Alibaba Cloud
Virtual Private Cloud

VPC network connections

Issue: 20190831

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 `cd / d C :/ windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*

Style	Description	Example
{} or {a|b}	**It indicates that it is a required value, and only one item can be selected.**	`swich` *{stand | slave}*

Contents

1 Network connection overview

This topic describes the network solutions provided by Alibaba Cloud for connecting your VPC to the Internet, other VPCs, and on-premises data centers.

Connect a VPC to the Internet

The following table lists the products and functions that you can use to connect a VPC to the Internet.

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_4.	You can use Data Transfer Plan. After changing a public IP address to an EIP, you can also use Internet Shared Bandwidth.
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.

Product	Function	Benefit
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.

Connect two VPCs

The following table lists the products or functions that you can use to connect a VPC to another VPC.

Product	Function	Benefit
Cloud Enterprise Network (CEN)	By using a CEN, you can connect VPCs in different regions under different accounts to build an interconnected network. For more information, see #unique_7.	· Global access · Low latency and fast speed · Nearest access and shortest path · Link redundancy and disaster recovery · Systematic management

Product	Function	Benefit
VPN Gateway	By using a VPN Gateway, you can create an IPsec-VPN connection to build an encrypted channel between two VPCs. For more information, see #unique_8.	· High security · High availability · Low cost · Easy configuration

Connect a VPC to an on-premises data center

The following table lists the products and functions that you can use to connect a VPC to an on-premises data center.

Product	Function	Benefit
Express Connect	By using Express Connect, you can connect a VPC to an on-premises data center through a physical connection. For more information, see Connect an on-premises data center to a VPC through a physical connection.	· Based on the backbone network, low latency · Secure and reliable physical connection
VPN Gateway	· By using a VPN Gateway, you can create an IPsec-VPN connection between a VPC and an on-premises data center. · You can connect a local client to a VPC by creating an SSL-VPN connection.	· High security · High availability · Low cost · Easy configuration

Product	Function	Benefit
CEN	- Connect to an on-premises data center By using a CEN, you can attach the virtual border router (VBR) associated with an on-premises data center to a CEN instance to build an interconnected network. - Connect multiple VPCs with on-premises data centers By using a CEN, you can attach multiple networks (VPC/VBR) to a CEN instance to build an interconnected network.	- Global access - Low latency and fast speed - Nearest access and shortest path - Link redundancy and disaster recovery - Systematic management
Smart Access Gateway (SAG)	- By using an SAG, you can connect on-premises branches (such as data centers and outlets) to Alibaba Cloud to build a hybrid cloud. - Interconnect on-premises branches.	- SAGs features automated configuration and out-of-the-box experience, and can quickly adapts to network topology changes. - Access is provided from the nearest endpoint over the Internet. Multiple local branches can access Alibaba Cloud by using active and standby SAGs or active and standby links. - Local branches and Alibaba Cloud are connected through an encrypted private network . The transmission over the Internet is also encrypted.

2 Connect a VPC to the Internet

This topic describes the four methods that you can use to connect a VPC to the Internet.

Overview

A VPC is a private network in Alibaba Cloud. By default, the cloud resources in a VPC cannot access the Internet or be accessed by the Internet. However, you can connect a VPC to the Internet by using an ECS public IP address, an Elastic IP (EIP), a NAT Gateway, or the Server Load Balancer (SLB) service.

VPCs provide Internet Shared Bandwidth and Data Transfer Plan to help you save the Internet cost. For more information, see How to save the Internet cost.

ECS public IP address

When you create a VPC ECS instance, you can assign the instance a public IPv4 address that supports access to the Internet or from the Internet.

An ECS IP address cannot be dynamically disassociated from the corresponding VPC ECS instance, but can be converted to an EIP. For more information, see #unique_4.

EIP

An EIP is a type of NAT IP address that is located on the Internet gateway of Alibaba Cloud and is mapped to the associated cloud resource through NAT. After a cloud resource is associated with an EIP, the cloud resource can communicate with the Internet through the EIP.

You can associate an EIP with a VPC ECS instance, Elastic Network Interface (ENI), VPC SLB instance, or NAT Gateway. For more information, see EIP User Guide.

