

Alibaba Cloud Virtual Private Cloud

Best practices

Issue: 20190918

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.	 Notice: 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.
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 How to choose a product to gain access to an intranet?.....	1
2 How to choose an Internet-facing product?.....	15
3 How to save the Internet cost?.....	20
4 How to use cloud products in a VPC?.....	25
5 Classic network-to-VPC migration.....	27
5.1 Overview of migration solutions.....	27
5.2 Hybrid access to ApsaraDB.....	29
5.2.1 Overview of the hybrid access mode of ApsaraDB.....	29
5.2.2 Switch the network type of an RDS instance.....	30
5.2.3 Switch the network type of a Redis instance.....	37
5.2.4 Switch the network type of a MongoDB instance.....	44
5.3 Cloud products that support hybrid access.....	48
5.4 Hybrid migration.....	49

1 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.

#unique_4/unique_4_Connect_42_section_wbw_gt5_sdb			
Product	Scenario	Benefits	Limits
Cloud Enterprise Network (CEN)	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
Express Connect	Establish a peering connection between two VPCs.	The connection between two VPCs in the same region is free of charge.	None
#unique_4/unique_4_Connect_42_section_klv_ft5_sdb			
Product	Scenario	Benefits	Limits

VPN Gateway	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 .
Cloud Enterprise Network (CEN)	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

Smart Access Gateway	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
-----------------------------	--	---	-------------

Express Connect	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 .
#unique_4/unique_4_Connect_42_section_ub1_r55_sdb			
Product	Scenario	Benefits	Limits
VPN Gateway	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

Smart Access Gateway + Express Connect	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
VPN Gateway	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.
#unique_4/unique_4_Connect_42_section_hdl_555_sdb			

Product	Scenario	Benefits	Limits
VPN Gateway (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
SSL-VPN software in 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.	High cost. Low reliability. You need to deploy and maintain the SSL-VPN software by yourself.

Connect VPCs

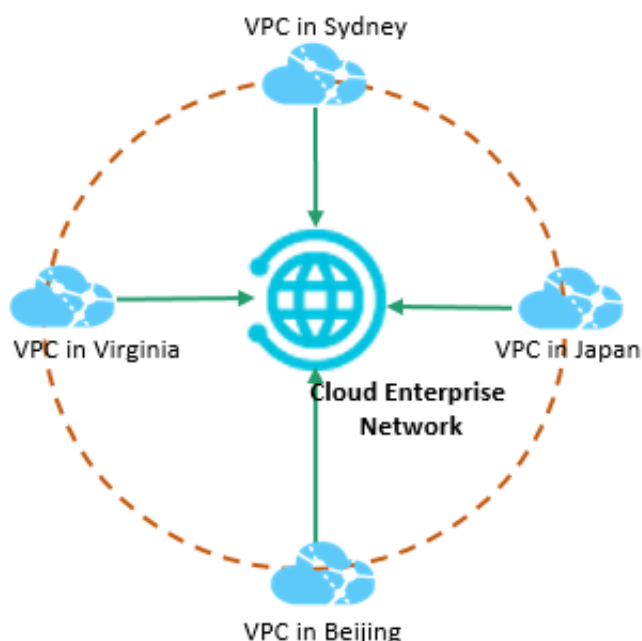
You can deploy different applications in different VPC networks to build a service network across regions. This architecture helps provide services from nearby locations, reduce network latency, achieve mutual backup and improve the reliability of the whole system.

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

- CEN

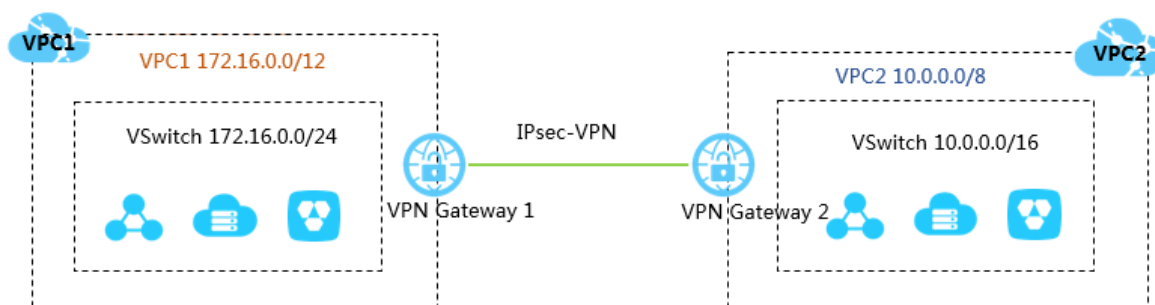
Cloud Enterprise Network (CEN) allows you to build an intranet-based communication channel between one or more VPCs. By using automatic route distribution and learning functions, CEN accelerates network convergence, improves the quality and security of cross-network communication, and interconnects resources

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

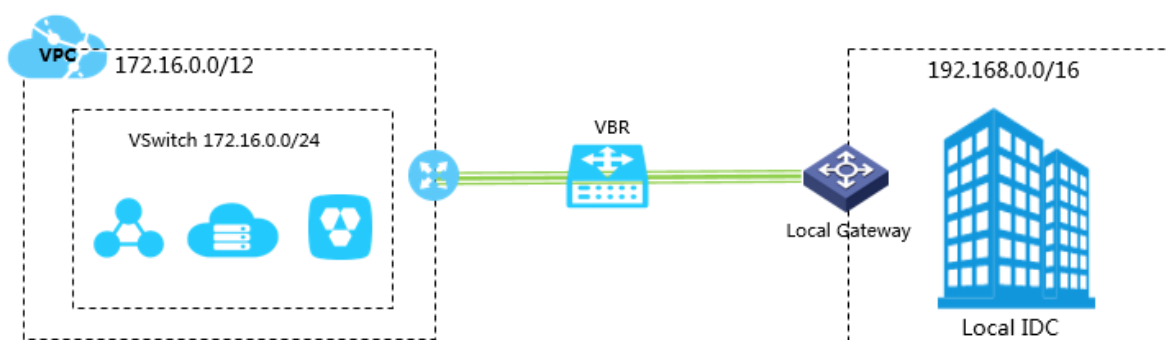
Alibaba Cloud, you can easily expand your local IT infrastructure to Alibaba Cloud to cope with changing service demands.

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.

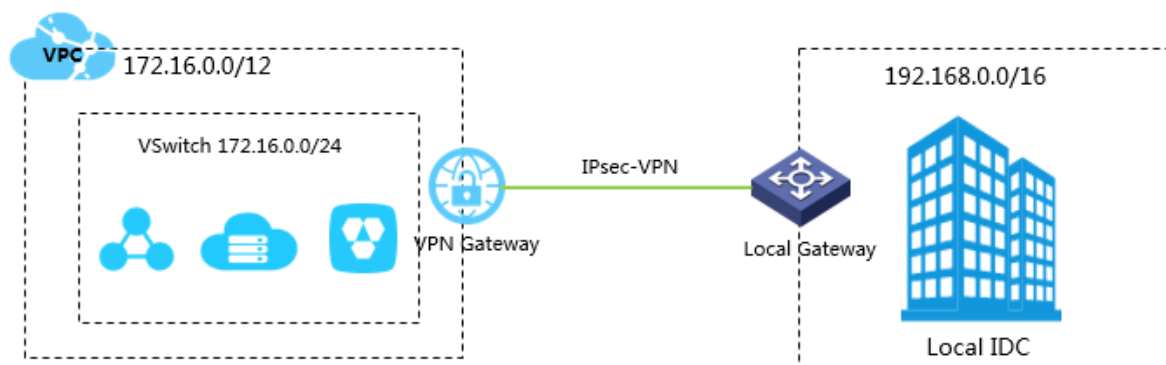
With Express Connect, the intranet connection of the leased line does not use the Internet. Therefore, compared with a traditional Internet connection, the physical connection features higher security, reliability, and speed while also providing lower network latency.



- VPN Gateway

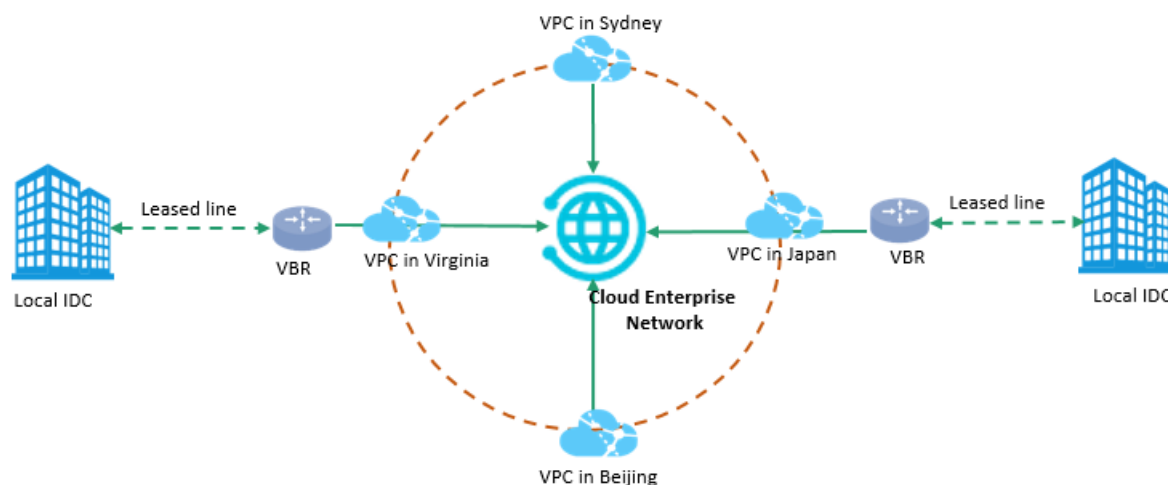
VPN Gateway can connect a local data center, a local site, an Internet terminal to a VPC in a secure and reliable way through an Internet-based and encrypted channel. VPN Gateway contains two different gateway instances which provide active/standby hot backup. The traffic is automatically distributed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

