ALIBABA CLOUD

Alibaba Cloud

Virtual Private Cloud

VPC network connections

Document Version: 20220318

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 05

2.Connect Virtual Private Cloud to the Internet 08

3.Connect VPCs 11

4.Connect a data center to a VPC 13

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.

Enable Internet access

The following table describes the services that you can use to enable Internet access for VPCs.

Service	Description	Benefit
Static public IP address	When you create an ECS instance in a VPC, you can specify whether you want the system to assign a public IPv4 address to the ECS instance. The ECS instance can use the public IP address to communicate with the Internet. You cannot disassociate the public IP address from the ECS instance. However, you can convert the public IP address to an EIP. For more information, see Convert the static public IP address of an ECS instance in a VPC to an EIP.	You can purchase data transfer plans for an ECS instance that is assigned a public IP address. You can also purchase EIP bandwidth plans for an ECS instance after you convert the public IP address of the ECS instance to an EIP. For more information, see What is an EIP bandwidth plan? and What is a 共享流量包data transfer plan?.
EIP	You can associate EIPs with or disassociate EIPs from ECS instances anytime. ECS instances in a VPC can use EIPs in SNAT entries to access the Internet and use EIPs in DNAT entries to provide Internet-facing services.	You can associate EIPs with or disassociate EIPs from ECS instances anytime. You can use EIP bandwidth plans and data transfer plans to reduce the cost of data transfer over the Internet.
Internet NAT Gateway	ECS instances in a VPC can use SNAT entries to access the Internet and use DNAT entries to provide Internet-facing services. **Note** Internet NAT gateways do not provide load balancing services. To balance the loads of ECS instances, use SLB.	An Internet NAT gateway allows multiple ECS instances in a VPC to communicate with the Internet. However, each EIP can be used by only one ECS instance.

Service	Description	Benefit
SLB	SLB provides load balancing services at Layer 4 and Layer 7. You can specify the ports on which SLB listens to distribute requests from the Internet to ECS instances. Alibaba Cloud provides two types of SLB instances: CLB and ALB. **Note** SLB does not support SNAT. ECS instances deployed in a VPC cannot access the Internet through SLB.	SLB supports DNAT. Each port on an SLB instance can be mapped to one or more ECS instances. SLB distributes network traffic across multiple ECS instances to prevent single points of failure. This improves the availability of application systems. After you associate an EIP with an SLB instance, you can purchase EIP bandwidth plans and data transfer plans to reduce costs.

Connect VPCs

The following table describes the services that you can use to connect two VPCs.

Service	Description	Benefit
CEN	Establishes connections among VPCs in different regions or within different accounts. For more information, see Use CEN to enable intra-region network communication.	• Connects networks in different regions. • Low network latency and high speed. • Connects networks through nearby access points. • Connection redundancy and disaster recovery. • Systematic management.
VPN Gateway	Establishes an IPsec-VPN connection between two VPCs for encrypted data transmission. For more information, see Establish IPsec-VPN connections between two VPCs.	• Security. • High availability. • Cost-effectiveness. • Ease of use.

Connect a data center to a VPC

The following table describes the services that you can use to connect a data center and a VPC.

Service	Description	Benefit

Service	Description	Benefit
Express Connect	You can use an Express Connect circuit to connect a data center and a VPC. For more information, see What is a connection over an Express Connect circuit?.	• Network traffic is distributed across the backbone networks of connectivity providers to minimize network latency. • Express Connect circuits ensure the security and reliability of data transfer.
VPN Gateway	• Establishes an IPsec-VPN connection between a data center and a VPC for encrypted data transmission. • Establishes an SSL-VPN connection between a client and a VPC.	• Security. • High availability. • Cost-effectiveness. • Ease of use.
CEN	• Connects to a data center. Connects to data center by attaching the VBR that is associated with the data center to the CEN instance. • Connects multiple VPCs and a data center. You can build an interconnected network by attaching multiple network instances such as VPCs and VBRs to a CEN instance.	• Connects networks in different regions. • Low network latency and high speed. • Connects networks through nearby access points. • Connection redundancy and disaster recovery. • Systematic management.
SAG	• Connects on-premises networks, such as data centers and branches, to Alibaba Cloud to build a hybrid cloud. • Connects on-premises networks.	• Supports automatic configurations and zero touch provisioning (ZTP), and automatically adapts to network topology changes. • Connects to nearby access points in a metropolitan area network. Branch offices can be connected to Alibaba Cloud through active and standby access devices or connections. • Data transmitted over the Internet between the data center and the VPC is encrypted.

