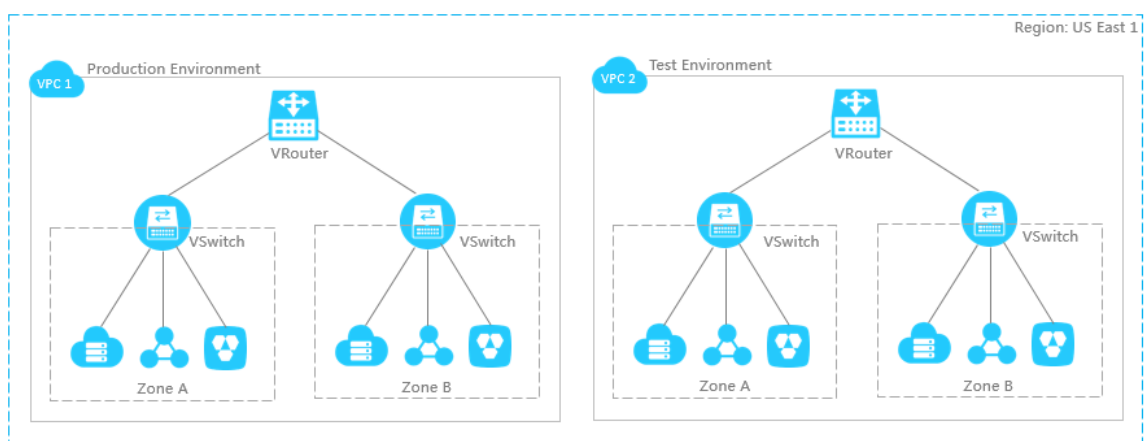


- Multiple VPCs

If you have the following requirements, two and more VPCs are recommended.

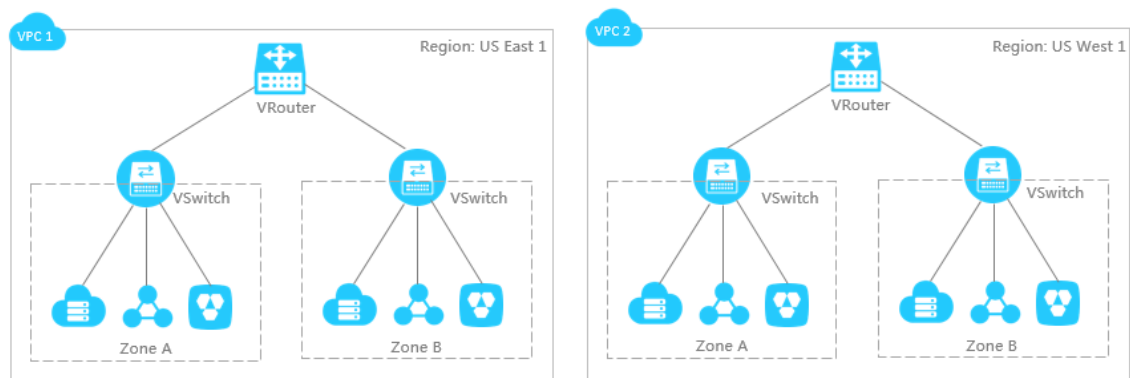
- Deploy cloud product resources in different regions

VPCs are a region-specific resource 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, it is recommended 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 protects your applications from a single point of failure.

Network latency between different zones in a 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 systems calls or cross-zone calls. Optimize and adjust the system to find a balance between high availability and low latency.

Additionally, the number of VSwitches is related to the system size and system design. If the front-end system requires mutual access to 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 and the VSwitch 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 IP address range as listed in the previous table.
- If you have multiple VPCs, or you want to build a hybrid cloud composed of one or more VPCs and local data centers, it is recommended that you use the 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 cloud product instances in a classic network with a VPC, it is recommended that 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 ranges from 192.168.0.0/17 to 192.168.0.0/29.

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

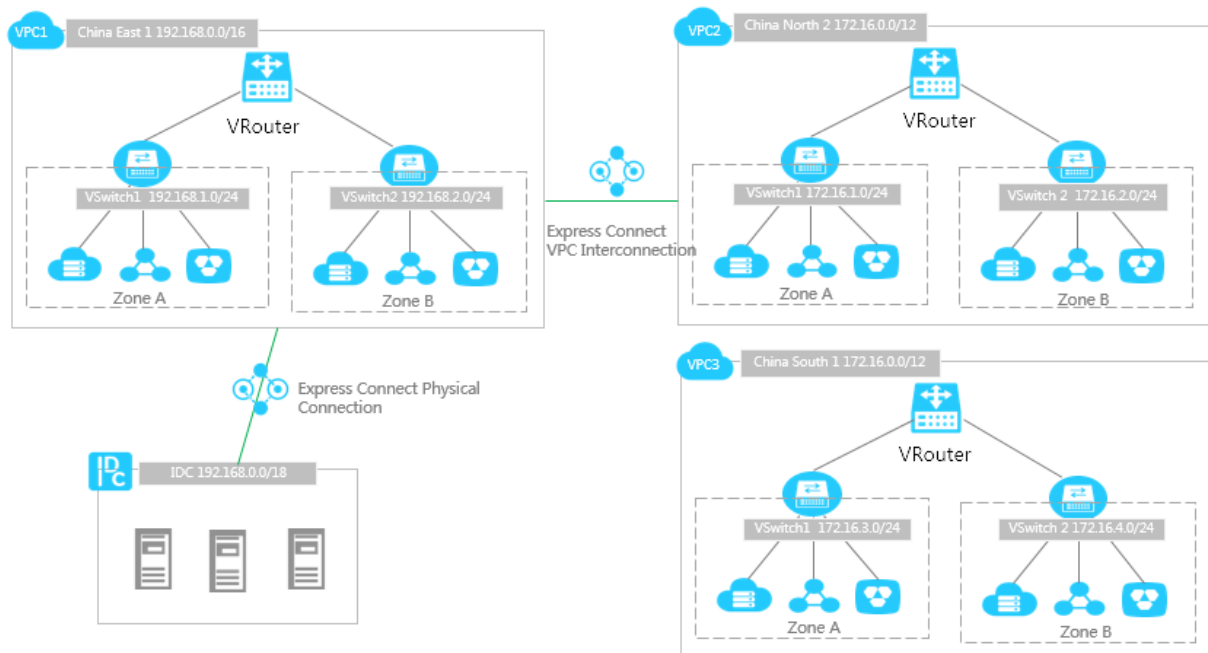
- The allowed block size for a VSwitch is between a /16 netmask and /29 netmask, which can provide 8 to 65,536 IP addresses. The /16 netmask is larger enough to use with 65,532 IP addresses, while the /29 netmask is too small.
- The first and last three IP addresses of a VSwitch are reserved by the system. 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 of 192.168.0.0/16, 10.0.0.0/8, and 172.16.0.0/12 IP address ranges. 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 cloud product 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 block for networks to be connect do not conflict with each other.

As shown in the following figure, you have a 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, 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. 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 VPCs.
- 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 private connectivity product?

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

This document summarizes available private connectivity solutions for connecting VPCs.

<i>Connect the VPCs</i>			
Product	Description	Benefit	Limit
VPN Gateway	Connect two VPC networks using an Internet-based and encrypted IPsec-VPN tunnel.	Low cost Security Out-of-the-box service.	However, the network latency and availability depend on the Internet.
Cloud Enterprise Network (CEN)	Connect one or more VPC networks in different regions and different accounts to build an interconnected network.	Simple configuration, and automatic route learning and distribution. Low latency and high speed. The networks (VPC/VBR) attached to a CEN instance are all connected with each other. Connecting networks in the same region is free of charge.	—
<i>Connect to a local IDC</i>			
Product	Description	Benefit	Limit
VPN Gateway	Connect a local IDC and a VPC through an Internet-based and encrypted IPsec-VPN tunnel.	Low cost Security Configurations take effect immediately.	However, the network latency and availability depend on the Internet.
Cloud Enterprise Network (CEN)	Through automatic route learning and distribution, CEN can connect resources	Simple configuration, and automatic route learning and distribution.	—

	in the whole network . You only need to attach the VBR associated with the local data center to the CEN instance.	Low latency and high speed. The networks (VPC/ VBR) attached to a CEN instance are all connected with each other. Connecting networks in the same region is free of charge.	
Smart Access Gateway	Connect a local data center to Alibaba Cloud.	Highly automatic and out-of-the-box service. 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.	—
Express Connect	Connect a local IDC and a VPC through the physical connection of Express Connect.	High network quality High bandwidth	High cost Long activation time
VPN software in Alibaba Cloud Marketplace	You can buy a VPN Gateway in Alibaba Cloud Marketplace and deploy it in the VPC, and connect a local data center to the VPC through an Internet-based and	Security Various VPN software are available. Configurations take effect immediately.	You must build and maintain the VPN Gateway by yourself. The network latency and availability depend on the Internet.

	encrypted IPsec-VPN tunnel.		
<i>Connect multiple sites</i>			
Product	Description	Benefit	Limit
VPN Gateway (VPN-Hub)	Establish secure communication among multiple sites through the VPN Gateway. The VPN-Hub function not only enables each site to communicate with the VPC on the cloud, but also allows each site to communicate with each other.	Low cost Out-of-the-box service	—
Smart Access Gateway	Buy Smart Access Gateways for local branches to be connected and add the Smart Access Gateways to a Cloud Connect Network (CCN). Attach the CCN to a CEN instance to enable intranet connections among these local branches.	Out-of-the-box service 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.	—
VPN Gateway (VPN-Hub) + Express Connect	You can use VPN Gateway and Express Connect to connect application systems and office sites around the world.	High network quality Out-of-the-box service	The network latency and availability depend on the Internet.