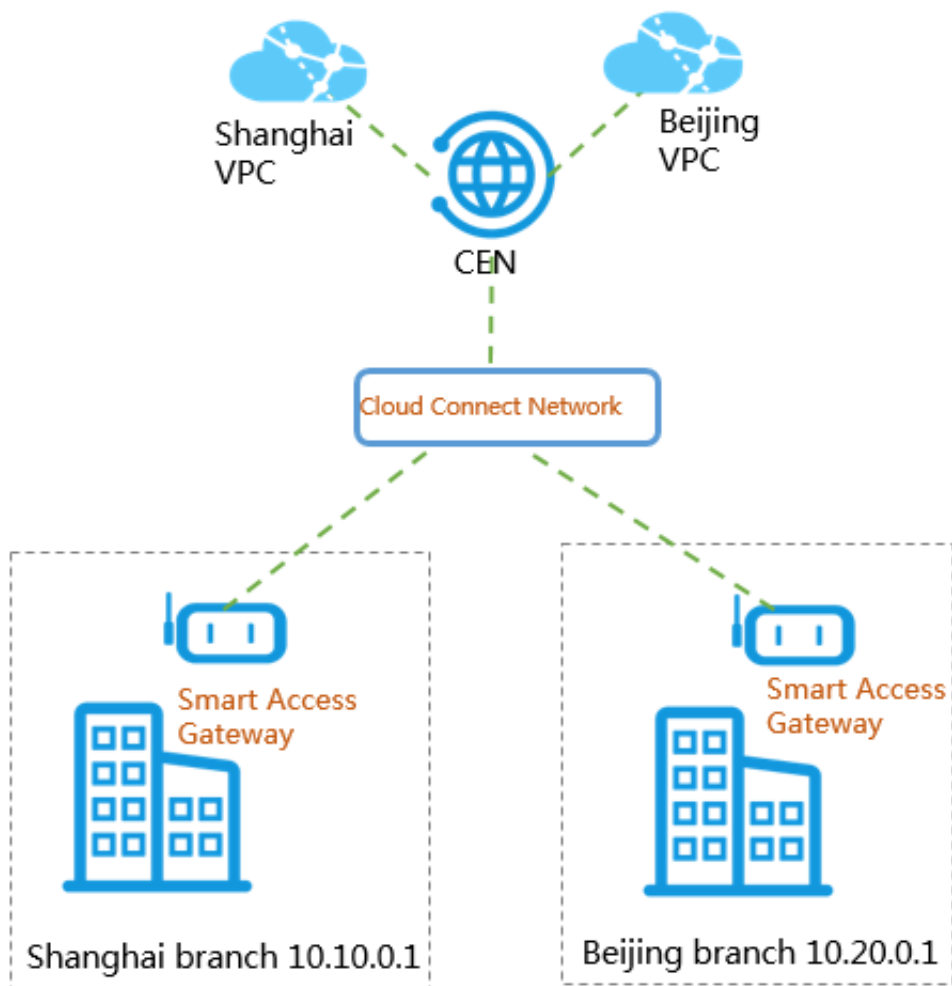


- Smart Access Gateway

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.

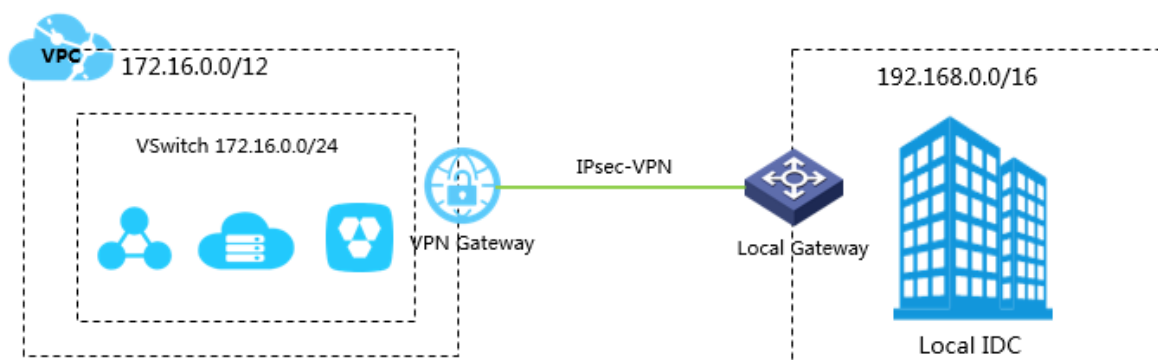
You can buy a Smart Access Gateway device for the local data center, and attach the CCN instance associated with the device to the CEN instance so as to connect the on-premises data center to Alibaba Cloud.



- 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

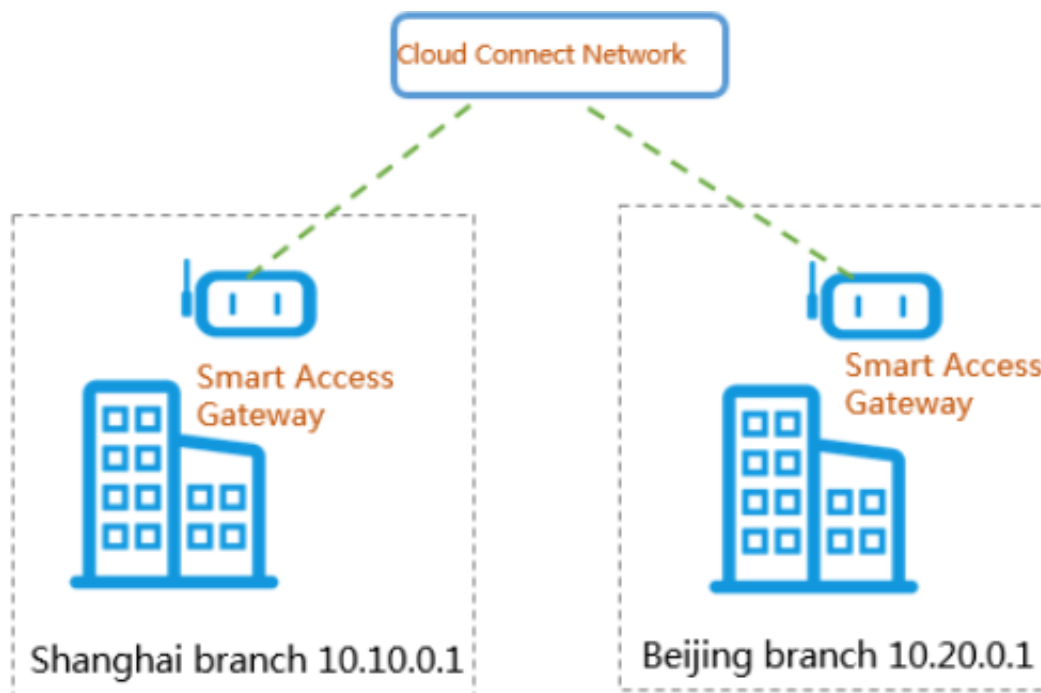
You can connect multiple sites through Smart Access Gateway or the VPN-Hub function of VPN Gateway.

- 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.