2.Connect Virtual Private Cloud to the Internet

You can deploy cloud resources on Elastic Compute Service (ECS) instances that run in a virtual private cloud (VPC). This allows the cloud resources to access the Internet through the public IP addresses, elastic IP addresses (EIPs), NAT gateways, or Server Load Balancer (SLB) instances that are associated with the ECS instances.

Overview

A VPC is a private network dedicated for your use. By default, cloud resources in a VPC cannot access the Internet or be accessed over the Internet. You can connect to the Internet by configuring the public IP addresses, EIPs, NAT gateways, SLB instances that are associated with ECS instances.

VPCs are provided with EIP bandwidth plans and data transfer plans to help you reduce cost of data transfer over the Internet. For more information, see How can I minimize the cost of data transfer over the Internet?.

Public IP address of an ECS instance

When you create an ECS instance in a VPC network, you can allow the system to automatically assign a public IP address to the ECS instance. Then, the ECS instance can use the public IP address to access the Internet.

You cannot disassociate a public IP address from an ECS instance if the ECS instance runs in a VPC network. However, you can convert the public IP address to an EIP. For more information, see Convert the static public IP address of an ECS instance in a VPC to an EIP.

EIPs

An EIP is a public IP address resource that you can purchase and hold independently. EIPs are based on NAT service. They are allocated to the Internet gateways of Alibaba Cloud and are mapped to the associated cloud resource through NAT. After an EIP is associated with a cloud resource, this cloud resource can access the Internet by using this EIP.

You can associate an EIP with an ECS instance in a VPC network, an Elastic Network Interface(ENI), an SLB instance, or a NAT gateway. For more information, see EIP user guide.

EIPs have the following benefits:

- Independent purchase and possession

  You can purchase and hold an EIP as an independent resource. You do not need to purchase it together with other computing or storage resources.

- Flexible association

  You can associate an EIP with a cloud resource as needed. You can also dissociate and release the EIP at any time.

- Configurable network capabilities

  You can adjust the bandwidth of an EIP at any time. The new bandwidth immediately takes effect.

NAT gateways

NAT gateways are enterprise-class Internet gateways. NAT gateways provide network address translation services, including SNAT and DNAT, with a throughput capacity of up to 10 Gbit/s. NAT gateways can also be used in cross-zone disaster recovery.

NAT gateways support multiple ECS instances by using the same public IP address to access the Internet. For more information, see Use the SNAT feature of an Internet NAT gateway to access the Internet.

NAT gateways have the following benefits:

- Easy-to-use forwarding capability

  NAT gateways serve Internet-facing enterprise workloads that are deployed in VPCs. Each NAT gateway supports SNAT and DNAT rules. You can configure SNAT and DNAT rules without the need to create a NAT gateway.

- High availability

  NAT gateways are virtual network devices that are developed based on distributed gateways of Alibaba Cloud. The software-defined networking (SDN) technology applies to NAT gateways. Each NAT gateway supports a forwarding capability of up to 10 Gbit/s, and can serve large-scale Internet applications.

- Flexible specification adjustment

  You can change the specification of your NAT gateway, or the number and specifications of the EIPs associated with the NAT gateway at any time to provide flexible support for your services.