The benefits of EIPs are as follows:

- Individual purchase

  You can purchase an EIP as an individual resource instead of purchasing it together with other computing or storage resources.
- Flexible association

  You can associate an EIP with the target resource or disassociate and release the EIP whenever necessary.

- Changeable network capability

  You can change the bandwidth of an EIP as needed. Bandwidth changes take effect immediately.

NAT Gateway

A NAT Gateway is an enterprise-class VPC Internet gateway that provides NAT proxy services (SNAT and DNAT), forwarding capacity of up to 10 Gbps, and cross-zone disaster recovery.

By using a NAT Gateway, multiple ECS instances in a VPC can access the Internet through a public IP address. For more information, see NAT Gateway User Guide.

The benefits of NAT Gateways are as follows:

- Flexible and easy-to-use

  NAT Gateways provide SNAT and DNAT functions. You can directly configure SNAT and DNAT rules without the need to set up a NAT Gateway.
- High availability

  NAT Gateways are virtual network hardware that is based on the distributed gateway of Alibaba Cloud and is virtualized by the SDN technology. With a forwarding capacity of up to 10 Gbps, NAT Gateways support large-scale Internet applications.
- Pay-AS-You-Go billing

  You can change the specification and the number of NAT Gateways and EIPs at any time to meet your service changes.

SLB service

SLB is a traffic distribution service that distributes traffic to multiple ECS instances to expand service capabilities and improve availability of applications.

The SLB service provides layer 4 and layer 7 server load balancing, which allows access to ECS instances from the Internet. For more information, see Server Load Balancer Overview.

> Note:
> VPC ECS instances cannot access the Internet (SNAT) through SLB.

The benefits of the SLB service are as follows:

- High availability of the SLB system

  Deployed in clusters, SLB can synchronize sessions to protect ECS instances against single points of failure (SPOFs). This improves redundancy and guarantees service stability.

- High availability of a single SLB instance

  SLB has deployed multiple zones in most regions to guarantee disaster recovery across data centers in the same region. When the primary zone is faulty or unavailable, SLB can switch to the secondary zone in about 30 seconds and restore services. After the primary zone is restored, SLB automatically switches back to the primary zone to provide services.

- High availability of multiple SLB instances

  You can deploy SLB instances and backend ECS instances in multiple zones of a region or in multiple regions and schedule access requests by using Alibaba Cloud DNS.

- High availability of backend ECS instances

  SLB determines the service availability of backend ECS instances through health checks. Health checks improve the availability of frontend services and reduce the impact on service availability when backend servers are faulty.

3 Connect two VPCs

This topic describes the methods that you can use to connect two VPCs. You can use a CEN or a VPN Gateway to connect two VPCs.

Cloud Enterprise Network

A Cloud Enterprise Network (CEN) is a solution that helps you establish private channels between VPCs. With automatic route distribution and learning, a CEN can improve network convergence, quality, and security to support mutual access among global resources. For more information, see What is Cloud Enterprise Network?

You can use a CEN to connect two VPCs under the same account or different accounts. The following table describes the scenarios.

Scenario	Method
Connect two VPCs under the same account	Connect two VPCs in the same region under the same account
	Connect two VPCs in different regions under the same account
Connect two VPCs under different accounts	Connect two VPCs in the same region under different accounts
	Connect two VPCs in different regions under different accounts

The benefits of CENs are as follows:

- Global access

  A CEN is an enterprise-class network that can connect Alibaba Cloud resources around the world and the resources that have access to Alibaba Cloud. CENs validate the IP address ranges of the connected networks to ensure that these IP address ranges do not conflict with each other. Moreover, CENs automatically forward and learn multi-node routes through controllers to rapidly converge global routes.
- Low latency and high speed

  CENs provide low-latency and high-speed network transmission. The maximum local access rate can reach the port forwarding rate of the gateway device. In global network communication, the latency of CENs is much shorter than that of the Internet.