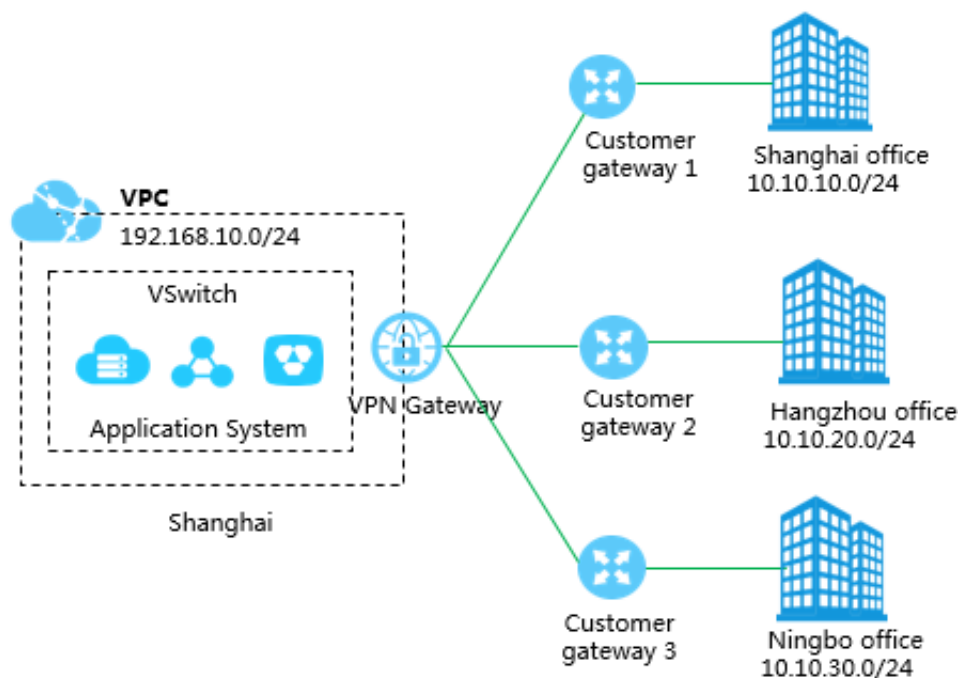
- VPN Gateway

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

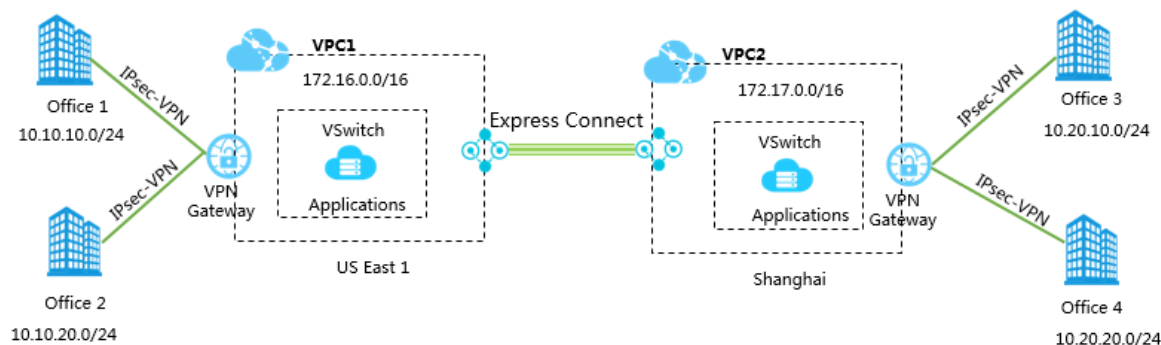
sites (Shanghai, Hangzhou, and Ningbo). In this example, you only need to create a VPN Gateway and three customer gateways, and establish three IPsec connections.



- 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

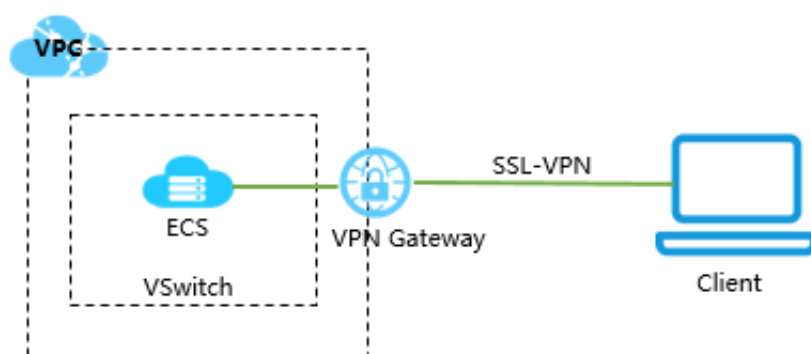
The SSL-VPN function of VPN Gateway provides site-to-site VPN connection.

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.

2 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	Function	Benefit
ECS public IP address	When you create a VPC ECS instance, you can assign the instance a public IPv4 address that supports access to or from the Internet. An ECS public IP address cannot be dynamically disassociated from the corresponding VPC ECS instance, but can be converted to an EIP. For more information, see #unique_10.	You can use Data Transfer Plan. After changing a public IP address to an EIP, you can also use Internet Shared Bandwidth.

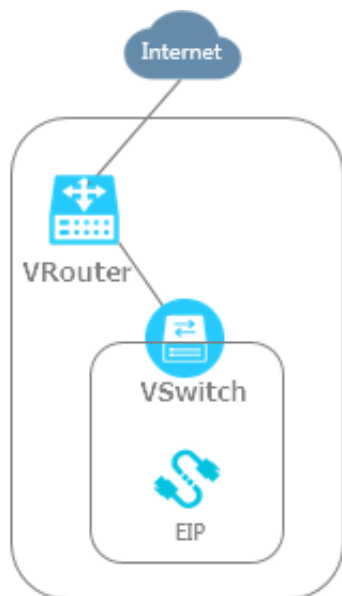
Product	Function	Benefit
Elastic IP (EIP)	With an EIP, the ECS instance can access the Internet (SNAT) and can be accessed from the Internet (DNAT).	You can associate an EIP with or disassociate an EIP from an ECS instance at any time. You can use Internet Shared Bandwidth and Data Transfer Plan to reduce Internet cost.
NAT Gateway	NAT Gateways allow multiple VPC ECS instances to access the Internet (SNAT) and be accessed from the Internet (DNAT).  Note: Compared with Server Load Balancer (SLB), NAT Gateways does not provide the traffic balancing function.	A NAT Gateway can be used for multiple ECS instances to access the Internet, while an EIP can be used for only one VPC ECS instance to access the Internet.
SLB	SLB provides layer 4 and layer 7 server load balancing, which allows access to ECS instances from the Internet.  Note: VPC ECS instances cannot access the Internet (SNAT) through SLB.	In DNAT, SLB can forward an Internet request to multiple ECS instances. SLB can distribute traffic to multiple ECS instances to expand service capabilities and improve availability of applications. After you associate an EIP with an SLB instance, you can use Internet Shared Bandwidth and Data Transfer Plan to reduce Internet cost.

Scenario 1: Provide external services

- Provide external services with a single ECS instance

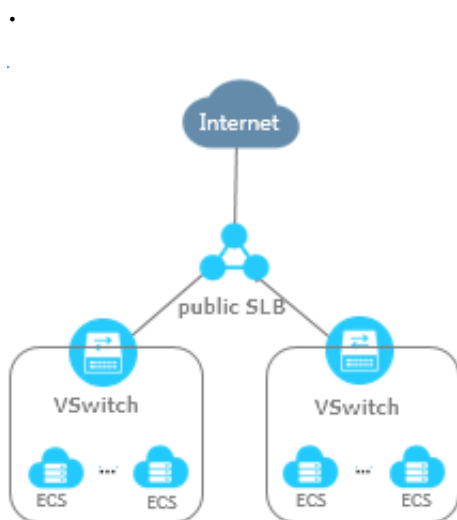
If you have only one application and the business is not large, a single ECS instance can meet your requirements. You can deploy applications, databases, and files

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

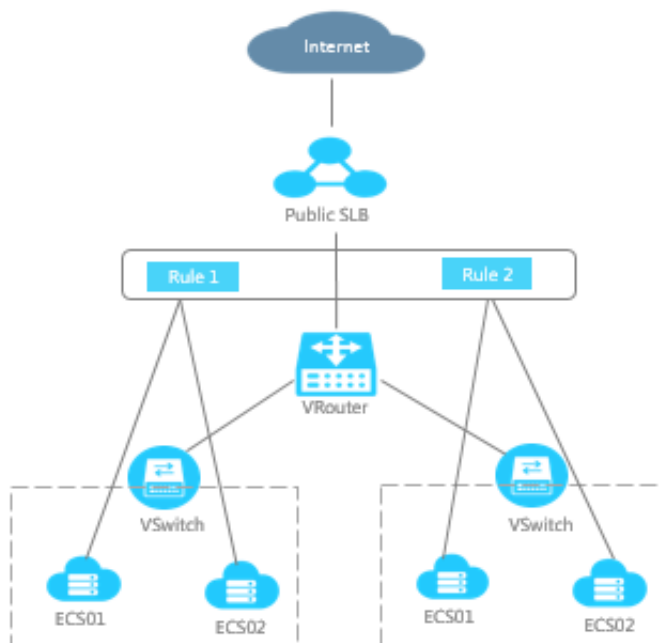
When the traffic is large, one ECS cannot support all access traffic. You must configure multiple ECS instances. In this case, you can configure an Internet SLB instance with a Layer-4 listener and add these ECS instances as the backend servers



- 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

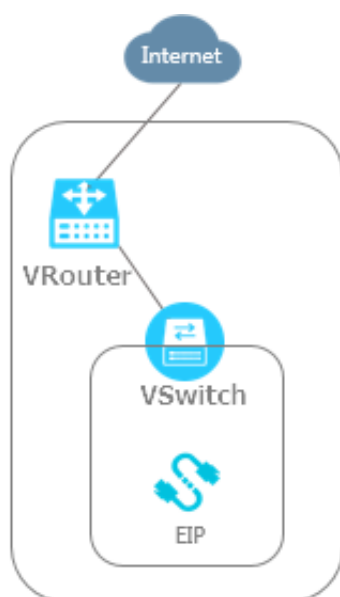
-7 listener. In this case, you can configure an Internet SLB instance with a Layer-7 listener and add these ECS instances as the backend servers.



