ALIBABA CLOUD

Alibaba Cloud

Virtual Private Cloud

VPC network connections

Document Version: 20200828

Alibaba Cloud

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	Danger: Resetting will result in the loss of user configuration data.
Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	Warning: Restarting will cause business interruption. About 10 minutes are required to restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	Notice: If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.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 public network

The following table lists the products that you can use to connect a VPC to the public network.

Product	Function	Benefits
ECS public IP address	A public IPv4 address that can be automatically assigned upon request when you create an ECS instance in a VPC network. An ECS public IP address enables the ECS instance access to or from the public network. An ECS public IP address cannot be dynamically detached from the corresponding ECS instance in VPC network, but it can be converted to an EIP. For more information, see Convert an automatically assigned public IP address to an EIP for a VPC network-connected ECS instance.	After purchasing a Data Transfer Plan, the traffic generated by an ECS instance is automatically deducted from the Data Transfer Plan. You can add an ECS instance to Internet Shared Bandwidth after converting its public IP address to an EIP.
Elastic public IP address (EIP)	Enables access to or from the public network for the associated ECS instances.	EIPs can be associated to or disassociated from ECS instances. You can purchase Internet Shared Bandwidth and Data Transfer Plan and associate them with EIPs to reduce Internet costs.
NAT Gateway	Allows multiple ECS instances to access the Internet (SNAT) and be accessed from the Internet (DNAT). Note NAT gateways do not support traffic balancing, which is a supported feature of Server Load Balancer (SLB).	A NAT Gateway can be used for multiple ECS instances to access the Internet, while an EIP can be used for only one ECS instance of the VPC network type to access the Internet.

Product	Function	Benefits
Server Load Balancer (SLB)	Provides layer-4 and layer-7 server load balancing, which makes ECS instances accessible from the public network. Note ECS instances of the VPC network type cannot access the public network through SLB (SNAT not supported).	The DNAT function of SLBs allows them to forward an Internet request to multiple ECS instances. SLB expands the external service capabilities by distributing traffic to multiple ECSs, and improves the availability of application systems by eliminating single points of failure. After you associate an EIP with an SLB instance, you can use Internet Shared Bandwidth and Data Transfer Plan to reduce Internet costs.

Connect two VPCs

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

Product	Function	Benefits
Cloud Enterprise Network (CEN)	Allows you to connect VPCs in different regions under different accounts to build an interconnected network. For more information, see Tutorial overview.	• Global access • Low latency and fast speed • Nearest access and shortest path • Link redundancy and disaster recovery • Systematic management
VPN gateway	Allows you to create an IPsec-VPN connection to build an encrypted channel between two VPCs. For more information, see Establish a connection between two VPCs.	• High security • High availability • Low cost • Easy configuration

Connect a VPC to an on-premises data center

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

Product	Function	Benefits
Express Connect	Connects a VPC to an on-premises data center through a physical connection. For more information, see What is physical connection.	• Based on the backbone network, low latency • Secure and reliable physical connection

Product	Function	Benefits
VPN gateway	• Allows you to create an IPsec-VPN connection between a VPC and an on-premises data center. • Allows you to connect a local client to a VPC by creating an SSL-VPN connection.	• High security • High availability • Low cost • Easy configuration
CEN	• Connects VBR to an on-premises data center You can attach the Virtual Border Router (VBR) associated with an on-premises data center to a CEN instance. By doing so, you can build an interconnected network. • Connects multiple VPCs to an on-premises data center 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	• Connects on-premises branches (such as data centers and outlets) to Alibaba Cloud to build a hybrid cloud. • Interconnects on-premises branches.	• SAGs feature automated configuration, out-of-the-box experience, and quick adaptation 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 Convert an automatically assigned public IP address to an EIP for a VPC network-connected ECS instance.

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 VPC networks

This topic describes how to connect Virtual Network Cloud (VPC) networks by using Cloud Enterprise Network (CEN) or VPN Gateway.

Cloud Enterprise Network

You can use CEN to establish private network connections between VPC networks. CEN uses automatic route distribution and learning to speed up network convergence and improves the quality and security of cross-network communication. For more information, see Cloud Enterprise Network.

You can use CEN to connect VPC networks created under the same account or different accounts. The following table describes the scenarios.