- Nearest access and shortest path

  CENs deploy multiple access points and forwarding points in more than 60 regions around the world to support nearest access to Alibaba Cloud.
- Link redundancy and disaster recovery

  CENs features high availability and network redundancy by providing at least four redundant links between any two access points. If a link fails, your services can still operate normally without network jitter or disruptions.
- Systematic management

  CENs have systematic network monitoring capabilities that automatically detect route conflicts caused by system changes and guarantee network stability.

VPN Gateway

A VPN Gateway is an Internet-based networking solution that supports route-based IPsec-VPN connections. You can use IPsec-VPN connections to connect different VPCs securely and reliably. For more information, see #unique_8.

The benefits of VPN Gateways are as follows:

- High security

  The IKE and IPsec protocols are used to encrypt transmission data to guarantee data security.
- High availability

  With hot backup, VPN Gateways automatically switch to the failover mode within seconds to ensure session continuity and service availability.
- Low cost

  The Internet-based encrypted channels established by VPN Gateways are more cost-effective than leased lines.
- Easy configuration

  VPN Gateways are ready for use after being activated. All configurations take effect in real time.

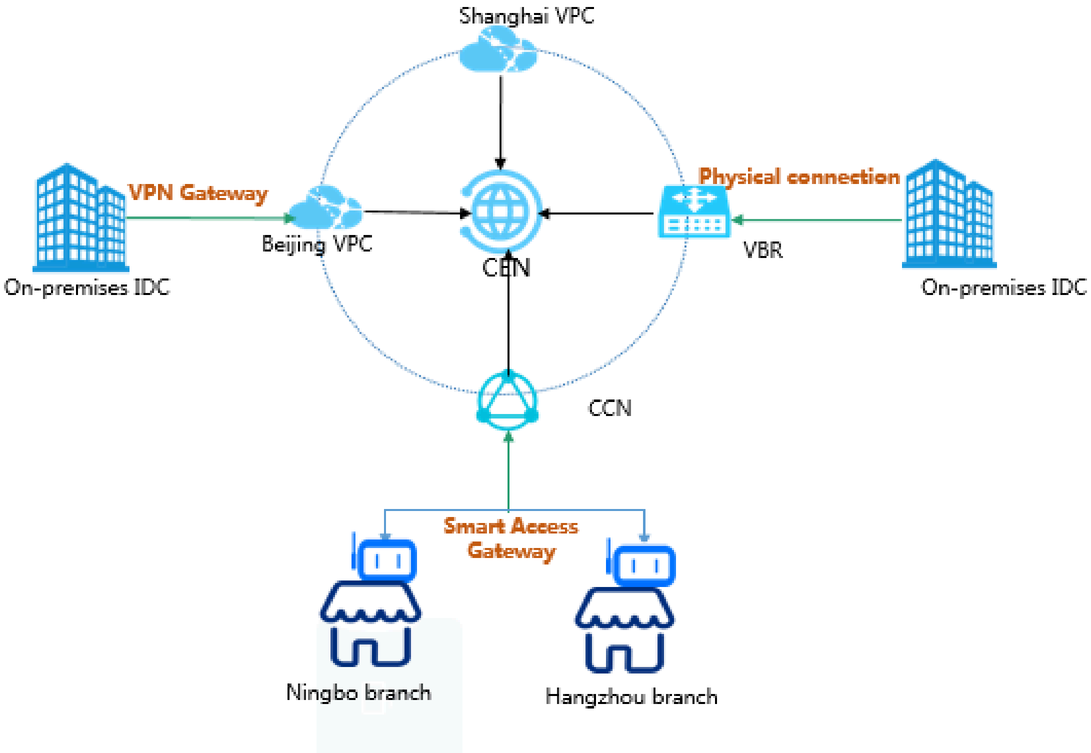
4 Connect a VPC to an on-premises data center

You can connect an on-premises data center to a VPC by using VPN Gateway, a physical connection of Express Connect, or Smart Access Gateway to build a hybrid cloud.

Overview

You can establish intranet communication between a local data center and Alibaba Cloud to build a hybrid cloud. Then you can seamlessly expand your local IT infrastructure to Alibaba Cloud to cope with service fluctuation and improve application stability by right of the mass computing, storage, network, and CDN resources of Alibaba Cloud.