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

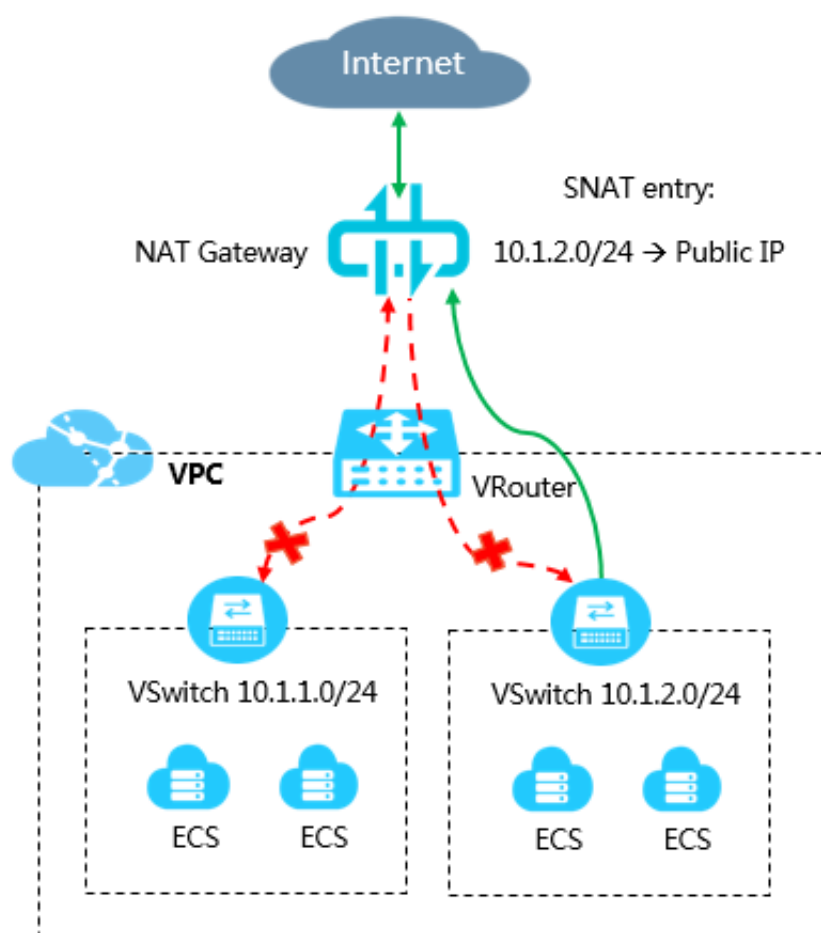
- Bind an EIP

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.



3 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, China 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, China 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, China 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.

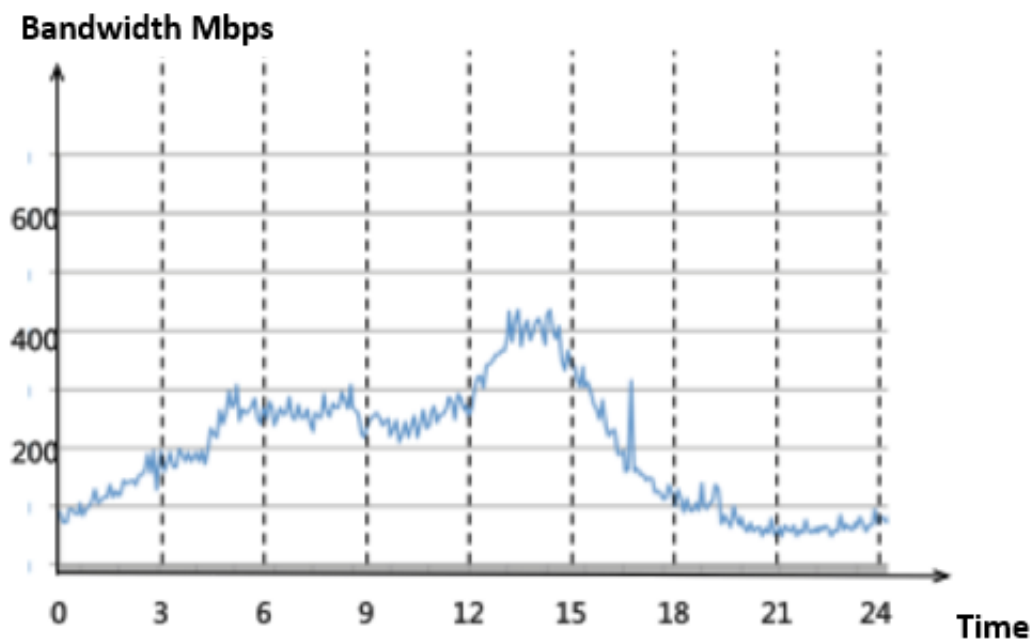


Note:

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, China 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>Hong Kong</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)	Hong Kong	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)	Hong Kong	Japan (Tokyo)	Singapore	Australia (Sydney)	Malaysia (Kuala Lumpur)															
Indonesia (Jakarta)	India (Mumbai)	US (Virginia)	US (Silicon Valley)	UAE (Dubai)	Germany (Frankfurt)															
Billing Method	☒ Pay by Bandwidth	Billing Method: Pay by Bandwidth Billing Cycle: 1 hour(s)																		
Bandwidth	☒ 500 Mbps	Bandwidth: 500Mbps Name: - Purchase Quantity: 1 Fee: CN¥70.000 / hour(s)																		
Name		Buy Now 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.

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 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 [#unique_15](#).

5 Classic network-to-VPC migration

5.1 Overview of migration solutions

This topic provides an overview of the solutions that are used to migrate cloud resources from a classic network to a Virtual Private Cloud (VPC). Compared with a classic network, a VPC is an isolated network environment with higher security.

Benefits

A VPC is a private network in Alibaba Cloud. You can use Alibaba Cloud resources in your VPC. The benefits of VPCs are as follows:

- Secure network environment

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

- Flexible network configurations

You can specify the IP address range and configure route tables and gateways in your VPC. Furthermore, you can connect your VPC to other VPCs or on-premises data centers to create a custom network environment through a physical connection or VPN. In this way, you can smoothly migrate applications to the cloud and extend on-premises data centers.

Migration solutions

You can use two solutions (hybrid migration and single ECS migration) to migrate your cloud resources from a classic network to a VPC. The two solutions can be used independently or together to meet your requirements in different scenarios.

- Hybrid migration

We recommend that you use the hybrid migration solution if your system is deployed on RDS, SLB, or other cloud products. By using this solution, you can migrate your system to a VPC without service disruptions.

Furthermore, this solution can be used along with the ClassicLink function to allow ECS instances in the classic network to access cloud resources in the VPC.

For more information, see [#unique_18](#).

- Single ECS migration

We recommend that you use the single ECS migration solution if your applications are deployed on an ECS instance and also if restarting the ECS instance does not affect your system.

Hybrid migration

The hybrid migration is a seamless migration solution that consists of hybrid access and hybrid attachment. This solution allows you to create a cloud instance (such as ECS instance) in a VPC and then migrate your system to the VPC. After all your systems are migrated to the VPC, you can release the cloud resources in the classic network. For more information, see [#unique_19](#).

- Hybrid attachment

Hybrid attachment refers to attaching a classic-network ECS instance and a VPC ECS instance to a Server Load Balancer (SLB) instance as backend servers to process forwarded requests. Hybrid attachment also allows you to attach a classic-network ECS instance and a VPC ECS instance to a VServer group.

Hybrid attachment is supported by Internet and intranet SLB instances.



Note:

If you attach a classic-network ECS instance and a VPC ECS instance to an intranet SLB instance and configure a layer-4 (TCP and UDP) listener, you can obtain the real client IP address from the VPC ECS instance, but cannot obtain this address from the classic-network ECS instance. If you configure a layer-7 (HTTP and HTTPS) listener, you can obtain the real client IP address from the VPC ECS instance and the classic-network ECS instance.

- Hybrid access

Hybrid access refers to a process during which classic-network ECS instances and VPC ECS instances access RDS, OSS, or other cloud products at the same time. These products have two endpoints. One is used to access the classic network and the other is used to access the VPC.

When you use the hybrid migration solution, note the following:

- If the classic-network ECS instances and VPC ECS instances in your system need to communicate with each other, you can use the ClassicLink function.

- This solution applies only to the migration of your system from a classic network to a VPC.

5.2 Hybrid access to ApsaraDB

5.2.1 Overview of the hybrid access mode of ApsaraDB

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

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

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

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

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

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

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

5.2.2 Switch the network type of an RDS instance

This topic describes how to switch the network type of an RDS instance from a classic network to a VPC by using the console or by calling the relevant API action.

For more information, see [#unique_23](#).



Note:

- When you switch the network type, you can specify a retention period for the classic network endpoint. After the retention period expires, the classic network endpoint is automatically deleted. Before the endpoint is deleted, you will receive a message.
- If the RDS instance is a subdatabase of a DRDS instance, the connection between the DRDS and the RDS instance will be broken after the network type is changed and must be manually reconnected.

Prerequisites

- The network type of the RDS instance is the classic network.
 - VPCs and VSwitches are available in the zone to which the RDS instance belongs.
- For more information, see [#unique_24](#).

Method 1 - Switch the network type by using the console

1. Log on to the ApsaraDB for RDS console.
2. Select the region to which the target instance belongs.
3. Click the ID of the target instance.
4. In the left-side navigation pane, select Database Connection.
5. On the Instance Connection tab page, click Switch to VPC Network.
6. On the Switch to VPC Network page, select the target VPC and VSwitch.