Scenario	Method
Connect VPC networks under the same account	Connect VPC networks in a region
	Connect VPC networks across regions
Connect VPC networks under different accounts	Connect VPC networks in a region
	Connect VPC networks across regions

The benefits of CEN are as follows:

- Global interconnection

  A CEN is an enterprise-class network that allows you to interconnect Alibaba Cloud resources on a global scale, and also interconnect your network resources on Alibaba Cloud. Networks connected to a CEN are managed based on IP addresses to avoid IP address conflicts. A CEN uses controllers to automatically learn and distribute routes among multiple nodes to achieve fast route convergence on a global scale.

- Low latency and high speed

  CENs provide low-latency and high-speed network transmission. The maximum transmission rate between two local sites can match the port rate of the gateway devices deployed near the local sites. The network latency of global communication through CEN is much lower than network communication over the Internet.

- Nearest access and shortest path transmission

  CEN deploys access points and nodes in more than 60 regions in the world to support nearest access to Alibaba Cloud. This reduces the response latency and packet loss caused by data transmission over the Internet.

- Connection resilience and disaster recovery

  CEN implements high availability and network redundancy by providing at least four redundant connections between any two access points. If a connection fails, your workloads can still function without network jitters or disruptions.

- Systematic management

  CEN provides capabilities for systematic network monitoring. It can automatically detect route conflicts caused by system changes and guarantee network stability.

VPN Gateway

VPN Gateway is an Internet-based connection service. It supports route-based IPsec-VPN connections. You can use IPsec-VPN connections to connect Virtual Private Cloud (VPC) networks for secure and reliable communication. For more information, see Establish a connection between two VPCs.

The benefits of VPN Gateway are as follows:

- High security

  Uses the IKE and IPsec protocols in data transmission to guarantee data security.

- High availability

  Uses a hot-standby architecture to support failovers within only a few seconds. This guarantees the continuity of your business.

- Cost-efficiency

  Establishes encrypted Internet connections, which are more cost-efficient than leased lines.

- Easy to use

  VPN Gateway instances are ready for use after they are activated. Configurations take effect immediately.

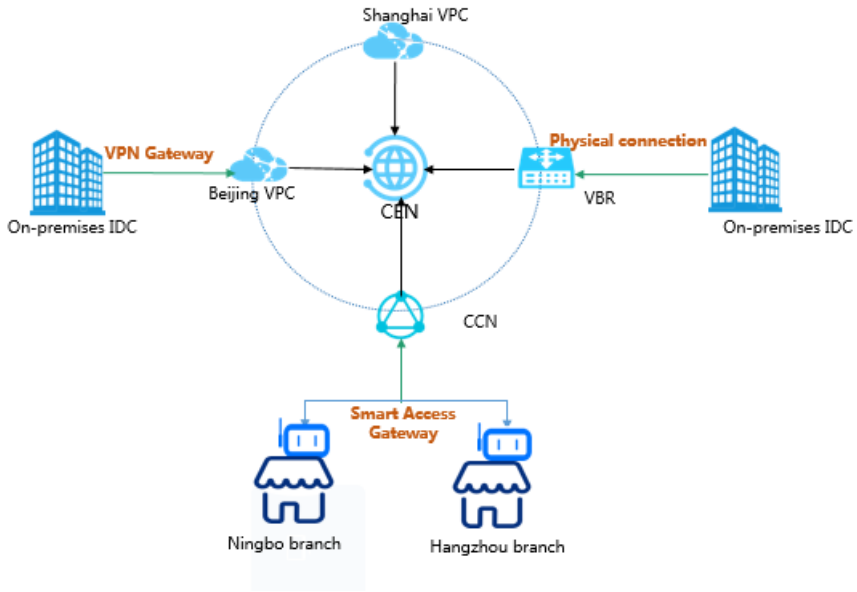
4.Connect an on-premises data center to a VPC network

This topic describes how to connect an on-premises data center to a Virtual Private Cloud (VPC) network to build a hybrid cloud. You can connect an on-premises data center to a VPC network through VPN Gateway, leased lines of Express Connect, or Smart Access Gateway (SAG).

Overview

You can establish private connections between an on-premises data center and an Alibaba Cloud VPC network to build a hybrid cloud. Then, you can connect your on-premises IT infrastructure to Alibaba Cloud. In this way, you can manage workload spikes and improve application stability by using resources of Alibaba Cloud, such as computing, storage, network, and Content Delivery Network (CDN) resources.