You can use VPN Gateway, a physical connection of Express Connect and Smart Access Gateway to connect a local data center to a VPC. In addition, you can interconnect global networks by using CEN.



Solutions

Solution	Description
VPN Gateway	You can use IPsec-VPN to connect a local data center to a VPC. VPN Gateway contains two different gateway instances which form active/standby hot backup. The traffic is automatically distributed to the standby node when the active node fails. The VPN Gateway is based on Internet communication , so its network latency and availability are decided by the Internet. If you do not have a particularly high demand for network latency, we recommend that you use VPN Gateway. For more information, see #unique_22.
Physical connection	You can use a leased line of your service provider to establish a physical connection between your on-premises IDC and an Alibaba Cloud access point. Physical connection features good network quality and large bandwidth. Therefore, if your priority is good network quality, we recommend that you select physical connection. For more information, see Connect a local data center to a VPC through a physical connection.
Redundant physical connections	You can use redundant physical connections to connect your on-premises data center to a VPC. Redundant physical connections provide high-quality and high-reliability intranet communication between your local data center and Alibaba Cloud. Alibaba Cloud supports up to four physical connections to achieve Equal-CostMultipathRouting (ECMP). For more information, see Create redundant physical connections.

Solution	Description
Smart Access Gateway	Smart Access Gateway (SAG) is an all-in-one solution for connecting local branches of an enterprise to the Alibaba Cloud. With Smart Access Gateway, enterprise s can access Alibaba Cloud through the Internet using a fully encrypted connection, which is more intelligent, more reliable, and more secure. Smart Access Gateway is an easy-to-configure and low -cost service. If you want to connect multiple local branches of an enterprise to the cloud, we recommend that you select Smart Access Gateway. For more information, see Connect local branches to Alibaba Cloud through Smart Access Gateway.
BGP active/standby links	Function by using both a physical connection and CEN, allowing you to connect an on-premises data center to VPCs in different regions through active/standby links. For more information, see Connect a local data center to Alibaba Cloud by using BGP active/standby links.
Physical connection + Smart Access Gateway	A solution using Smart Access Gateway as the backup link of the existing physical connection to build a reliable and high-availability hybrid cloud. For more information, see Tutorial for configuring Smart Access Gateway as the backup of a physical connection.

5 ClassicLink

5.1 ClassicLink overview

VPC provides the ClassicLink function so that ECS instances of the classic network can communicate cloud resources in a VPC network through the intranet.

Background

The basic implementation for the connection of classic networks with VPCs is the same as that of two classic networks. Therefore, when connecting a classic network to a VPC, the intranet latency and bandwidth limits remain unchanged. Moreover, operations, such as downtime migration, hot migration, stopping, starting, restarting, and system disk replacement will not change the link of a previously established ClassicLink.

The classic network and VPC network are two different network planes. ClassicLink establishes a private communication channel between these two network planes through routing. Therefore, to use the ClassicLink function, you must plan IP addresses properly to avoid IP address conflicts.

The IP address range used by classic networks in Alibaba Cloud is 10.0.0.0/8 (excluding 10.111.0.0/16). As long as the IP address range of a VPC does not conflict with 10.0.0.0/8, you can use ClassicLink to establish a private communication. VPC IP address ranges that can communicate with the classic network are 172.16.0.0/12, 10.111.0.0/16 and 192.168.0.0/16.

Limits

Note the following before you use the ClassicLink function:

- Up to 1,000 ECS instances of the classic network can be connected to the same VPC.
- An ECS instance of the classic network can be connected to only one VPC, and the VPC must be under the same account and belong to the same region.

  For cross-account connection such as ones connecting an ECS instance under account A to a VPC under account B, you can transfer the ECS instance from account A to account B.

- To enable the ClassicLink function of a VPC, the following conditions must be met:

VPC CIDR block	Limitations
172.16.0.0/12	There is no custom route entry destined for 10.0.0.0/8 in the VPC.
10.0.0.0/8	- There is no custom route entry destined for 10.0.0.0/8 in the VPC. - Make sure that the CIDR block of the VSwitch to communicate with the ECS instance in the classic network is within 10.111.0.0/16.
192.168.0.0/16	- There is no custom route entry destined for 10.0.0.0/8 in the VPC. - Add a route entry, of which the destination CIDR block is 192.168.0.0/16 and the next hop is the private NIC, to the ECS instance of the classic network. Download the Route script. Note: Before running the script, read the readme file in the script carefully.