<i>Remote access to a VPC</i>			
Product	Description	Benefit	Limit
VPN Gateway (SSL-VPN)	Use the SSL-VPN function to securely and quickly access VPC from a remote client.	Low cost Reliable Easy to configure and deploy	—
SSL-VPN software in Alibaba Cloud Marketplace	Buy SSL-VPN software in Alibaba Cloud Marketplace, deploy it in VPC, and access the VPN server from a remote client.	Various SSL-VPN software is available.	High cost Low reliability Deploy and maintain the SSL-VPN software by yourself.

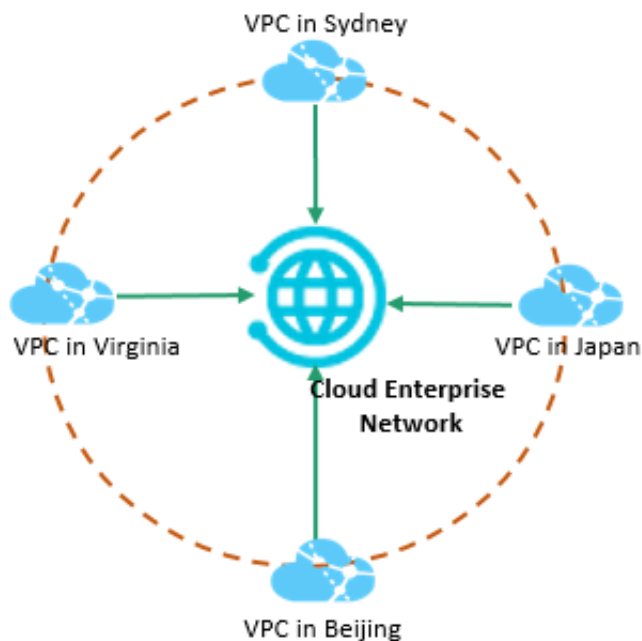
Connect the VPCs

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

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

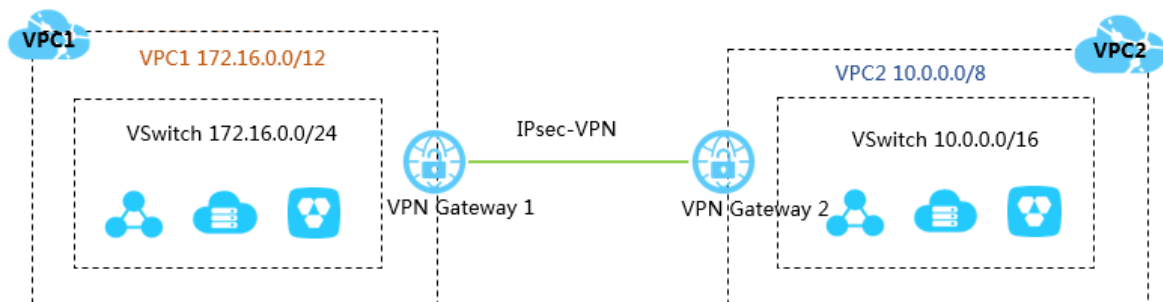
- Cloud Enterprise Network (CEN)

CEN (Cloud Enterprise Network) helps you to build an Intranet communication channel between one or more VPCs. Through automatic route distribution and learning, it accelerates network convergence, improves the quality and security of cross-network communication, and connects resources in the whole network, thus helping you build an interconnected network with enterprise-grade scale and communication ability.



- 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. You can connect VPCs in different regions and different accounts through VPN Gateway. You need to create one VPN Gateway and one customer gateway for the VPCs respectively, and establish an IPsec encrypted tunnel between the VPC Gateway and the corresponding customer gateway to achieve intranet communication.



Connect to a local IDC

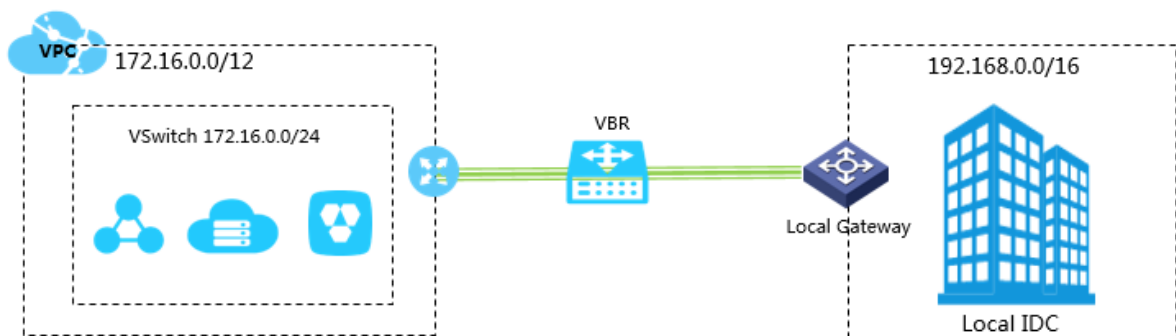
You can connect a VPC to a local IDC to build a hybrid cloud. With the secure and reliable connection between the VPC and IDC, and massive computing, storage, network, CDN, and GBP resources on Alibaba Cloud, you can extend IDC local IT infrastructure seamlessly to Alibaba Cloud in real time in Pay-As-You-Go mode to deal with fluctuations in service.

You can connect a local IDC to a VPC through Express Connect, VPN Gateway or CEN.

- Express Connect

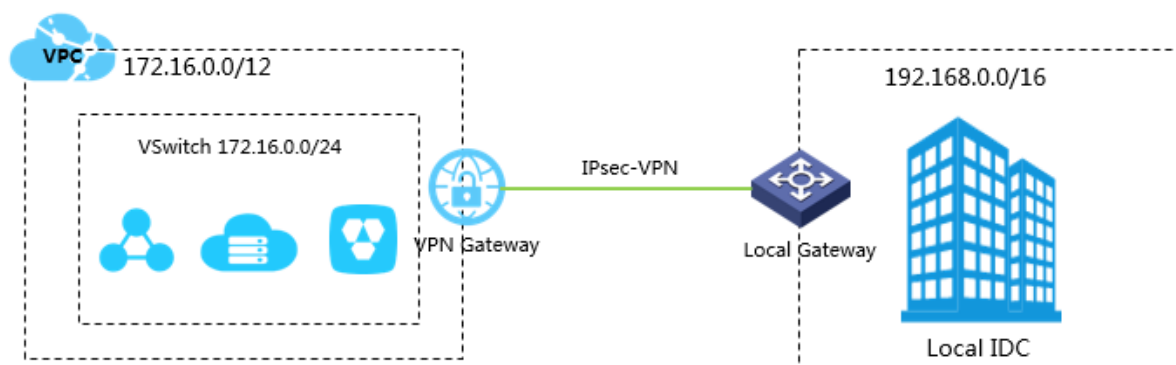
Express Connect provides the physical connection function. After a leased line is accessed to an Alibaba Cloud access point, you can create a peer connection between a VBR and a VPC to build a hybrid cloud.

The intranet connection of leased line does not go through the Internet. Therefore, compared with the traditional Internet connection, the physical connection features higher security, reliability and speed and lower latency.