You can connect an on-premises data center to a VPC network through VPN Gateway, leased lines of Express Connect, or SAG. You can also use Cloud Enterprise Network (CEN) to connect to your global network resources.



Solutions

Solution	Description

Solution	Description
VPN Gateway	You can use VPN Gateway to establish IPsec VPN connections between your on-premises data centers and VPC networks. The hot-standby architecture of VPN Gateway ensures automatic failovers within a few seconds. VPN connections are established over the Internet. The latency and availability of your VPN connections depend on the quality of the Internet. If you do not require low network latency, we recommend that you use VPN Gateway. For more information, see Establish a connection between a VPC and an on-premises data center.
Leased lines	You can use a leased line provided by an Internet Service Provider (ISP) to establish a physical connection between your on-premises data center and an Alibaba Cloud access point. Express Connect allows you to connect to Alibaba Cloud by applying for an exclusive physical connection in the Express Connect console. Physical connections offer high network quality and large bandwidth. We recommend that you choose physical connections if your priority is high network quality. For more information, see Create a dedicated physical connection.
Redundant physical connections	You can use redundant physical connections to connect your on-premises data center to a VPC network. Redundant physical connections provide high-quality and high-reliability internal communication between on-premises data centers and Alibaba Cloud VPC networks. You can use up to four physical connections to achieve equal-cost multi-path routing (ECMP). For more information, see Create active/standby physical connections.
Smart Access Gateway	Smart Access Gateway is an all-in-one solution for connecting your workloads to Alibaba Cloud. Smart Access Gateway allows enterprises to connect to the nearest access points of VPC networks through encrypted connections over the Internet. It provides more intelligent, reliable, and secure connections to the cloud. SAG is easy to use and cost-effective. We recommend that you use Smart Access Gateway if you need to connect multiple local branch sites to Alibaba Cloud. For more information, see Deploy an SAG device in inline mode.

Solution	Description
Active/standby connections over Border Gateway Protocol (BGP)	You can use a leased line and a Cloud Enterprise Network (CEN) instance to connect an on-premises data center to VPC networks in different regions. For more information, see Connect an on-premises data center to Alibaba Cloud by using BGP active/standby links.
Leased line + Smart Access Gateway	After you connect your on-premises data center to Alibaba Cloud, you can use Smart Access Gateway to establish a standby connection. This ensures the high availability of your hybrid cloud. For more information, see Use SAG to set up standby network connections (leased line connected to a local Internet-facing device).

5.ClassicLink

5.1. Overview

Virtual Private Cloud (VPC) supports the ClassicLink feature, which allows classic network-connected Elastic Compute Service (ECS) instances to communicate with cloud resources in VPC networks.

> **Note** The ClassicLink feature is supported only in regions that support classic networks. For more information, see View privileges and quotas by resource type.

Limits

Before you use the ClassicLink feature, note the following limits:

- You can connect up to 1,000 classic network-connected ECS instances to a VPC network.
- A classic network-connected ECS instance can be connected to only one VPC network created under the same account in the same region.

  If you want to connect an ECS instance of Account A to a VPC network that is under Account B, you must first transfer the ECS instance from Account A to Account B.
- Classic network-connected ECS instances can communicate only with ECS instances in the primary CIDR block of a VPC network. Classic network-connected ECS instances cannot communicate with ECS instances in the secondary CIDR block of the VPC network.
- To enable the ClassicLink feature for a VPC network, the following conditions must be met.

CIDR block of the VPC network	Limit
172.16.0.0/12	The VPC network does not contain a custom route entry with the following destination CIDR block: 10.0.0.0/8.
10.0.0.0/8	○ The VPC network does not contain a custom route entry with the following destination CIDR block: 10.0.0.0/8. ○ Make sure that the CIDR block of the VSwitch that is used to communicate with the classic network-connected ECS instances falls within 10.111.0.0/16.
192.168.0.0/16	○ The VPC network does not contain a custom route entry with the following destination CIDR block: 10.0.0.0/8. ○ Add a route to each classic network-connected ECS instance. This route points 192.168.0.0/16 to the Elastic Network Interface (ENI) of the ECS instance where the route is added. You can add the route by using the provided script. Download script. **Note** Before you run the script, read the readme file in the downloaded package.

Scenarios

The following table describes how ECS instances in a classic network are connected to a VPC network.