Connection scenarios

The following table lists the scenarios of connecting an ECS instance of a classic network to a VPC network.

Network type of the initiator	Region/ account	Network type of the acceptor/intranet communication	
		Classic network	VPC network
Classic network	Same region Same account	Add a same-account authorization rule in the security group.	Build a ClassicLink connection.

	Same region Different accounts	Add a cross-account authorization rule in the security group.	- Solution A: 1. Migrate the ECS instance of the classic network to the VPC network 2. Connect the VPCs - Solution B: 1. Transfer the ECS instance of the classic network to the account of the VPC 2. Build a ClassicLink connection
	Different regions Same account	1. Migrate both ECS instances to the VPC network. 2. Connect the two VPCs.	1. Migrate the initiator ECS instance to the VPC network. 2. Connect the two VPCs.
	Different regions Different accounts		
VPC	Same region Same account	Build a ClassicLink connection	Connect the VPCs

	Same region Different accounts	· Solution A: 1. Migrate the ECS instance of the classic network to the VPC 2. Connect the VPCs · Solution B: 1. Migrate the ECS instance of the classic network to the account of the VPC. 2. Build a ClassicLink connection	
	Different regions Same account	1. Migrate the receiver ECS instance of the classic network to the VPC 2. Connect the VPCs	
	Different regions Different accounts		

Example scenario

After an ECS instance of the classic network is connected to a VPC through ClassicLin k:

- The ECS instance in the classic network can access cloud resources in the VPC.

  After a ClassicLink connection is successfully established, ECS instances in the classic network can access other cloud resources in the connected VPC (such as other ECS, RDS, or SLB instances). An real example may be that an ECS instance in the classic network is connected to a VPC of which the IP address range is 10.0.0 .0/8, and the VPC has a VSwitch of which the IP address range is 10.111.1.0/24. If you have deployed cloud resources (such as ECS and RDS instances) in the VSwitch , then the ECS instance in the classic network can access these resources through ClassicLink.

- After the ClassicLink connection is successfully established, ECS instances in the VPC can only access ECS instances in the classic network connected to the VPC and cannot access ECS instances or any other cloud resources in classic networks that are not connected to the VPC.

5.2 Enable ClassicLink

This topic describes how to enable ClassicLink. After you enable the ClassicLink function, you can connect classic-network ECS instances to the cloud resources (such as ECS instances, RDS instances, and SLB instances) in a VPC through the intranet.