- VPN Gateway

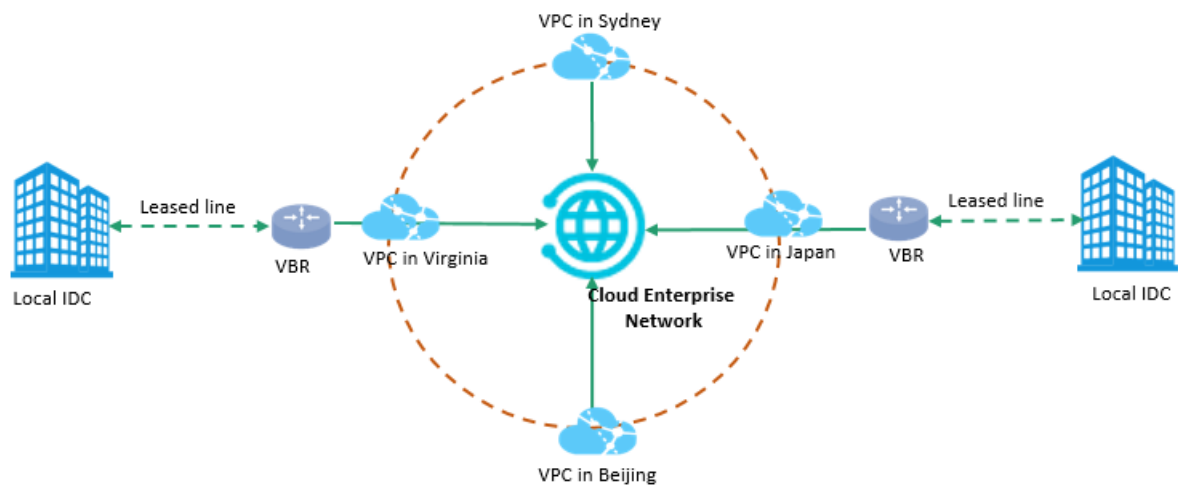
VPN Gateway can connect a local data center, a local site, an Internet terminal to a VPC in a secure and reliable way through an Internet-based and encrypted channel. VPN Gateway contains two different gateway instances which provide active/standby hot backup. The traffic is automatically distributed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



- Cloud Enterprise Network (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 local IDC to a CEN instance

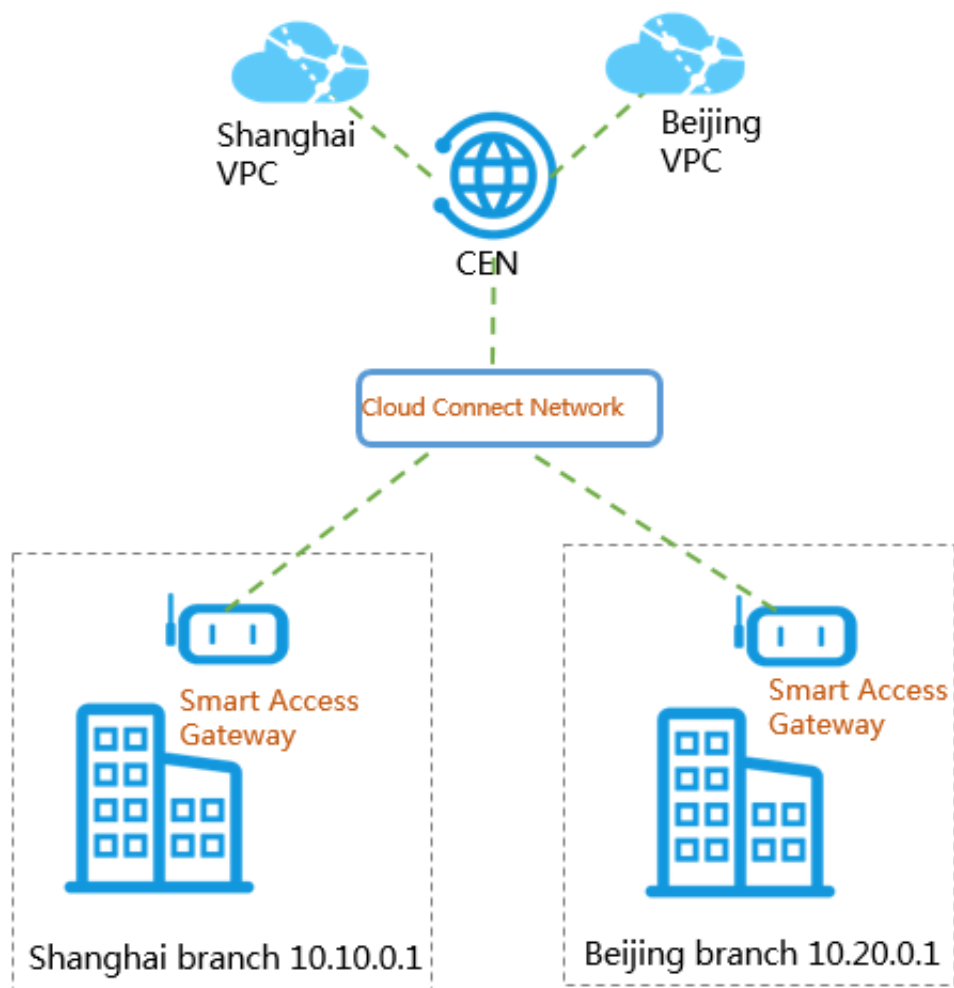
, then the local IDC can communicate with all networks (VPCs or VBRs) attached to the CEN instance.



- Smart Access Gateway

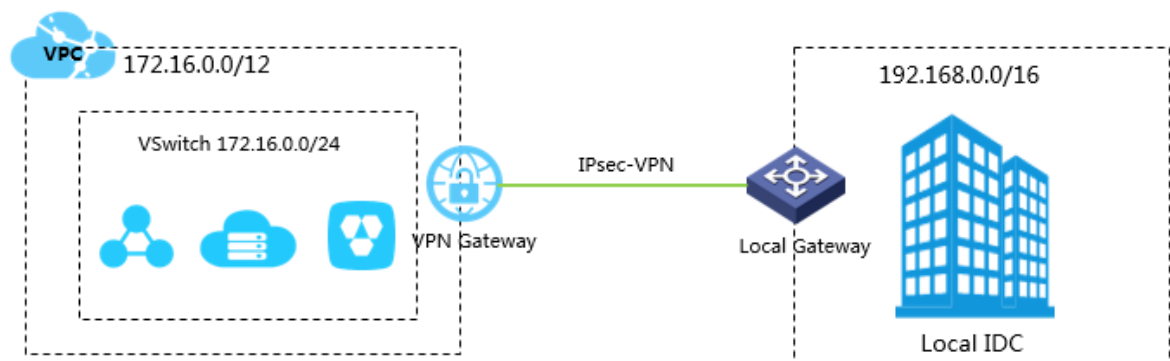
Smart Access Gateway is a one-stop solution for connecting local organizations to the Alibaba Cloud. With Smart Access Gateway, enterprises can access Alibaba cloud through the Internet in an encrypted way, and get a more intelligent, more reliable, and more secure experience in accessing the Alibaba Cloud.

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



- VPN software in Alibaba Cloud Marketplace

Alibaba Cloud Marketplace provides various VPN software or images. You can buy VPN software in 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 local IDC through the Internet.



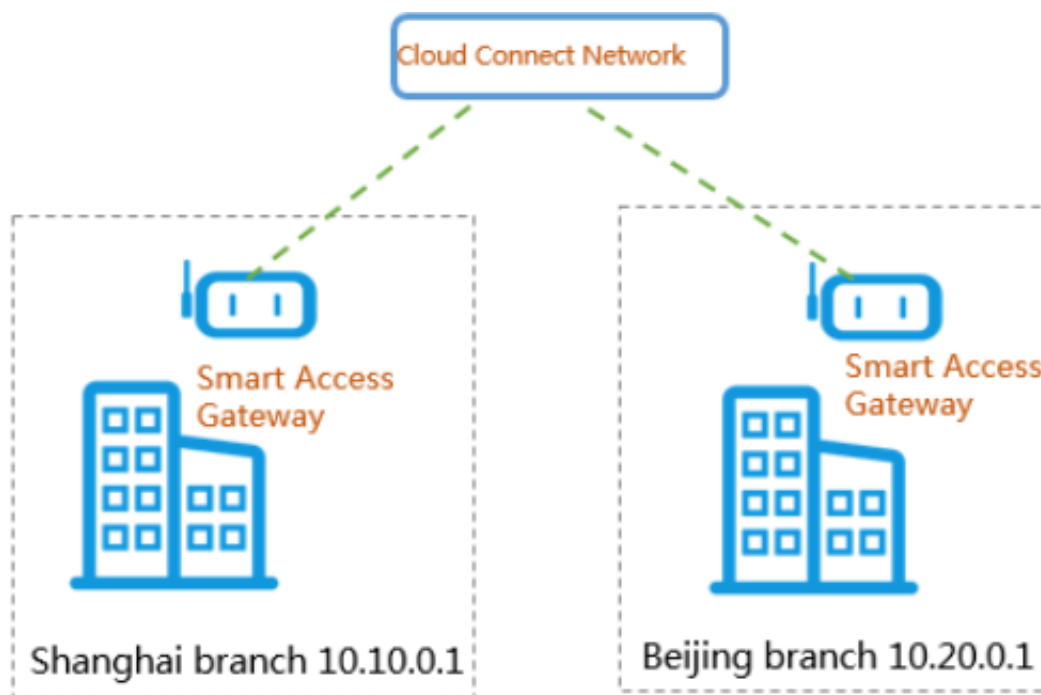
Connect multiple sites

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 one-stop solution for connecting local organizations to the Alibaba Cloud. With Smart Access Gateway, enterprises can access Alibaba cloud through the Internet in an encrypted way, and get a more intelligent, more reliable, and more secure experience in accessing the Alibaba Cloud.