<table>
<tr><th rowspan="2">Source network type</th><th rowspan="2">Region/Account</th><th colspan="2">Destination network/Internal communication</th></tr>
<tr><th>Classic network</th><th>VPC network</th></tr>
<tr><td rowspan="5">Classic network</td><td>In the same region
Under the same account</td><td>Modify the security groups of the ECS instances to allow intercommunication under the same account.</td><td>Establish a ClassicLink connection.</td></tr>
<tr><td>In the same region
Cross accounts</td><td>Modify the security groups of the ECS instances to allow intercommunication across accounts.</td><td>• Plan A:
i. Migrate the classic network-connected ECS instances to a VPC network.
ii. Connect the VPC network to the destination VPC network.
• Plan B:
i. Transfer the classic network-connected ECS instances to the account to which the source VPC network belongs.
ii. Establish a ClassicLink connection.</td></tr>
<tr><td>Cross regions
Under the same account</td><td rowspan="3">1. Migrate the ECS instances in the source and destination networks to two VPC networks, respectively.
2. Connect the two VPC networks.</td><td rowspan="3">1. Migrate the ECS instances from the source network to a VPC network.
2. Connect the VPC network to the destination VPC network.</td></tr>
<tr><td>Cross regions
Cross accounts</td></tr>
<tr><td></td></tr>
</table>

<table>
<tr><th rowspan="2">Source network type</th><th rowspan="2">Region/Account</th><th colspan="2">Destination network/Internal communication</th></tr>
<tr><th>Classic network</th><th>VPC network</th></tr>
<tr><td rowspan="4">VPC network</td><td>In the same region
Under the same account</td><td>Establish a ClassicLink connection.</td><td rowspan="4">Connect the two VPC networks.</td></tr>
<tr><td>In the same region
Cross accounts</td><td>• Plan A:
i. Migrate the classic network-connected ECS instances to a VPC network.
ii. Connect the VPC network to the destination VPC network.
• Plan B:
i. Transfer the classic network-connected ECS instances to the account to which the destination VPC network belongs.
ii. Establish a ClassicLink connection.</td></tr>
<tr><td>Cross regions
Under the same account</td><td rowspan="2">1. Migrate the ECS instances from the destination classic network to a VPC network.
2. Connect the VPC network to the destination VPC network.</td></tr>
<tr><td>Cross regions
Cross accounts</td></tr>
</table>

How ClassicLink works

Connections between classic network-connected ECS instances and a VPC network can be established in the same way as those between two classic networks. Therefore, both the latency and the bandwidth limit of internal network connections remain unchanged. An established ClassicLink connection remains unchanged after you migrate, start, stop, or restart the instance, replace the system disk, or perform other operations on the instance.

Classic network and VPC network are two different network planes. A ClassicLink connection connects the two network planes and enables them to communicate with each other through routes. To use ClassicLink, you must plan network addresses properly to avoid overlapped CIDR blocks.

The CIDR block used in classic networks of Alibaba Cloud is 10.0.0.0/8 (excluding 10.111.0.0/16). To use ClassicLink to establish connections, make sure that the CIDR block of the VPC network does not overlap with that of the classic network. The CIDR blocks of VPC networks that can be connected to classic networks are 172.16.0.0/12, 10.111.0.0/16, and 192.168.0.0/16.

Usage notes

After you use ClassicLink to connect ECS instances in a classic network to a VPC network:

- The ECS instances in the classic network can communicate with all cloud resources in the VPC network.

  The ECS instances in the classic network can access cloud resources in the VPC network, such as ECS instances, ApsaraDB for RDS (RDS) instances, and Server Load Balancer (SLB) instances. For example, ECS instances in the classic network are connected to a VPC network whose CIDR block is 10.0.0.0/8, and the VSwitch of the VPC network is assigned the CIDR block 10.111.1.0/24. If you have deployed cloud resources such as ECS instances and RDS instances in the VSwitch, the ECS instances in the classic network can access these resources through ClassicLink connections.
- ECS instances in the VPC network can access only ECS instances in the classic network. ECS instances in the VPC network cannot access other cloud resources in the classic network or ECS instances deployed outside the classic network.