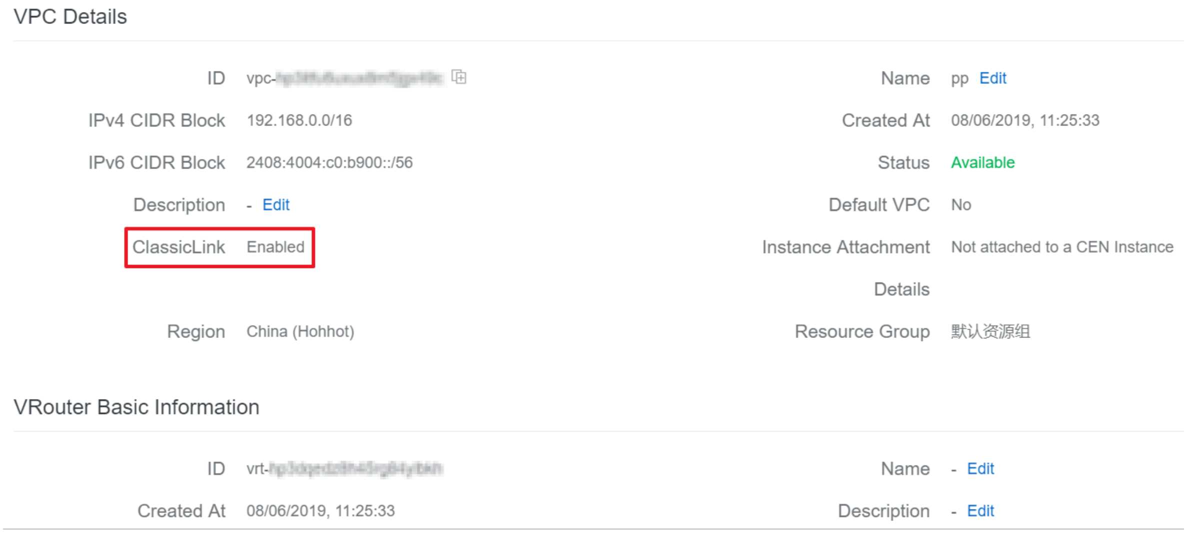
Context

The ECS instance in the VPC can access classic-network ECS instances connected to the VPC, but cannot access those not connected to the VPC or access other resources in the VPC. For more information, see #unique_29.

Procedure

1. Log on to the VPC console.
2. Select the region to which the target VPC belongs.
3. On the VPCs page, find the target VPC, and then click Manage in the Actions column.
4. On the VPC Details page, click Enable ClassicLink.
5. In the Enable ClassicLink dialog box, click OK.

   After ClassicLink is enabled, the status of ClassicLink is changed to Enabled.



VPC Details

ID	vpc-[redacted]	Name	pp Edit
IPv4 CIDR Block	192.168.0.0/16	Created At	08/06/2019, 11:25:33
IPv6 CIDR Block	2408:4004:c0:b900::/56	Status	Available
Description	- Edit	Default VPC	No
ClassicLink	Enabled	Instance Attachment Details	Not attached to a CEN Instance
Region	China (Hohhot)	Resource Group	默认资源组

VRouter Basic Information

ID	vrt-[redacted]	Name	- Edit
Created At	08/06/2019, 11:25:33	Description	- Edit

5.3 Establish a ClassicLink connection

This topic describes how to establish a ClassicLink connection. After you establish a ClassicLink connection, you can connect classic-network ECS instances to the cloud resources deployed in a VPC.

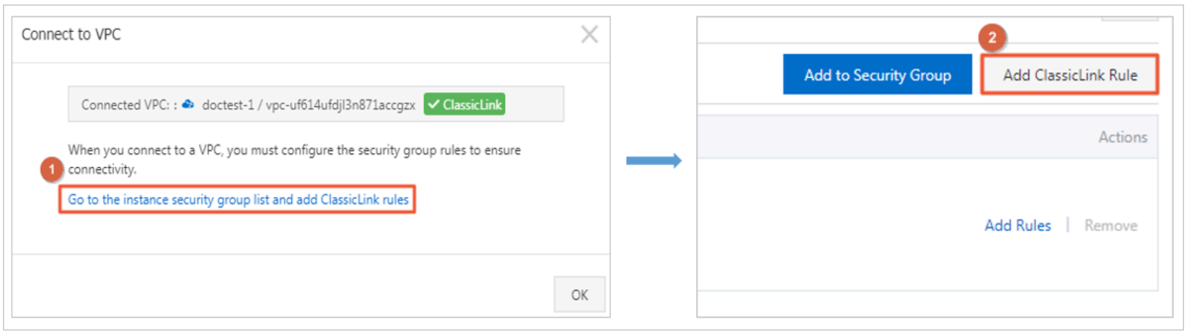
Prerequisites

Before you can establish a ClassicLink connection, the following conditions must be met:

- The limits for establishing ClassicLink connections are known. For more information, see #unique_29.
- The ClassicLink feature in the VPC in which you want to establish a ClassicLink connection is enabled. For more information, see #unique_31.

Procedure

1. Log on to the ECS console.
2. In the left-side navigation pane, choose Instances & Images > Instances.
3. Select the region to which the target ECS instance belongs.
4. On the Instances page, find the target classic-network instance, and then choose More > Network and Security Group > Set classic link in the Actions column.
5. In the Connect to VPC dialog box, select the target VPC, and then click OK.
6. Click Go to the instance security group list and add ClassicLink rules, and then click Add ClassicLink Rule.