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

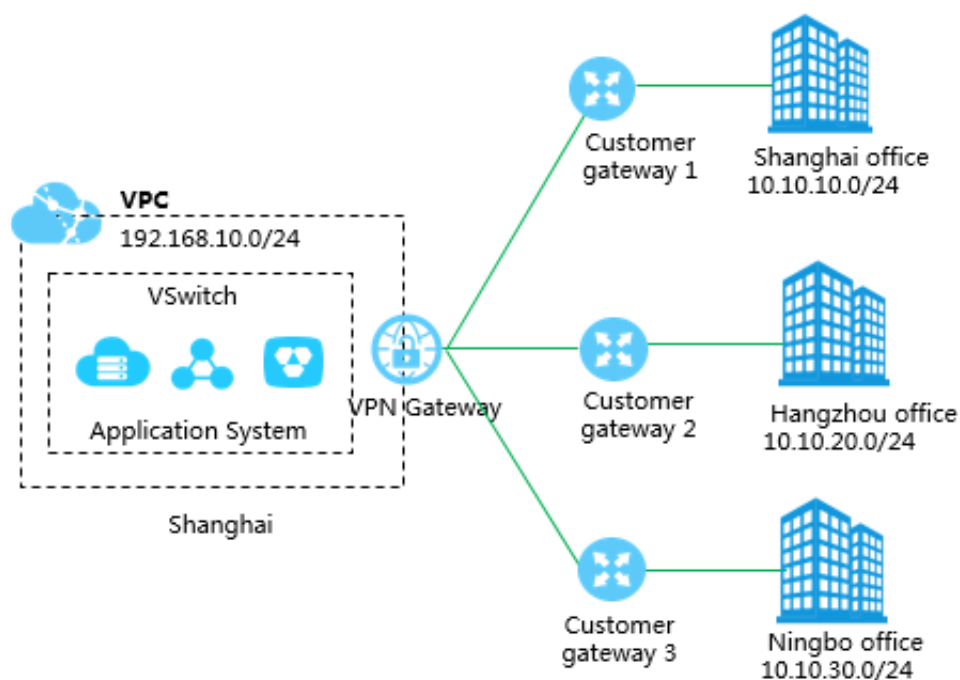


- Connect multiple sites

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 IDCs or local sites in different areas.

You can establish secure communication among multiple sites through the VPN-Hub function. The sites cannot only communicate with the connected VPC but also can communicate with each another. VPN-Hub meets the needs of large enterprises to establish intranet communication among different sites.

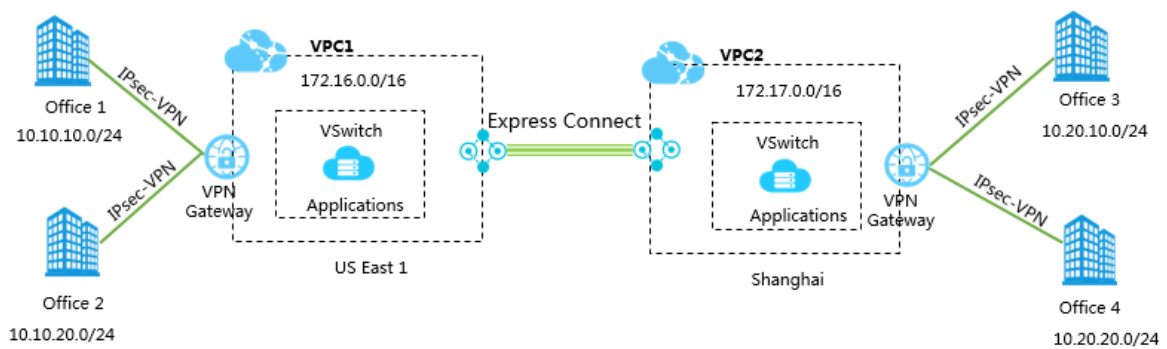
The VPN-Hub function is enabled by default. You only need to configure the IPsec-VPN connection between each office site and Alibaba Cloud, and no additional charges are billed. A VPN Gateway supports up to 10 IPsec connections. Therefore, you can connect up to 10 office sites with one VPN Gateway. As shown in the following figure, to connect the three office sites (Shanghai, Hangzhou, and Ningbo), 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 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 East and the VPC in Shanghai respectively, connect the VPCs through Express Connect and connect office sites in the two regions to the two VPCs through IPsec-VPN.



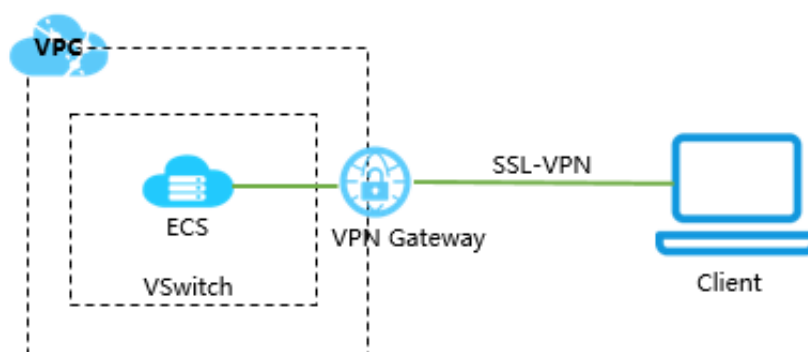
Remote access to a VPC

The SSL-VPN function of VPN Gateway provides site-to-site VPN connection. Terminals can directly access a VPC without configuring customer gateways. You can deploy local internal applications in a VPC, and internal staff access the internal system through SSL-VPN. For example, local IT staff access the VPC through intranet to perform operation and maintenance, and staff on a business trip can access local applications in the VPC from remote sites.

Both VPN Gateway or VPN software/image in Alibaba Cloud Marketplace can 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.



- Purchase SSL-VPN software in Alibaba Cloud Marketplace

You can buy an SSL-VPN software or image in Alibaba Cloud Marketplace and deploy SSL-VPN on an ECS instance bound with EIP in the VPC, then you can access the Internet from a remote client.

3 How to choose an Internet-facing product?

In the VPC network, you can use Elastic IP Address (EIP), NAT Gateway, Internet Server Load Balancer (SLB) and 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, 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 address, ECS, NAT Gateway, and SLB has supported binding EIP as the public IP.



您可以将EIP加入到####和#####中，灵活应对波峰波谷，降低公网成本。

Internet-facing products

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

此外，为了降低使用公网的带宽和流量成本，阿里云在VPC环境下提供了####和#####两款独立的产品。您可以根据自己的业务模型选择使用不同的产品，以达到降低成本的目的。

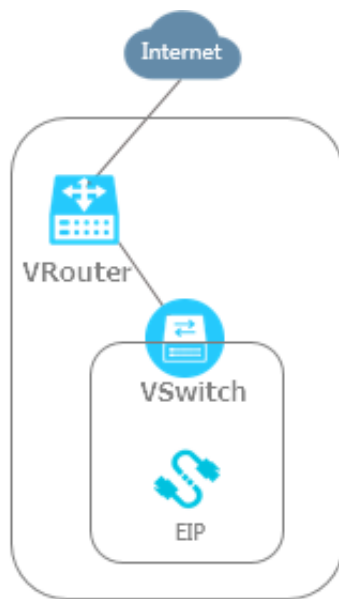
Product	Function	Benefit
ECS public IP	The public IP allocated by Alibaba Cloud when creating an ECS instance of the VPC network. With this public IP, the ECS instance can access the Internet (SNAT) and also can be accessed from the Internet (DNAT). However, you cannot unbind the public IP from the ECS instance. 目前默认不能动态和VPC ECS解绑，但可以将公网IP转换为EIP。详情参见 ECS#####IP###EIP 。	支持使用共享流量包，将公网IP转换为EIP后也可以使用####。
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. 可以使用####和#####，降低公网成本。
NAT Gateway	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).	The core difference between NAT Gateway and EIP is that NAT Gateway supports Internet access of multiple ECS instances but EIP can only be used by an ECS instance.