7. Select **Reserve original classic endpoint**, and then select the **Expiration time**.

- From the seventh day before the classic network endpoint is deleted, the system will send a message to the mobile phone associated with your account every day.
- When the classic network endpoint expires, it is automatically deleted and you cannot access the database through the classic network endpoint. To avoid service disruptions, set the retention period according to your specific needs. After you configure the hybrid access mode, you can change the expiration time.

8. Click **OK**. An **Original classic endpoint** is added in the console.

Modify the retention period of the classic network endpoint through the console

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

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

1. Log on to the ApsaraDB for RDS console.
2. Select the region to which the target instance belongs.
3. Click the ID of the target instance.
4. In the left-side navigation pane, select **Database Connection**.
5. On the **Instance Connection** tab page, click **Change Expiration Time**.
6. Select the expiration time and click **OK**.

Method 2 - Switch the network type by calling the relevant API action

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 action to switch the network type.

Request parameters

Parameter	Type	Required ?	Description
Action	String	Yes	The name of this action. Valid value: ModifyDBInstanceNetworkType
DBInstanceId	String	Yes	The ID of the Instance.
InstanceNetworkType	String	Yes	The network type of the instance. Valid values: • VPC : VPC instance. • Classic : classic-network instance
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.
PrivateIpAddress	String	No	An IP address in the VSwitch CIDR block. If no IP address is entered, the system assigns a private IP address according to the VPC ID and the VSwitch ID.
RetainClassic	String	No	Indicates whether to retain the classic network endpoint. Default: False . • True : The classic network endpoint will be retained. • False : The classic network endpoint will not be retained.

Parameter	Type	Required?	Description
ClassicExpiredDays	String	No	The retention period of the classic network endpoint in days. The shortest period is 1 day, the longest period is 180 days, and the default period is 7 days. This parameter must be specified if RetainClassic is set to True.

Response parameters

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

Example code

If you want to retain the classic network endpoint:

- Set the RetainClassic parameter to True.
- Set the ClassicExpiredDays parameter. After the classic network endpoint expires, it will be deleted.

```
import com.aliyuncs.DefaultAcsClient;
import com.aliyuncs.IAcsClient;
import com.aliyuncs.exceptions.ClientException;
import com.aliyuncs.exceptions.ServerException;
import com.aliyuncs.profile.DefaultProfile;
import com.aliyuncs.profile.IClientProfile;
import com.aliyuncs.rds.model.v20140815.ModifyDBInstanceNetworkTypeRequest;
import com.aliyuncs.rds.model.v20140815.ModifyDBInstanceNetworkTypeResponse;
import org.junit.Test;
public class ModifyDBInstanceNetworkTypeTest {
    @Test
    public void switchNetwork_success() {
        ModifyDBInstanceNetworkTypeRequest request = new
        ModifyDBInstanceNetworkTypeRequest();
        request.setInstanceId("< Your instance ID >");
        request.setInstanceNetworkType("VPC");
        request.setVPCId("< VpcId: This parameter is
        required when the TargetNetworkType is VPC >");
        request.setVSwitchId("< VSwitchId: This parameter
        is required when the TargetNetworkType is VPC >");
        request.setRetainClassic("< Whether to retain
        the classic network endpoint >");
    }
}
```

```

        request . setClassic ExpiredDays (" The retention
period of the classic network endpoint ");
        IClientProfile profile = DefaultProfile .
getProfile (" cn - hangzhou ", "< Your AK >",
"< Your Security >");
        IAcsClient client = new DefaultAcsClient ( profile
);
        try {
            ModifyDBInstanceNetworkTypeResponse response
= client . getAcsResponse ( request );
            System . out . println ( response . getRequest Id
());
        } catch ( ServerException e ) {
            e . printStackTrace ();
        }
        catch ( ClientException e ) {
            e . printStackTrace ();
        }
    }
}

```

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

Request parameters

Parameter	Type	Required?	Description
Action	String	Yes	The name of this action. Valid value: DescribeDBInstanceNetInfo
DBInstanceId	String	Yes	The ID of the Instance.

Response parameters

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

DBInstanceNetInfo

Parameter	Type	Description
ConnectionString	String	The connection string of DNS.

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

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.DescribeDBInstanceNe tInfoRequest;
import com.aliyuncs.rds.model.v20140815.DescribeDBInstanceNe tInfoResponse;
import org.junit.Test;
public class DescribeDB InstanceNe tInfoTest {
    @Test
    public void describeDB InstanceNe tInfo_success () {
        DescribeDB InstanceNe tInfoRequest request = new
        DescribeDB InstanceNe tInfoRequest ();
        request.setInstanc eId("< Your instance ID >");
        IClientProfile profile = DefaultProfile .
        getProfile ("cn - hangzhou ", "< Your AK >",
        "< Your Security >");
        IAcsClient client = new DefaultAcs Client ( profile
        );
        try {
            DescribeDB InstanceNe tInfoResponse 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 ();
        }
    }
}

```

```
}
```

Modify the retention period of the classic network endpoint through the relevant 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 `ModifyDBInstanceNetworkExpireTime` API action to modify the retention period of the classic network endpoint.

Request parameters

Parameter	Type	Required?	Description
Action	String	Yes	The name of this action. Valid value: <code>ModifyDBInstanceNetworkExpireTime</code> .
DBInstanceId	String	Yes	The ID of the instance.
ConnectionString	String	Yes	The classic network endpoint whose retention period you want to extend. Classic network endpoints are divided into the classic network endpoint of the current instance and the classic network endpoint with separate read and write.
ClassicExpiredDays	Integer	Yes	The retention period of the classic network endpoint. Value range: 1 to 120 days.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Example code

```
public static void main ( String [] args ) {  
    ModifyDBInstanceNetworkExpireTimeRequest request = new  
    ModifyDBInstanceNetworkExpireTimeRequest ();  
}
```

```

        request . setClassic ExpiredDay s ( 3 );
        request . setConnect ionString ("< The link string >");
        request . setDBInsta nceId ("< The instance ID >");
        IClientPro file profile
            = DefaultPro file . getProfile (" cn - qingdao ", "<
Your AK >",
            "< Your SK >");
        IAcsClient client = new DefaultAcs Client ( profile );
        try {
            ModifyDBIn stanceNetE xpireTimeR esponse 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 ();
        }
    }
}

```

5.2.3 Switch the network type of a Redis instance

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

Prerequisites

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

- The network type of the Redis instance is the classic network.
- VPCs and VSwitches are available in the zone to which the Redis instance belongs. For more information, see [#unique_24/unique_24_Connect_42_section_ufr_rhv_rdb](#).

Switch the network type by using the console

1. Log on to the ApsaraDB for Redis console.
2. Select the region to which the target instance belongs.
3. Click the ID of the target instance.
4. On the Instance Information page, click Switch to VPC Network.

5. In the displayed dialog box, complete these settings:

- Select the target VPC and VSwitch.
- Select to retain the classic network endpoint and select a retention period.



Note:

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

c. Click OK.

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

The screenshot shows the ApsaraDB for Redis console interface. At the top, there's a header for instance 'test1111' (Running) with buttons for 'Log into Database', 'Migrate Database', 'Refresh' (highlighted with a red box), 'Modify Password', 'Clear Data', 'Upgrade', and 'Downgrade'. Below this is the 'Instance Information' section. It contains a table with basic information: Instance ID, Instance Name, Status (Running), Zone, Network (VPC), Maintenance Window, Instance Type, VSwitch ID, Maximum Internal Bandwidth, Version, and Lua Status. Below the table is the 'Connection Information' section, which includes fields for Internal Connection Address (Host), Port Number (6379), Public endpoint (Host), and Connection Password. A note states: 'Note: The VPC may change during service maintenance. We recommend that you use the specified connection strings to connect to the target instance.' At the bottom, there's a section for 'Retained Classic Network IP Address (Expires in 3 Days)' with a 'Change Expiration Date' button and a dropdown arrow.

Modify the retention period of the classic network endpoint through the console

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

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

1. Log on to the ApsaraDB for Redis console.

2. Select the region to which the target instance belongs.
3. Click the ID of the target instance.
4. In the Retained Classic Network IP Address area, click Change Expiration Date.
5. In the displayed dialog box, select a new expiration date, and then click OK.

Switch the network type by calling the relevant API action

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 action to switch the network type.

Request parameters

Parameter	Type	Required ?	Description
Action	String	Yes	The name of this action. Valid value: SwitchNetwork
InstanceId	String	Yes	The ID of the instance.
TargetNetworkType	String	Yes	The network type of the instance. Valid values: · VPC : a VPC instance · Classic : a classic-network instance
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.

Parameter	Type	Required?	Description
RetainClassic	String	No	Indicates whether to retain the classic network endpoint. Default: <code>False</code> . <code>True</code>: The classic network endpoint will be retained. <code>False</code>: The classic network endpoint will not be retained.
ClassicExpiredDays	String	No	The retention period of the classic network endpoint in days. The shortest period is 1 day, the longest period is 120 days, and the default period is 7 days. This parameter must be specified if <code>RetainClassic</code> is set to <code>True</code> .

Response parameters

Parameter	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
period 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 action to view the classic network endpoint and the VPC endpoint.

Request parameters

Parameter	Type	Required?	Description
Action	String	Yes	The name of this action. Valid value: DescribeDBInstanceNetInfo
InstanceId	String	Yes	The ID of the instance.

Response parameters

Parameter	Type	Description
NetInfoItems	List	The connection information of the instance.

Parameter	Type	Description
InstanceNetworkType	String	The network type of the instance. Valid values: - VPC : a VPC instance. - Classic : a classic-network instance.

InstanceNetInfo

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

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.DescribeDBInstanceNetworkInfoRequest;
import com.aliyuncs.r_kvstore.model.v20150101.DescribeDBInstanceNetworkInfoResponse;
import org.junit.Test;

/**
 *
 */
public class DescribeDBInstanceNetworkInfoTest {
    @Test
    public void describeDBInstanceNetworkInfo_success() {
        DescribeDBInstanceNetworkInfoRequest request = new DescribeDBInstanceNetworkInfoRequest();
        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 period of the classic network endpoint through the relevant 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 ModifyInstanceNetExpireTime API action to switch the network type.

Request parameters

Parameter	Type	Required?	Description
Action	String	Yes	The name of this action. Valid value: ModifyInstanceNetExpireTime.
InstanceId	String	Yes	The ID of the instance.
Connection String	String	Yes	The classic network endpoint.

Parameter	Type	Required?	Description
ClassicExpiredDays	Integer	Yes	The retention period. Valid values: 14, 30, 60, or 120.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Example code