Connected VPC: : doctest-1 / vpc-uf614ufdjl3n871accgzx ✓ ClassicLink

When you connect to a VPC, you must configure the security group rules to ensure connectivity.

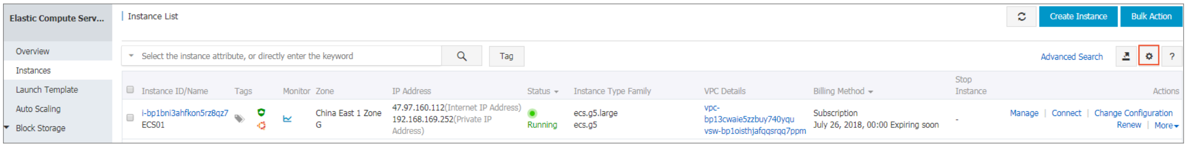
7. In the Add ClassicLink Rule dialog box, set the parameters, and then click OK. The following table describes the parameters.

Configuration	Description
Classic Security Group	The name of the classic network security group.

Configuration	Description
Select VPC Security Group	Select the security group of the VPC.
Mode	Select one of the following modes: · Classic <=> VPC: The connected resources can access each other (recommended). · Classic => VPC: Authorize the classic-network ECS instance to access cloud resources in the VPC. · Classic <= VPC: Authorize the cloud resources in the VPC to access the classic-network ECS instance.
Protocol Type	Select the protocol for communication.
Port range	Select the port for communication. The port must be in the format of xx/xx. For example, if port 80 is used, enter 80/80.
Priority	Set the priority for the security group rule. A smaller value indicates a higher priority.
Description	Enter a description for the security group rule.

8. On the ECS instances page, click the Column Filter icon in the upper-right corner, select Connection Status, and then click OK to view the connection status of the ECS instance.

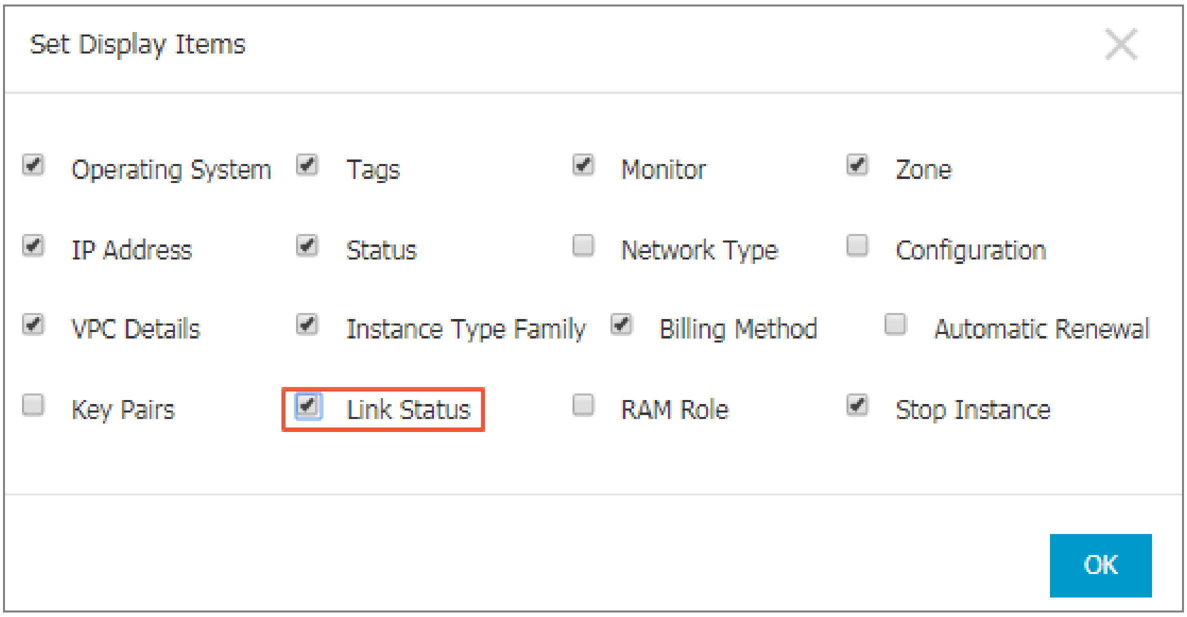
Figure 5-1: Column Filters icon



Instance ID/Name	Tags	Monitor	Zone	IP Address	Status	Instance Type Family	VPC Details	Billing Method	Stop Instance	Actions