Product	Function	Benefit
	 Note: Compared to Server Load Balancer, NAT Gateway itself does not provide the traffic balancing function.	
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>  Note: The ECS instance without a public IP cannot access the Internet (SNAT) through Server Load Balancer.	<p>In DNAT, Server Load Balancer supports forwarding an Internet request to multiple ECS instances. Server Load Balancer is a traffic distribution control service that distributes the incoming traffic among multiple ECS instances according to the configured forwarding rules . It expands application service capabilities and enhances application availability.</p> <p>绑定EIP后，支持使用####和#####，降低公网成本。</p>

Scenario 1: provide external services

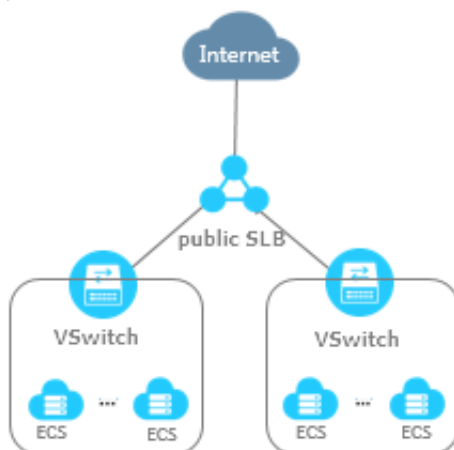
- Provide external services with a single ECS instance

If you have only one application and the business is not large, a single ECS can meet your requirements. You can deploy applications, databases, and files on this ECS. Then, bind an EIP to the ECS instance. Therefore, users can access the deployed application through the Internet.



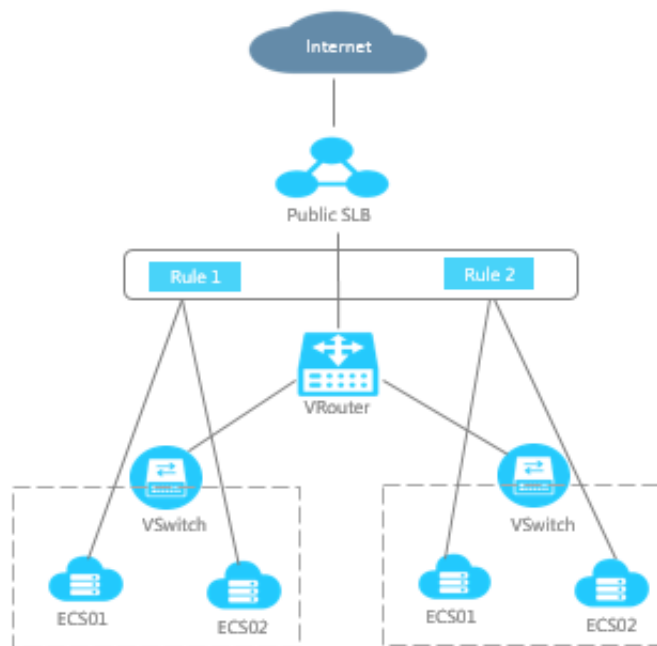
- Provide external services with Layer-4 load balancing

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 server.



- Provide external services with Layer-7 load balancing

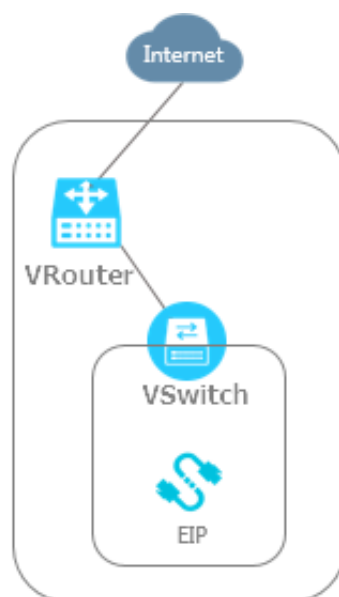
In addition to the basic traffic distribution, if you want to distribute different requests to different backend servers, you can add URL forwarding rules to a Layer-7 listener. In this case, you can configure an Internet SLB instance with a Layer-7 listener and add these ECS instances as the backend server.



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

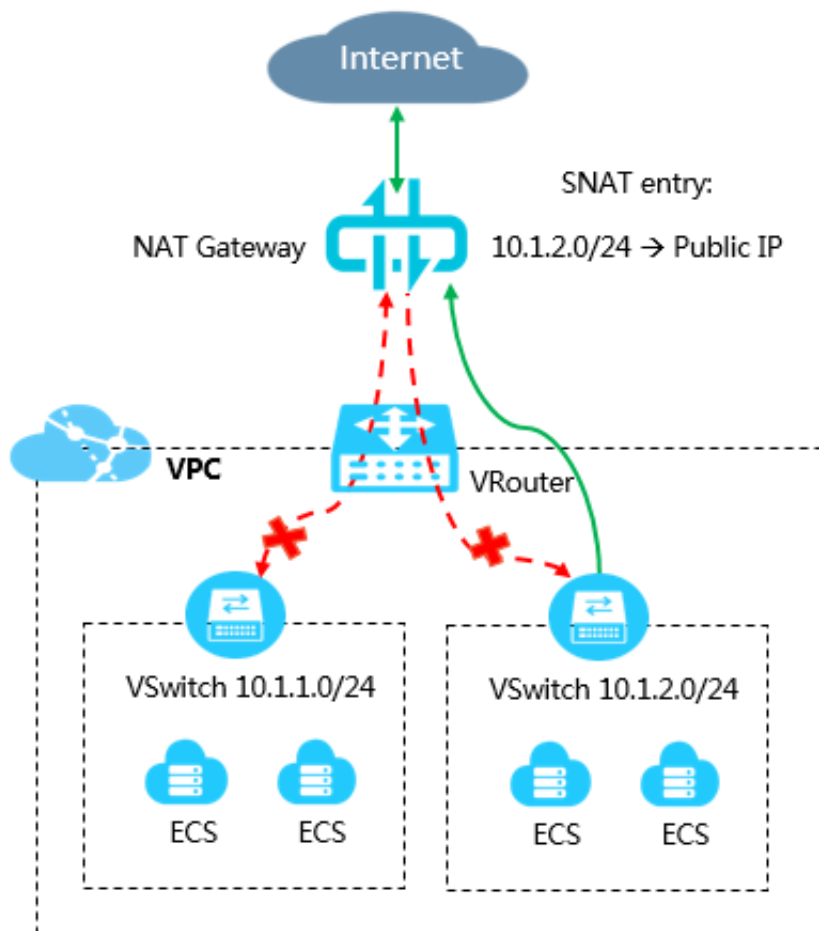
- Bind an EIP

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 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 create an instance, 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 cloud products such as ApsaraDB for RDS, you can change the network type from the classic network to VPC on the console.
- Alibaba Cloud supports switching a classic ECS instance to the VPC network.
- 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](#).

5 Migrate from the classic network to VPC

5.1 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 addition 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.

单ECS迁移方案

单ECS迁移方案，即无需通过创建镜像、重新购买等步骤就能把经典网络的ECS实例迁移到专有网络。

在控制台上完成迁移预约后，阿里云会根据您设置的迁移时间进行迁移，迁移完成后，您将收到迁移成功的短信消息提醒。

在使用单ECS迁移方案时，注意：

- 迁移过程中ECS需要进行重启，请关注对系统的影响。
- 迁移后，不需要进行任何特殊配置，ECS实例的公网IP都不变。
 - 虽然公网IP没有变化，但无法在ECS的操作系统中查看到这个公网IP（称之为VPC类型的ECS的固定公网IP）。您可以将按流量计费的ECS实例的固定公网IP转换为EIP，方便管理，详情参见[Change an ECS public IP to an EIP](#)。
 - 如果您的个别应用对ECS操作系统上可见的公网IP有依赖，迁移后会有影响，请谨慎评估。
- 迁移后，所有地域的ECS实例的私网IP都会变化。
- 迁移到的目标VPC的交换机的可用区必须和待迁移的ECS的可用区相同。
- 迁移过程中实例ID及登录信息不变。
- 包年包月购买方式的实例迁移过程中不需要额外付费。从新的计费周期开始，按照同规格专有网络的价格计算。且迁移到VPC后，ECS的使用费用会降低。
- 迁移前如有续费变配未生效订单或未支付订单，迁移后该订单将被取消且不能恢复，您需要重新下单。
- 迁移到VPC后，若ECS有使用其它云服务，需将访问方式调整到VPC访问方式(云产品混访方案)。

5.2 Database hybrid access

5.2.1 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/bypass 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 reservation time of the classic network endpoint. The classic network endpoint is automatically released when the time is reached.

Note the following limits on the hybrid access of ApsaraDB:

- Currently, the following databases support hybrid access:
 - ApsaraDB for RDS MySQL, SQL Server, PPAS and PostgreSQL in the safe connection 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 safe connection mode.
 - 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.

5.2.2 Change the network type of ApsaraDB for RDS

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

For more information, see [Migrate from the classic network to VPC](#).



Note:

- 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.
- If the RDS instance is a split table of a DRDS instance, the network connection between the DRDS and the RDS instances will be interrupted and you must reconnect them.

For more information, see [Repair link to branch database](#).