```

public static void main ( String [] args ) {
    ModifyInstanceNetExpirationTimeRequest request = new
    ModifyInstanceNetExpirationTimeRequest ();
    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 {
        ModifyInstanceNetExpirationTimeResponse 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 ();
    }
}

```

5.2.4 Switch the network type of a MongoDB instance

This topic describes how to switch the network type of a MongoDB instance from classic network to VPC by using the console or by calling the relevant API action.

When you switch the network type, you can specify a retention period for the classic

network endpoint. After the retention period expires, the classic network endpoint is automatically deleted.

Prerequisites

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

- The network type is the classic network.
- The instance type must be MongoDB replica set.
- VPCs and VSwitches are available in the zone to which the MongoDB instance belongs. For more information, see [#unique_24/unique_24_Connect_42_section_ufw_rhv_rdb](#).

Switch the network type by using the console

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



Note:

After you select to retain the classic network endpoint, classic-network ECS instances can access the database normally. When the classic network endpoint expires, it is automatically deleted 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.

Intranet Connection - VPC

Enable password-free access

Switch to Classic Network

Update Connection String

Role	Address
Primary	dds-bp1oeead55ba9541813.mongodb.rds.aliyuncs.com:3717
Secondary	dds-bp1oeead55ba9542725.mongodb.rds.aliyuncs.com:3717
ConnectionStringURI	mongodb://root:****@dds-bp1oeead55ba9541813.mongodb.rds.aliyuncs.com:3717,dds-bp1oeead55ba9542725.mongodb.rds.aliyuncs.com:3717?readPreference=primary&replicaSet=rs01

Public IP Connection

Apply for Public Connection String

Role	Address
No data is available	

Retained Classic Network Address - Expire at Oct 1, 2019

Change Expiration Time

Role	Address
Primary	dds-bp1oeead55ba9541813.mongodb.rds.aliyuncs.com:3717
Secondary	dds-bp1oeead55ba9542725.mongodb.rds.aliyuncs.com:3717
ConnectionStringURI	mongodb://root:****@dds-bp1oeead55ba9541813.mongodb.rds.aliyuncs.com:3717,dds-bp1oeead55ba9542725.mongodb.rds.aliyuncs.com:3717?readPreference=primary&replicaSet=rs01

Switch the network type by calling the relevant API action

1. Download the SDK.
 - [aliyun-python-sdk-dds.zip](#)
 - [aliyun-java-sdk-dds.zip](#)
 - [aliyun-php-sdk-dds.zip](#)
2. Call the `ModifyDBInstanceNetworkType` to switch the network type.

Request parameters

Parameter	Type	Required ?	Description
Action	String	Yes	The name of this action. Valid value: ModifyDBInstanceNetworkType
DBInstanceId	String	Yes	The ID of the Instance.
NetworkType	String	Yes	The network type of the instance. • VPC : a VPC instance. • Classic : a classic-network instance.
VPCId	String	No	The ID of the VPC.

Parameter	Type	Required ?	Description
VSwitchId	String	No	The ID of the VSwitch. This parameter must be specified if the VPC ID is specified.
RetainClassic	String	No	Indicates whether to retain the classic network endpoint. Default: <code>False</code> . <code>True</code> : The classic network endpoint will be retained. <code>False</code> : The classic network endpoint will not be retained.