5.2. Enable ClassicLink

Virtual Private Cloud (VPC) networks support the ClassicLink feature. This feature allows classic network-connected Elastic Compute Service (ECS) instances to communicate with cloud resources deployed in VPC networks. Before you establish a ClassicLink connection, make sure that the ClassicLink feature is enabled.

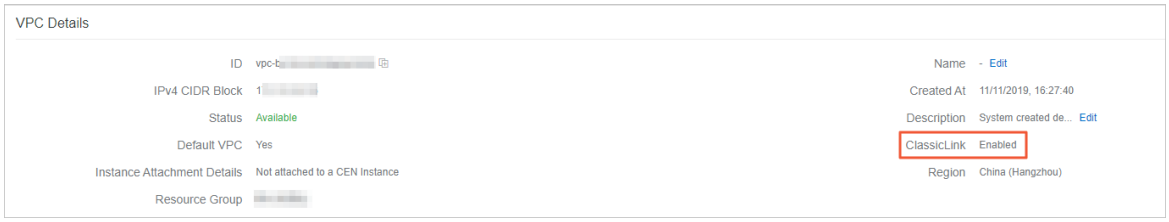
Context

The ClassicLink feature allows classic network-connected ECS instances to communicate with cloud resources such as ECS instances, ApsaraDB for RDS (RDS) instances, and Server Load Balancer (SLB) instances that are deployed in VPC networks. ECS instances in a VPC network can access only ECS instances in a classic network that is already connected to the VPC network. ECS instances in the VPC network cannot access other cloud resources in the classic network or ECS instances deployed outside the classic network. For more information, see Overview.

> **Note** The ClassicLink feature is supported only in regions that support classic networks. For more information, see View privileges and quotas by resource type.

Procedure

1. Log on to the VPC console.
2. On the top navigation bar, select the region where the VPC network is deployed.
3. On the **VPCs** page, find the target VPC network and click **Manage** in the **Actions** column.
4. In the upper-right corner of the VPC Details page, click **Enable ClassicLink**.
5. In the **Enable ClassicLink** message, click **OK**.After ClassicLink is enabled, the status of ClassicLink in the VPC Details section changes to **Enabled**.



5.3. Establish a ClassicLink connection

After you establish a ClassicLink connection, you can connect an Elastic Compute Service (ECS) instance in a classic network to the cloud resources deployed in a Virtual Private Cloud (VPC) network.

Prerequisites

Before you can establish a ClassicLink connection, make sure that the following conditions are met:

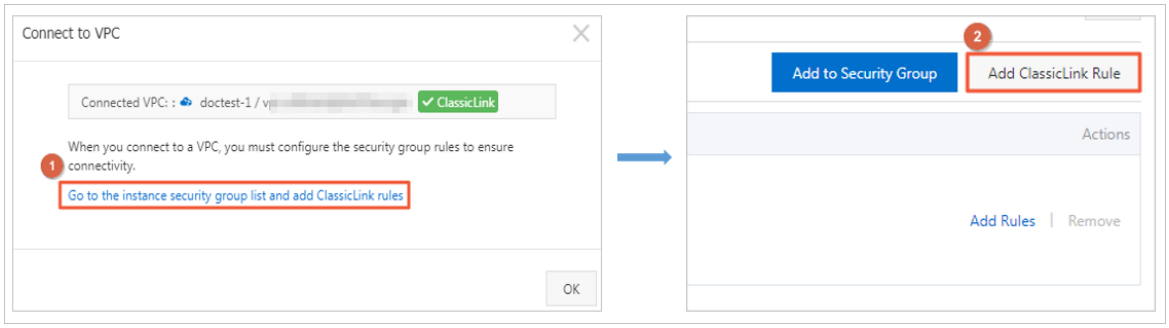
- You have read and understand the limits for establishing a ClassicLink connection. For more information, see Overview.
- The ClassicLink feature is enabled for the VPC network to which the ClassicLink connection is established. For more information, see Enable ClassicLink.

Procedure

1. Log on to the ECS console.
2. In the left-side navigation pane, choose **Instances & Images > Instances**.
3. Select the region where your ECS instance is deployed.
4. On the **Instances** page, find the classic network-connected ECS instance, choose **More >**

Network and Security Group > **Set classic link** in the **Actions** column.

5. In the **Connect to VPC** dialog box, select the VPC network to be connected, and click **OK**.
6. Click **Go to the instance security group list and add ClassicLink rules**, and click **Add ClassicLink Rule**.