Prerequisites

- The access mode of the instance is the safe connection mode. For more information, see [Set access mode](#). MySQL 5.7, SQL Server 2012 and SQL Server The 2016 version only support the standard mode. This mode supports changing the network type.
- 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 where the target instance is located.
3. Click the ID of the target instance.
4. In the left-side navigation pane, select **Database Connection**.
5. In the **Instance Connection** tab, click **Switch to VPC**.
6. On the **Switch to VPC** page, select the VPC and VSwitch where the RDS instance is located.
7. Select the **Reserve original classic endpoint** check box, and select an **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 retention time of the classic network endpoint expires, the classic network endpoint will be automatically released, and you will not be able to access the database through the classic network endpoint. To prevent service interruption, set the retention time according to your needs. After the hybrid access configuration is complete, you can change the expiration time.
8. Click **OK**. A **Retained Connection Address of the Classic Network** is added on the console.

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. 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 in to the RDS Console.
2. Select the region where the target instance is located.
3. Click the ID of the target instance.
4. In the left-side navigation pane, select **Database Connection**.
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. 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">• <code>VPC</code>: An instance of the VPC network.• <code>Classic</code>: An instance of the classic network.
VPCId	String	No	The ID of the VPC.

Name	Type	Required	Description
VSwitchId	String	No	The ID of the VSwitch. This parameter must be specified if the VPC ID is specified.
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"> • <code>True</code>: Retain • <code>False</code>: Do not retain
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 <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_success() {
    ModifyDBInstanceNetworkTypeRequest request=new ModifyDBInstanceNetworkTypeRequest ();
    request.setInstanceId("<Your instance ID>");
    request.setInstanceNetworkType ("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 {
        ModifyDBInstanceNetworkTypeResponse response
            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: DescribeDBInstanceNetInfo
DBInstanceId	String	Yes	The ID of the instance.

Response parameters

Name	Type	Description
DBInstanceNetInfos	List	A list of the network information of the instance.
InstanceNetworkType	String	The network type of the instance. <ul style="list-style-type: none"> VPC: An instance of the VPC network. Classic: An instance of the classic network.

DBInstanceNetInfo

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

Example 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 {
            DescribeDBInstanceNetInfoResponse response
                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.
 - [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 retention time of the classic network endpoint.

Description on Request Parameter

Name	Type	Required	Field description
Action	String	Yes	required parameter. Value: Change the expiration time of the original classic endpoint .
DBInstanceId	String	Yes	ID of the target RDS instance.
ConnectionString	String	Yes	The classic network connection string to be postponed. There are two string types: the classic network endpoint of the current instance and the classic network endpoint separating reading and writing
ClassicExpiredDays	Integer	Yes	The retention time of the classic network endpoint is [1-120] days.

Response parameters

Name	Type	Description
RequestId	String	The ID of the request.

Example code

```
public static void main(String[] args) {  
    ModifyDBInstanceNetExpireTimeRequest request = new ModifyDBInstanceNetExpireTimeRequest();  
    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 {  
    ModifyDBInstanceNetExpireTimeResponse response  
        = client.getAcsResponse(request);  
    System.out.println(response.getRequestId());  
} catch (ServerException e) {  
    e.printStackTrace();  
}  
} catch (ClientException e) {  
    e.printStackTrace();  
}  
}
```

5.2.3 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:

When retaining the classic network endpoint is selected, ECS instances of the classic network can still access the database 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**.

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: <code>SwitchNetwork</code>
InstanceId	String	Yes	The ID of the instance.
TargetNetworkType	String	Yes	The network type of the instance. <ul style="list-style-type: none">• VPC: VPC

Name	Type	Required	Description
			<ul style="list-style-type: none"> Classic: Classic network
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 <code>False</code> : <ul style="list-style-type: none"> <code>True</code>: Retain <code>False</code>: Do not retain
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 <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

```
import com.aliyuncs.DefaultAcsClient;
import com.aliyuncs.IAcsClient;
import com.aliyuncs.exceptions.ClientException;
import com.aliyuncs.exceptions.ServerException;
import com.aliyuncs.profile.DefaultProfile;
import com.aliyuncs.profile.IClientProfile;
import com.aliyuncs.r_kvstore.model.v20150101.SwitchNetworkRequest;
import com.aliyuncs.r_kvstore.model.v20150101.SwitchNetworkResponse;
import org.junit.test;
/**
 * Created by wb259286 on 2017/6/9.
 */
public class SwitchNetworkTest {
    @Test
    public void switchNetwork_success() {
        SwitchNetworkRequest request=new SwitchNetworkRequest();
        request.setInstanceId("<your instance ID>");
        request.setTargetNetworkType("VPC");
    }
}
```

```

        request.setVpcId("<VpcId: This parameter is required when
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: DescribeDBInstanceNetInfo
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"> • VPC: An instance of the VPC network. • Classic: An instance of the classic network.

InstanceNetInfo

Name	Type	Description
ConnectionString	String	The connection string of DNS.

Name	Type	Description
IPAddress	String	The IP address.
IPType	String	The IP type of an instance of the classic network: Inner Public. The IP type of an instance of the VPC network: Private Public.
Port	String	The port information.
VPCId	String	The ID of the VPC.
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: <code>ModifyInstanceNetExpireTime</code> .
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());
        }
    } catch (Exception e) {
        e.printStackTrace();
    }
}
```

```
        System.out.println(item.getIPAddress());
        System.out.println(item.getExpiredTime());
    }
} catch (ServerException e) {
    e.printStackTrace();
}
} catch (ClientException e) {
    e.printStackTrace();
}
}
```

5.2.4 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 **Database Connection** 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 **Database Connection** 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: <code>ModifyDBInstanceNetworkType</code>
DBInstanceId	String	Yes	The ID of the instance.
NetworkType	String	Yes	The network type of the instance. <ul style="list-style-type: none">• <code>VPC</code>: VPC• <code>Classic</code>: Classic network
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 <code>False</code> : <ul style="list-style-type: none">• <code>True</code>: Retain• <code>False</code>: Do not retain
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 <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.

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: <code>DescribeReplicaSetRole</code>
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: <code>Primary</code> <code>Secondary</code>
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">• <code>VPC</code>: VPC• <code>Classic</code>: Classic network

5.3 Hybrid access of other products

Hybrid access means that the product can be accessed by both ECS instances of the classic network and ECS instances of 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](#)
- Archive Storage: [Obtain endpoints](#)

Application service

- Log Service: [Obtain endpoints](#)

Middleware

- Message Service: [Obtain endpoints](#)
- Message Queue
 - TCP access: [Obtain endpoints](#)
 - Management and control: [Obtain endpoints](#)
- Distributed Relational Database Service (DRDS):

Hybrid access is not supported. For more information, see [Obtain endpoints](#).

另外，如果要切换的RDS实例是DRDS实例的一个分库，当RDS切换了网络类型后，DRDS与RDS之间的网络连通性会被破坏，需要手动修复。详情参见[#####](#)。

Big data

- MaxCompute: [Obtain endpoints](#)
- DataHub: [Obtain endpoints](#)

Others

Currently, the following product only provides Internet endpoint:

- ApsaraVideo for Media Transcoding: [Obtain endpoints](#)

5.4 Example of hybrid access and hybrid addition migration

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

Prerequisites

Before migrating, make sure that:

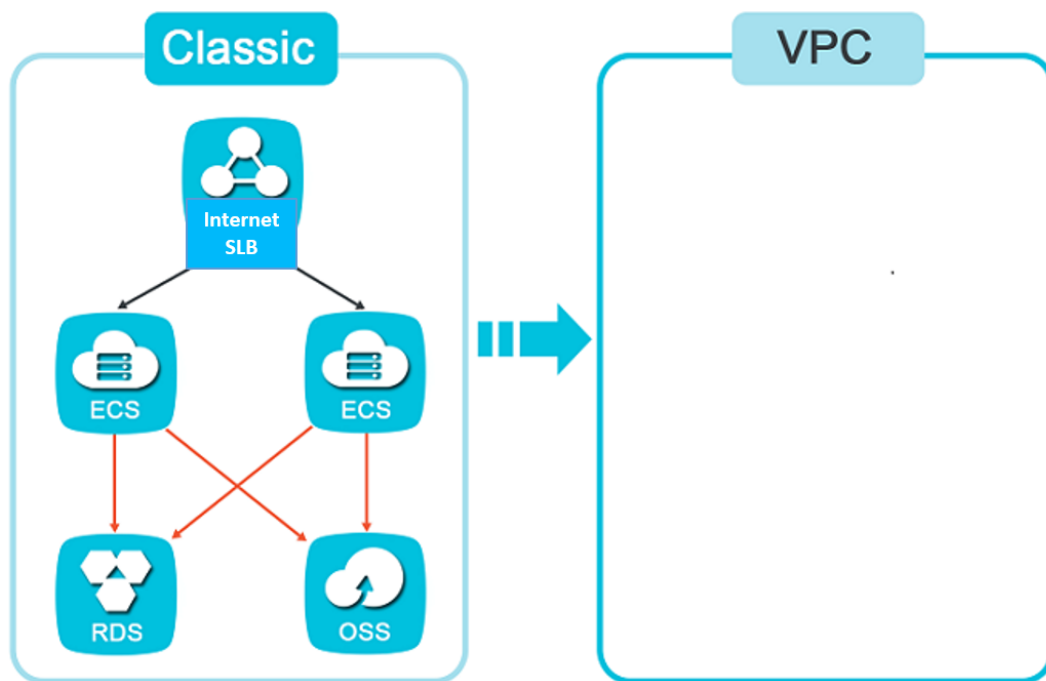
- You have known the details and limits of the migration. For more information, see [Migration overview](#).
- You are familiar with the VPC and the related products. VPC and the classic network are very different. Apart from the network isolation, VPC enables you to control your private network by using 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 precise migration plan.