ClassicExpiredDays	String	No	The retention period of the classic network endpoint in days. The shortest period is 1 day, the longest period is 120 days, and the default period is 7 days. This parameter must be specified if <code>RetainClassic</code> is set to <code>True</code> .

Response parameters

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

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

Request parameters

Parameter	Type	Required ?	Description
Action	String	Yes	The name of this action. Valid value: <code>DescribeReplicaSetRole</code>

Parameter	Type	Required ?	Description
DBInstance Id	String	Yes	The ID of the instance.

Response parameters

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

ReplicaSetRole

Parameter	Type	Description
ReplicaSet Role	String	The replica set role. Valid values: Primary Secondary .
Connection Domain	String	The connection domain of the instance.
Connection Port	String	The connection port of the instance.
ExpiredTime	String	The remaining retention period of the classic network endpoint in seconds.
NetworkType	String	The network type of the instance. - VPC : a VPC instance. - Classic : a classic-network instance.

5.3 Cloud products that support hybrid access

This topic provides links to the endpoints of the cloud products that support hybrid access, including Object Storage Service (OSS), Table Store, Log Service, Message Queue, and MaxCompute. Specifically, these cloud products can be accessed by classic-network ECS instances and VPC ECS instances simultaneously.

Cloud storage products

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

Application Services

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

Middleware

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

Big data

- MaxCompute: [Obtain endpoints](#).

5.4 Hybrid migration

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

Prerequisites

Before the hybrid migration, make sure that:

- You are aware of the limits of the hybrid migration solution. For more information, see [#unique_15](#).
- You are familiar with VPCs and the related products. VPCs are isolated private networks that allow you to manage your cloud resources by using relevant cloud products.
- You conduct an assessment of network architecture and system dependencies before you create a migration plan.

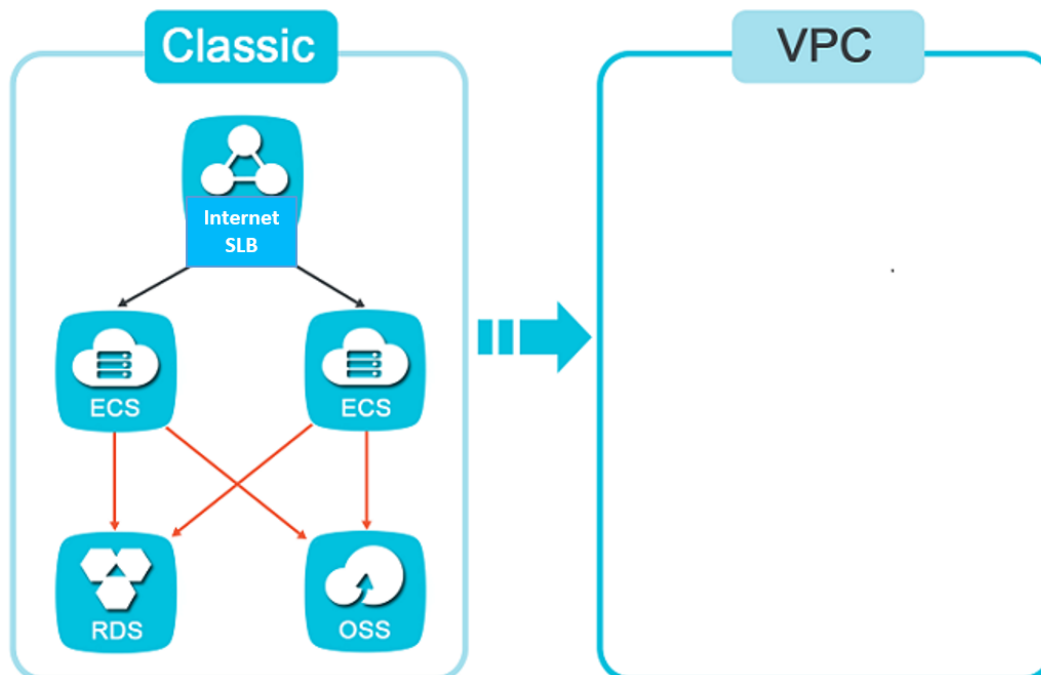
Example systems

The following two systems are used as examples to describe the hybrid migration procedure.

- System 1

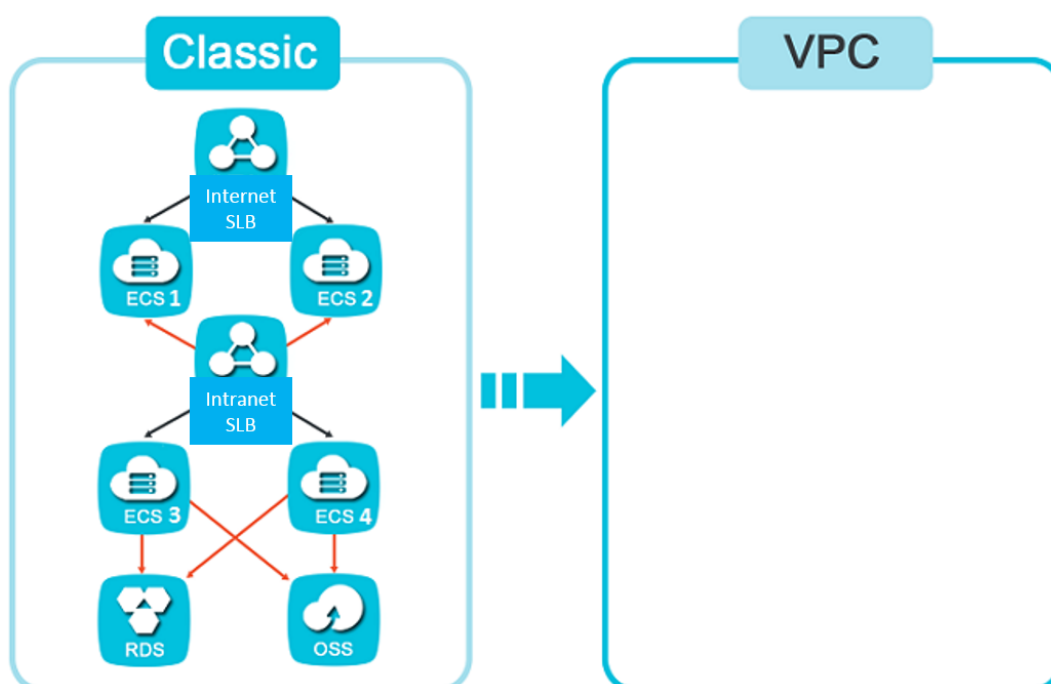
System 1 is a classic network system that consists of SLB, ECS, RDS, and OSS instances. The Internet SLB instance uses two ECS instances as backend servers

. The applications deployed on the two ECS instances need to access the RDS instance and the OSS instance.



• System 2

System 2 is a classic network system that has a more complex architecture than system 1. The Internet SLB instance uses two ECS instances (ECS 1 and ECS 2) as backend servers. Both ECS instances need to access an intranet SLB instance. The intranet SLB instance also uses two ECS instances (ECS 3 and ECS 4) as backend servers. Both ECS instances need to access the RDS instance and the OSS instance.



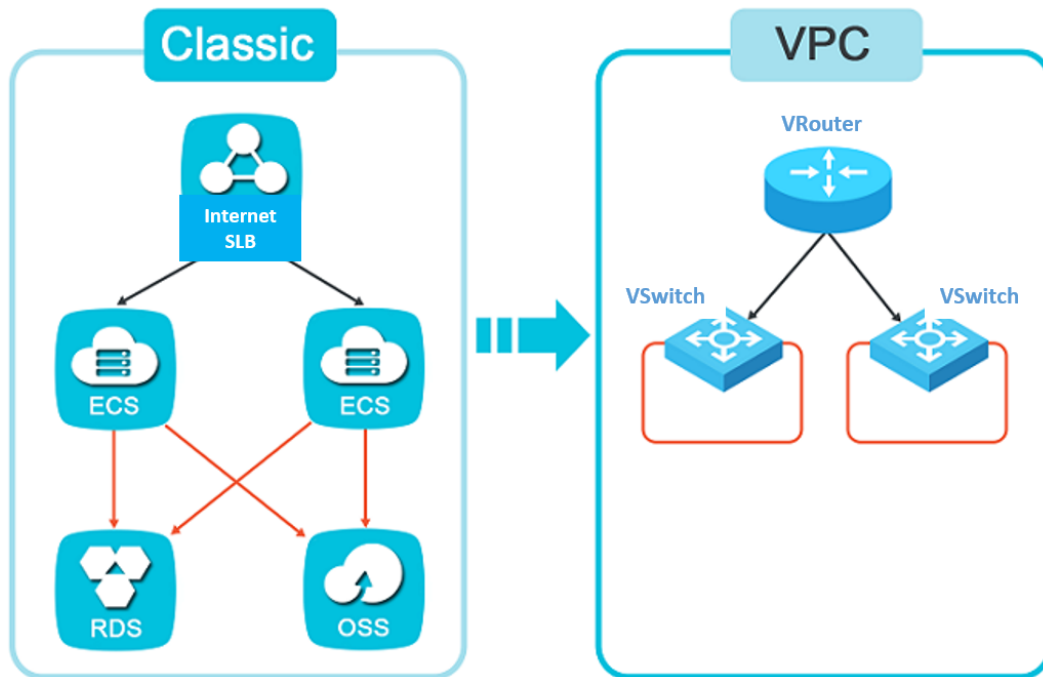
Migrate system 1 to a VPC

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

1. Prepare the network environment.