i-bp1bni3ahfkon5rz8qz7
ECS01
			China East 1 Zone G	47.97.160.112(Internet IP Address)
				192.168.169.252(Private IP Address)
					Running	ecs.g5.large
						ecs.g5
							vpc-bp13cwaie5zzbuy740yqu
							vsw-bp1oisthjafqqsrqq7ppm
								Subscription
								July 26, 2018, 00:00 Expiring soon
									-	Manage | Connect | Change Configuration
										Renew | More

Figure 5-2: Connection Status


Set Display Items

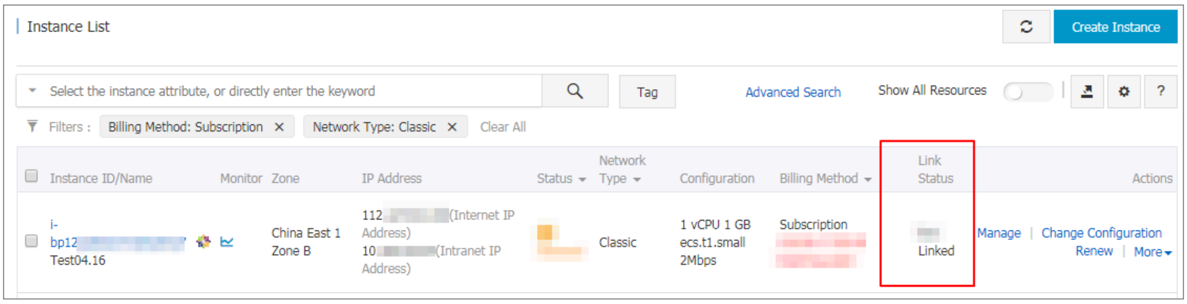
☑ Operating System ☑ Tags ☑ Monitor ☑ Zone

☑ IP Address ☑ Status ☐ Network Type ☐ Configuration

☑ VPC Details ☑ Instance Type Family ☑ Billing Method ☐ Automatic Renewal

☐ Key Pairs ☑ Link Status ☐ RAM Role ☑ Stop Instance

Figure 5-3: Connected to a VPC



Instance ID/Name	Monitor	Zone	IP Address	Status	Network Type	Configuration	Billing Method	Link Status	Actions
i-bp12[redacted] Test04.16		China East 1 Zone B	112[redacted](Internet IP Address) 10[redacted](Intranet IP Address)	[redacted]	Classic	1 vCPU 1 GB ecs.t1.small 2Mbps	Subscription [redacted]	[redacted] Linked	Manage | Change Configuration Renew | More

5.4 Disconnect a ClassicLink connection

This topic describes how to disconnect the ClassicLink connection between a classic-network ECS instance and a VPC. After you disconnect the ClassicLink connection, the classic-network ECS instance and the VPC can no longer communicate with each other.

Procedure

1. Log on to the ECS console.
2. In the left-side navigation pane, choose Instances & Images > Instances.
3. Select the region to which the target classic-network ECS instance belongs.
4. On the Instances page, find the target classic-network ECS instance, and then choose More > Network and Security Group > Set classic link in the Actions column.
5. In the Disconnect from VPC dialog box, click OK.

5.5 Disable ClassicLink

This topic describes how to disable the ClassicLink function of a VPC. After you disable the ClassicLink function of a VPC, classic-network ECS instances cannot establish a ClassicLink connection with the VPC.

Prerequisites

The ClassicLink connection between the classic-network ECS instance and the VPC is disconnected. For more information, see #unique_34.

Procedure

1. Log on to the VPC console.
2. Select the region to which the target VPC belongs.
3. On the VPCs page, find the target VPC, and then click Manage in the Actions column.
4. On the VPC Details page, click Disable ClassicLink.
5. In the Disable ClassicLink dialog box, click OK.