Example systems

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

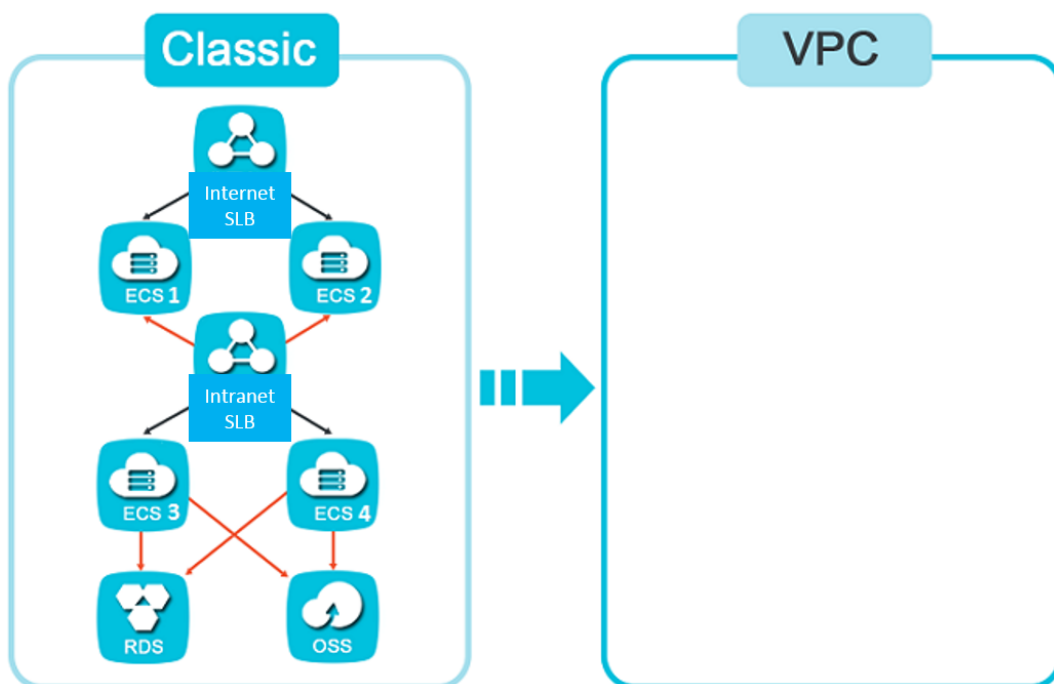
- **System 1**

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.



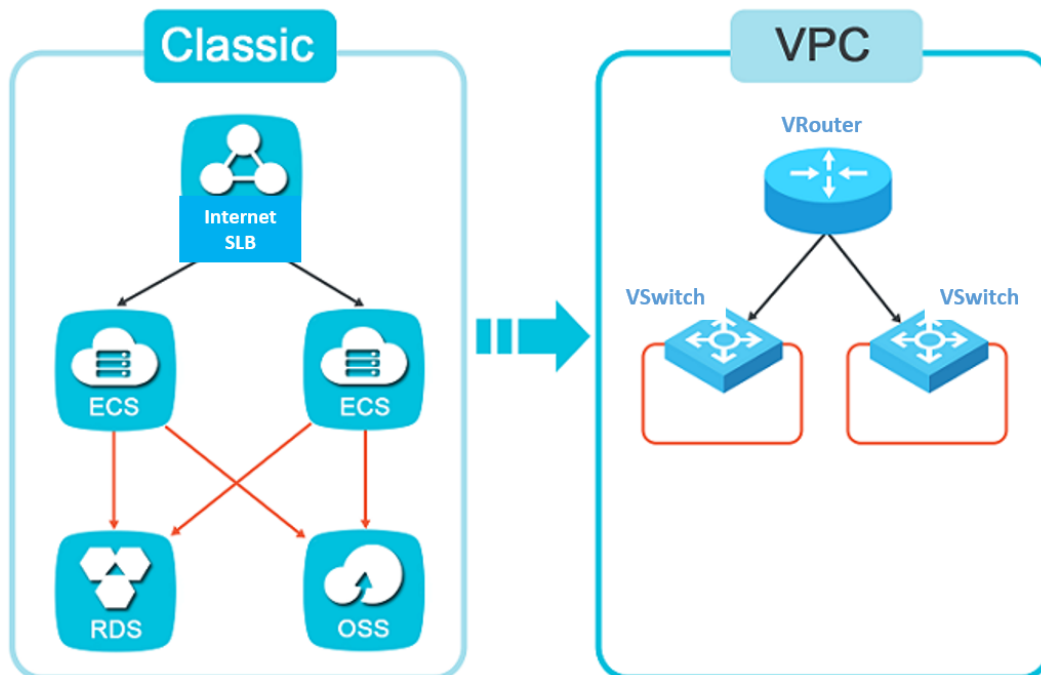
Migrate system 1 to VPC

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 [Build VPC](#).



2. Obtain the VPC endpoints of RDS and OSS.

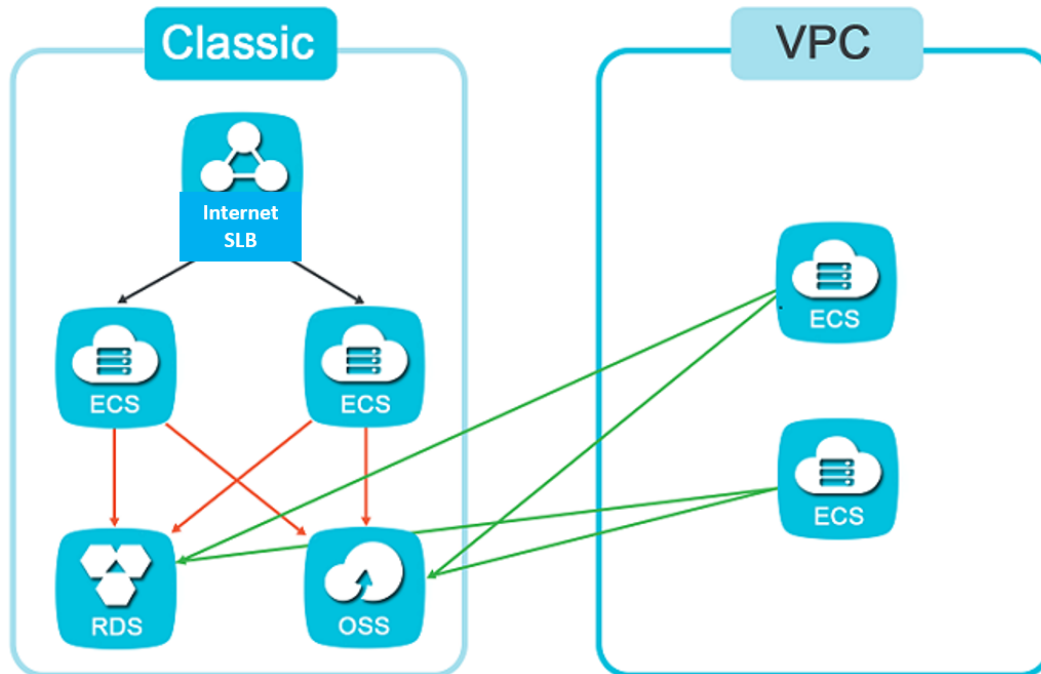
- You can migrate the RDS instance to the VPC either through the API or on the console and reserve its classic network endpoint at the same time. For more information, see [Change the network type of ApsaraDB for RDS](#).

After the migration, the classic network endpoint stays 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](#).