Create a VPC and a VSwitch to which the system is migrated.

For more information, see [#unique_29](#).



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

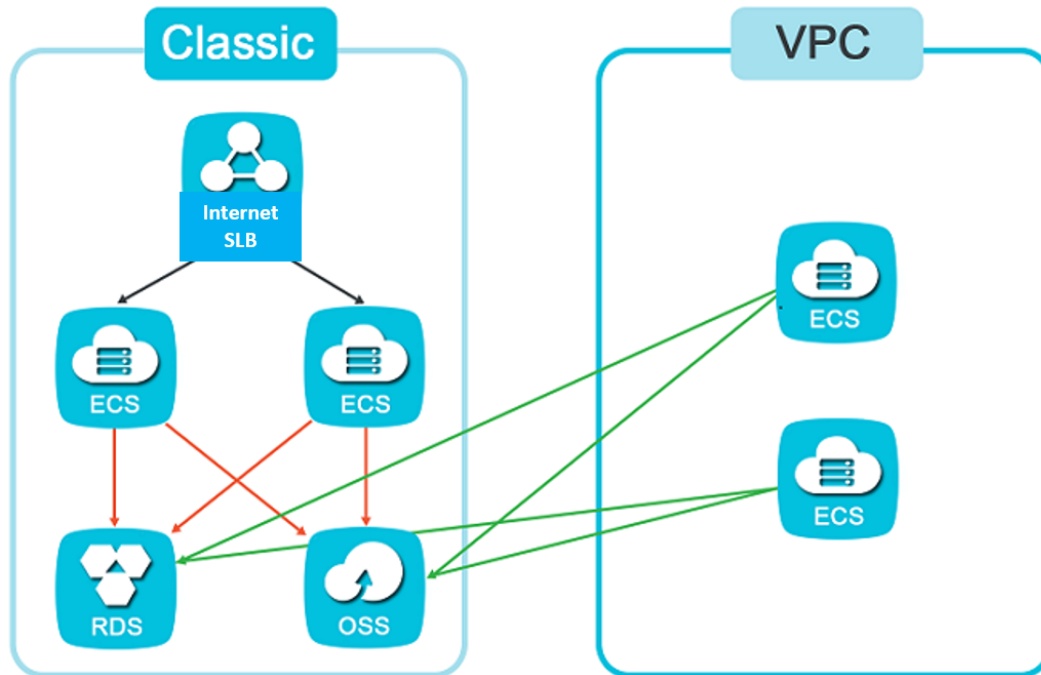
- You can use the console or call the relevant API action to switch the network type of the RDS instance to VPC and reserve its classic network endpoint. For more information, see [#unique_30](#).

After the migration, the classic network endpoint remains unchanged and a new VPC endpoint is added. As a result, the ECS instances in the classic network can still access the database without service disruptions. When the classic network endpoint expires, it is automatically deleted and you cannot access the database through the classic network endpoint.

- The OSS instance provides a classic network endpoint and a VPC endpoint. You do not need to switch its network type. To obtain the VPC endpoint of the OSS instance, see [#unique_31](#).

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

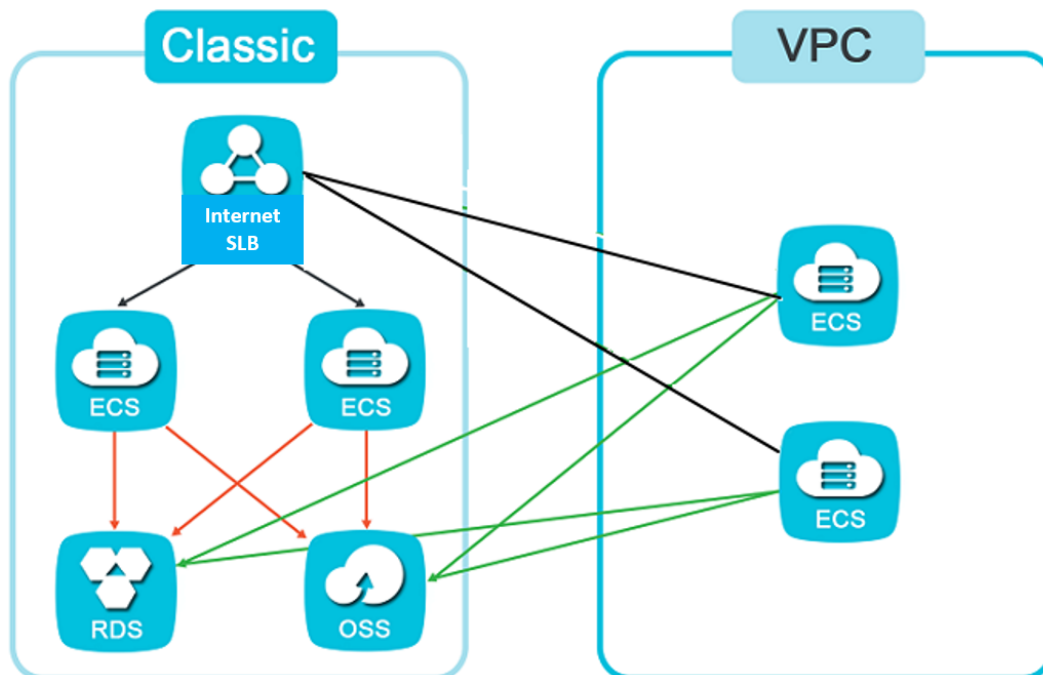
Create two ECS instances in the VPC, deploy applications on the ECS instances, and change the RDS and OSS endpoints to their VPC endpoints. After that, conduct a test to verify that the ECS instances can access the OSS instance and the RDS instance.



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

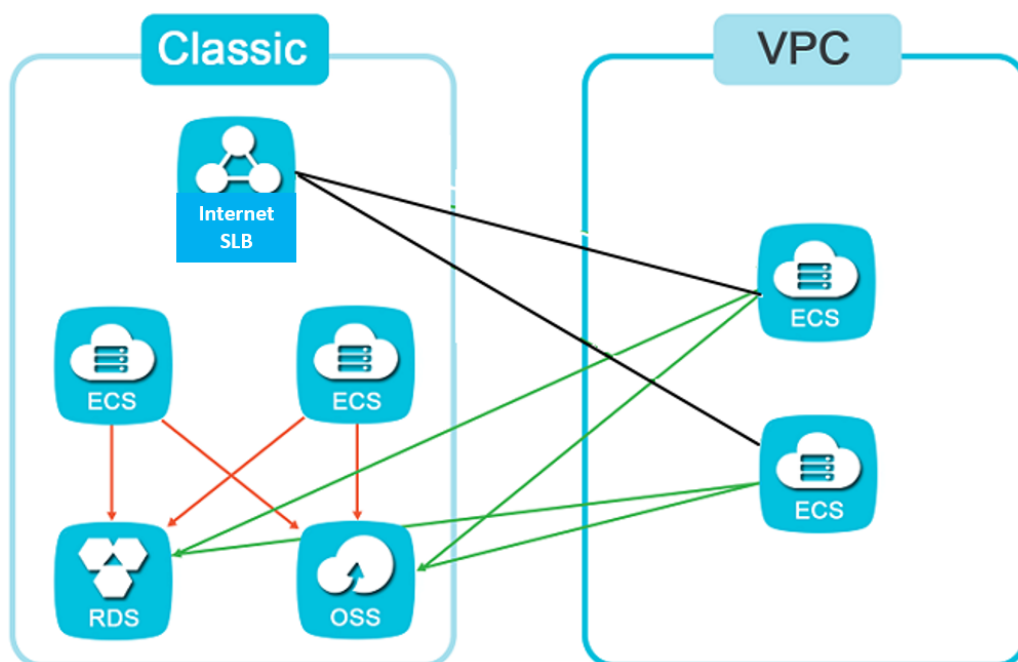
Add the two ECS instances in the VPC to the Internet SLB instance. Check the health status of the ECS instances. We recommend that you set a lower weight for

the ECS instances. This can reduce the impact of unexpected faults on the system. Check the system status, traffic monitoring, and health check logs.



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

Remove the classic-network ECS instances from the Internet SLB instance. We recommend that you set the weight of the classic-network ECS instances to 0 and then remove them when they no longer receive requests.



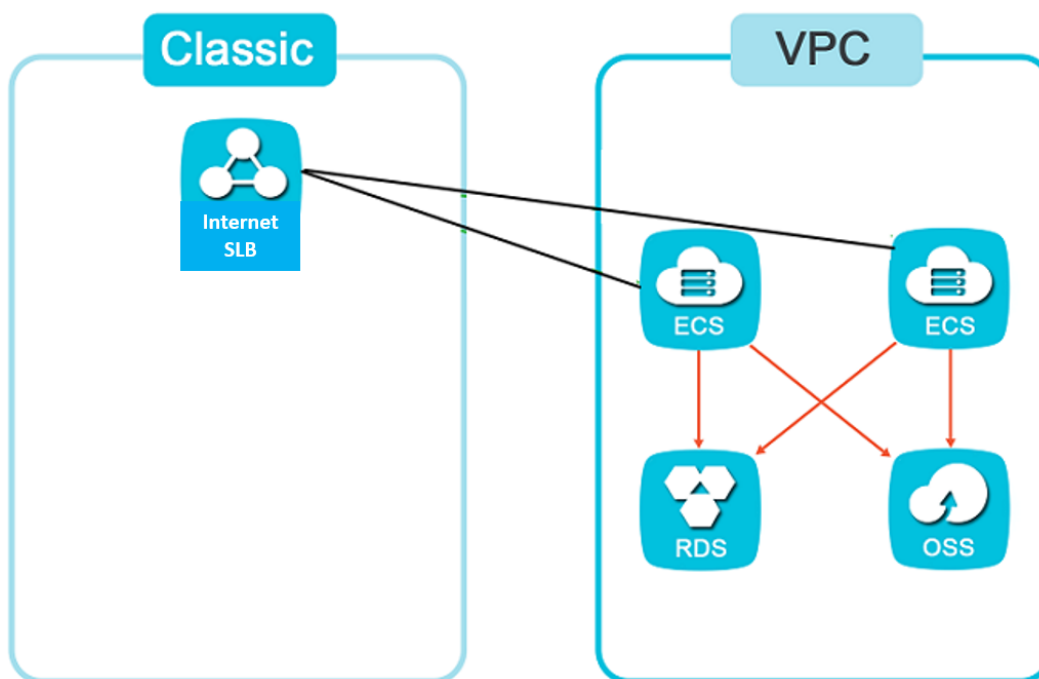
6. Release the classic-network ECS instances.

Release the classic-network ECS instances after the system runs normally for a period of time. You do not need to migrate the Internet SLB instance because VPC ECS instances can be added to it directly.



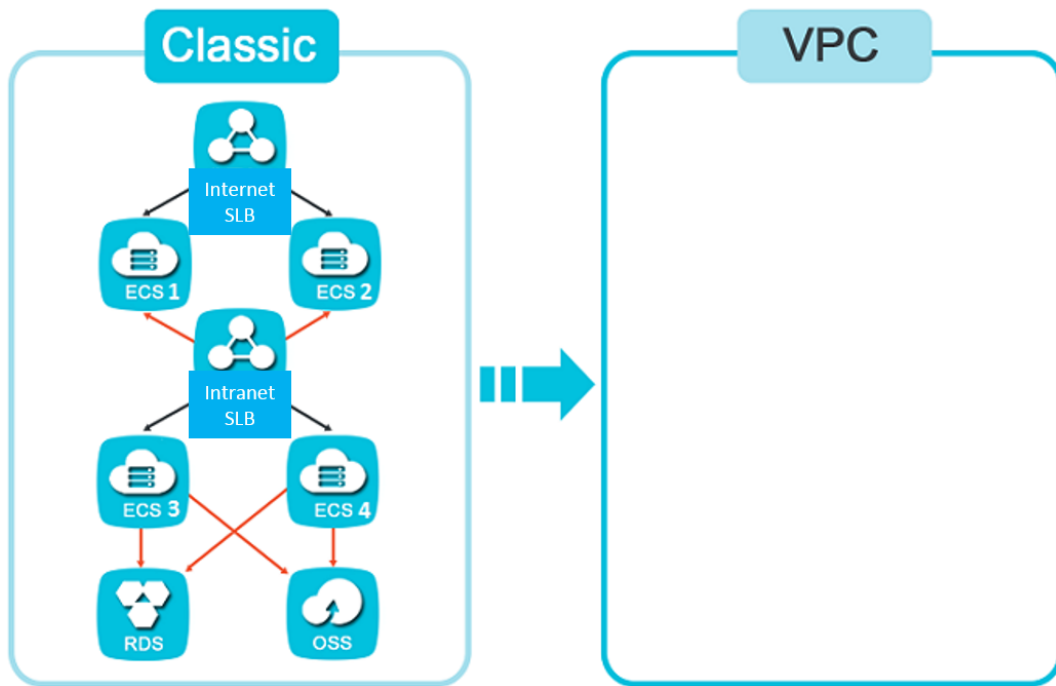
Note:

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



Migrate system 2 to a VPC

When you migrate system 2 to a VPC, the preceding procedure does not apply. If you use the preceding procedure, the ECS instances in the VPC cannot access the ECS instances in the classic network because the SLB instance does not support hybrid access.



To migrate system 2 to a VPC, follow these steps:

1. Create two ECS instances in the VPC to migrate ECS 3 and ECS 4 added to the intranet SLB instance.
2. Configure the two ECS instances, and change the endpoint of the RDS instance and the OSS instance to the endpoint of the VPC endpoint.
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 backend servers.
5. Create two more ECS instances in the VPC to migrate the ECS 1 and ECS 2 added to the Internet SLB instance.
6. Configure the two new ECS instances. Change the classic network endpoint of the intranet SLB instance to the VPC endpoint of this instance.
7. Refer to steps 4 to 6 described in the migration of system 1 to complete the migration of system 2.