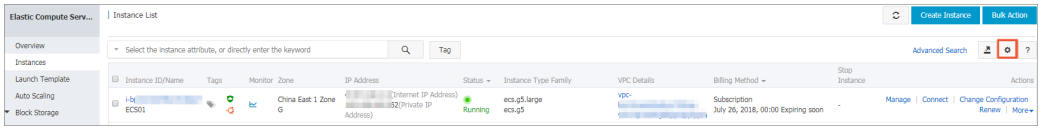


7. In the **Add ClassicLink Rule** dialog box, set the required parameters, and click **OK**. The following table describes the parameters.

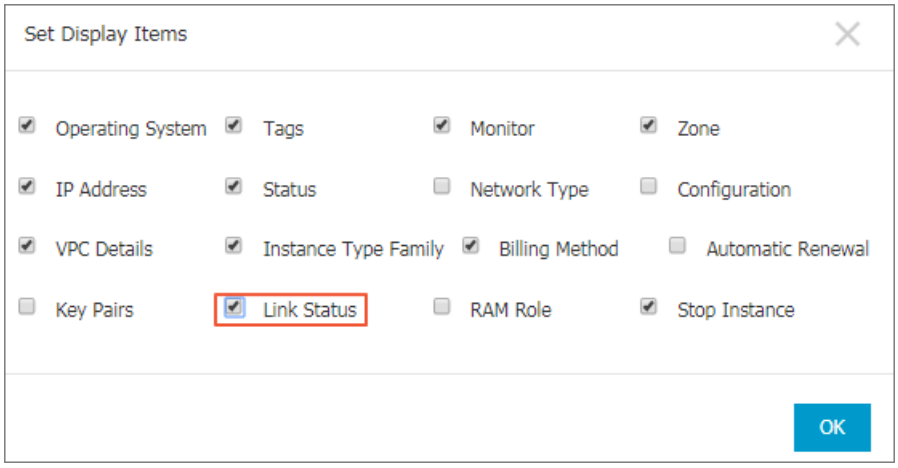
Parameter	Description
Classic Security Group	The name of the classic security group.
Select VPC Security Group	Select the security group of the VPC network.
Mode	Select one of the following authorization modes: ○ Classic <=> VPC: allows the ECS instance in the classic network and cloud resources in the VPC network to access each other (recommended). ○ Classic => VPC: allows the ECS instance in the classic network to access cloud resources in the VPC network. ○ VPC => Classic: allows the cloud resources in the VPC network to access the ECS instance in the classic network.
Protocol Type	Select the protocol for communication.
Port Range	Specify the ports for communication. Ports must be specified in the format of xx/xx. For example, if port 80 is used, enter 80/80.
Priority	Specify the priority of the security group rule. A smaller value indicates a higher priority.
Description	Enter a description for the security group.

8. Go back to the Instances page, click the Column Filters icon in the upper-right corner. In the dialog box that appears, select **Connection Status**, and click **OK** to check the connection status of the ECS instance.

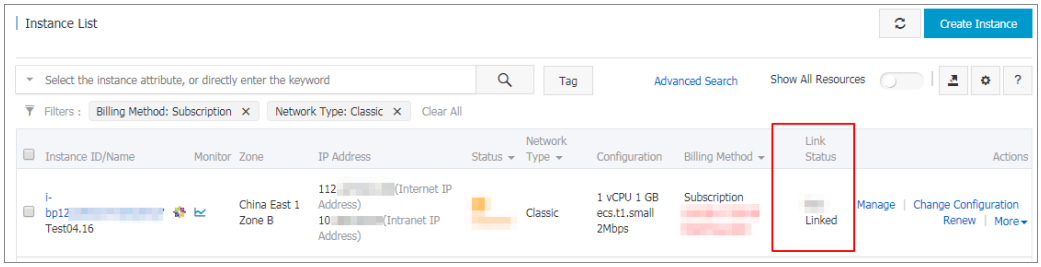
Column Filters



Connection Status



Connected



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 Disconnect a ClassicLink connection.

Procedure

1.
2.
3. In the top navigation bar, select the region where your VPC is deployed.
4. On the **VPCs** page, find the target VPC network and click **Manage** in the **Actions** column.
5. On the **VPC Details** page, click **Disable ClassicLink**.
6. In the **Disable ClassicLink** dialog box, click **OK**.