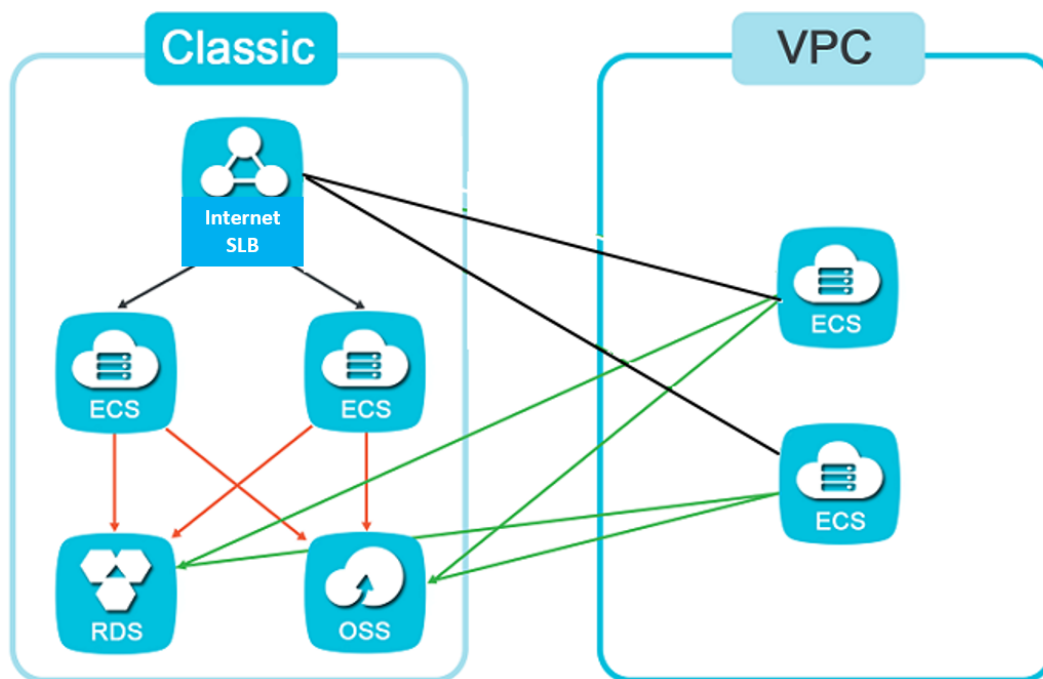
3. Create two ECS instances in the VPC and configure the ECS instances.

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.



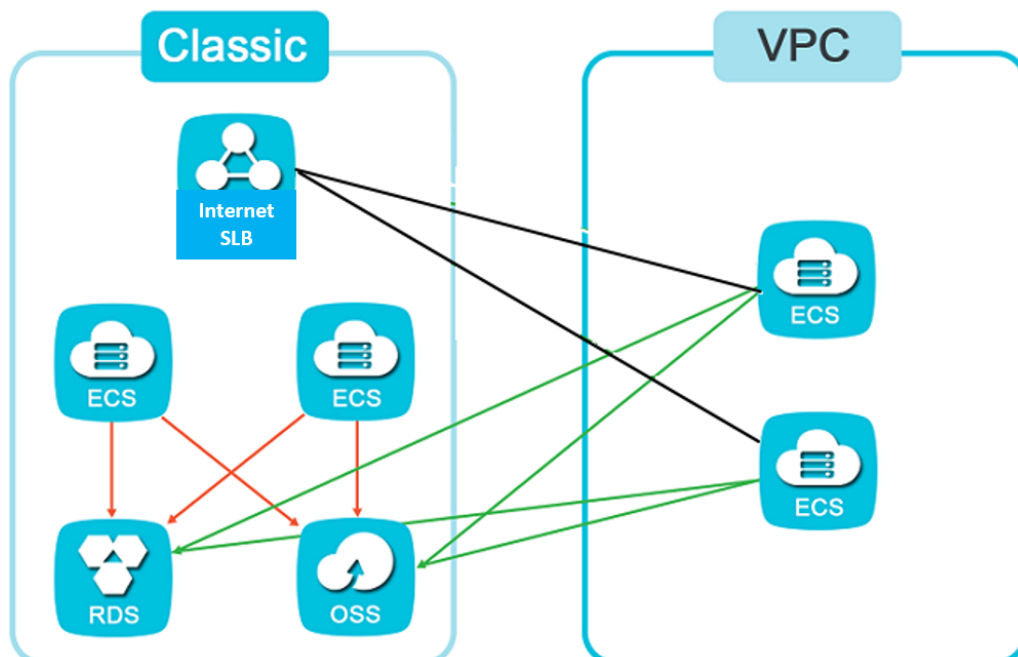
4. Add the ECS instances in the VPC to the Internet SLB instance.

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 0 and then remove them when no more traffic is distributed to them.

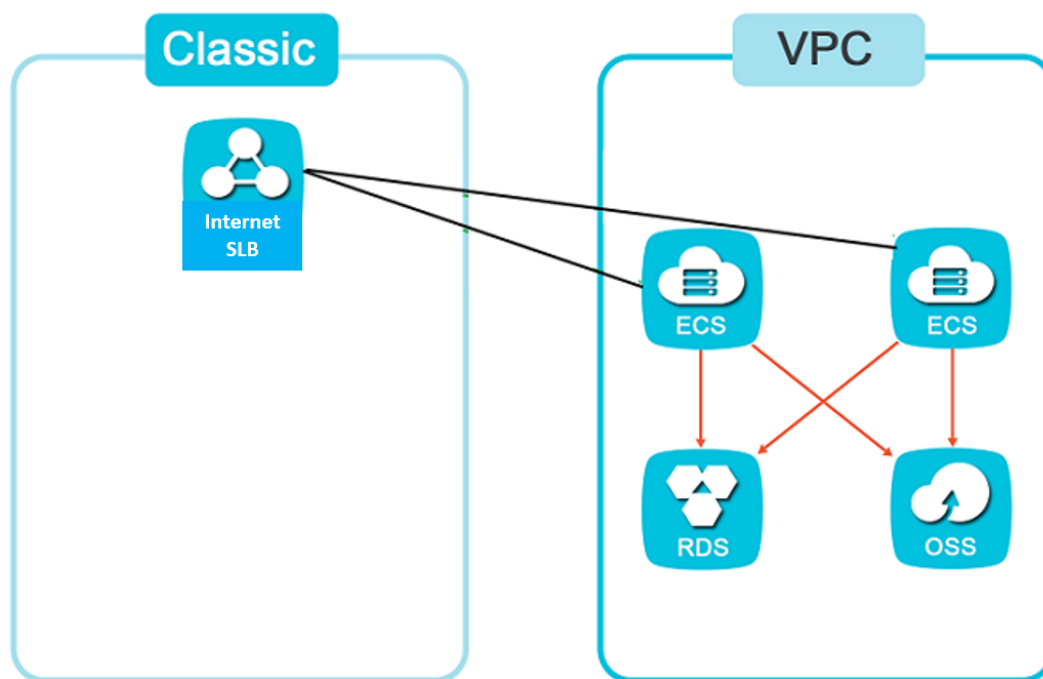


6. Release the instances of the classic network.

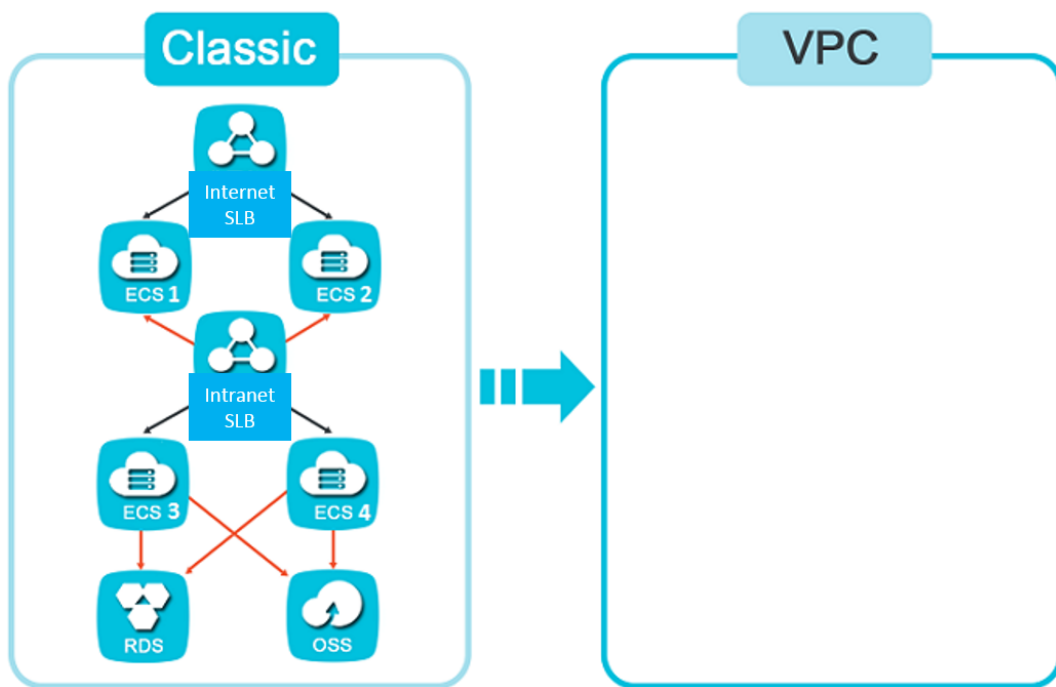
As shown in the following figure, release the ECS instances of the classic network after the system has been running normally for a period of time. The Internet SLB instance supports adding ECS instances of the VPC network itself, so no migration is required. Till now, you have finished the migration.

**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.