SLB instances

SLB instances can be used to distribute network traffic among multiple ECS instances. This optimizes the service capabilities of your applications. This also eliminates single point of failures (SPOFs) and improves the availability of your applications.

SLB is a port-based service that provides Layer-4 and Layer-7 load balancing. ECS instances that are connected to SLB can be accessed over the Internet. For more information, see Server load balancer overview.

> **Note** ECS instances that are deployed in VPC networks cannot access the Internet through SLB. In this case, SNAT rules are not supported.

SLB has the following benefits:

- High availability of the SLB architecture

  SLB instances are deployed in clusters to synchronize sessions and protect backend servers from SPOFs. This improves redundancy and ensures service stability.

- High-availability with one SLB instance

  SLB supports cross-zone deployment in most regions. This allows you to achieve disaster recovery across data centers. If the primary zone suffers an outage, a failover is triggered to redirect requests to the servers in the secondary zone within approximately 30 seconds. After the primary zone is restored, traffic will be automatically switched back to the servers in the primary zone.

- High-availability with multiple SLB instances

  You can deploy SLB instances and ECS instances in multiple zones within the same region or across different regions, and use Alibaba Cloud DNS to schedule requests.

- High-availability with backend ECS instances

SLB performs health checks to verify the availability of backend ECS instances. The health check feature improves the availability of frontend services by minimizing downtime caused by health issues of backend servers.

3.Connect VPCs

You can connect different virtual private clouds (VPCs) by using Cloud Enterprise Network (CEN) and VPN gateways.

CEN

CEN allows you to establish private connections between VPCs. CEN facilitates network convergence and improves the quality and security of communication through automatic route advertising and learning. For more information, see Cloud Enterprise Network.

You can use CEN to connect VPCs that belong to the same Alibaba Cloud account or different Alibaba Cloud accounts. The following table describes the scenarios.

Scenario	References
Connect VPCs that belong to the same Alibaba Cloud account	Use Enterprise Edition transit routers to enable intra-region communication between on-premises and cloud networks
Connect VPCs that belong to different Alibaba Cloud accounts	Use Enterprise Edition transit routers to connect VPCs across regions and accounts

CEN has the following benefits:

- Network connections in different regions

  CEN allows cloud resources that are deployed in different regions around the world to communicate with each other. CEN ensures that the IP addresses are unique and do not conflict with each other. In addition, CEN automatically advertises and learns routes to accelerate route convergence.

- Low latency and high speed

  CEN provides low-latency and high-speed network transmission. CEN ensures that on-premises networks communicate with each other at the highest data transfer rate supported by the device ports. CEN provides network connections with lower latency than Internet connections.

- Nearest access and shortest path transmission

  CEN has access points and nodes deployed on a global scale to support nearest access to Alibaba Cloud. Compared with communication over the Internet, CEN connections provide lower network latency.

- Standby connections and disaster recovery

  CEN provides at least four standby connections between two nodes. Therefore, CEN ensures high availability for your services. If some connections fail to work, the standby connections take over. This way, CEN ensures that your service is not interrupted and prevents network jitter.

- Systematic management

  CEN can monitor networks in a systematic manner and automatically detects route conflicts that are caused by system changes. This ensures the stability of your services.

VPN Gateway

VPN Gateway is an Internet-based networking service that supports route-based IPsec-VPN connections. You can connect VPCs by establishing secure and reliable IPsec-VPN connections. For more information, see Establish IPsec-VPN connections between two VPCs.

VPN Gateway has the following benefits:

- Security

  VPN Gateway uses the IKE and IPsec protocols in data transmission to ensure data security.

- High Availability

  The active-active architecture enables VPN Gateway to perform failovers within seconds. This ensures that your service and session are not interrupted when errors occur.

- Cost-effectiveness

  The encrypted Internet-based connections provided by VPN Gateway are more cost-effective than Express Connect circuits.

- Simple configurations

  VPN Gateway is an out-of-the-box service and configurations immediately take effect.

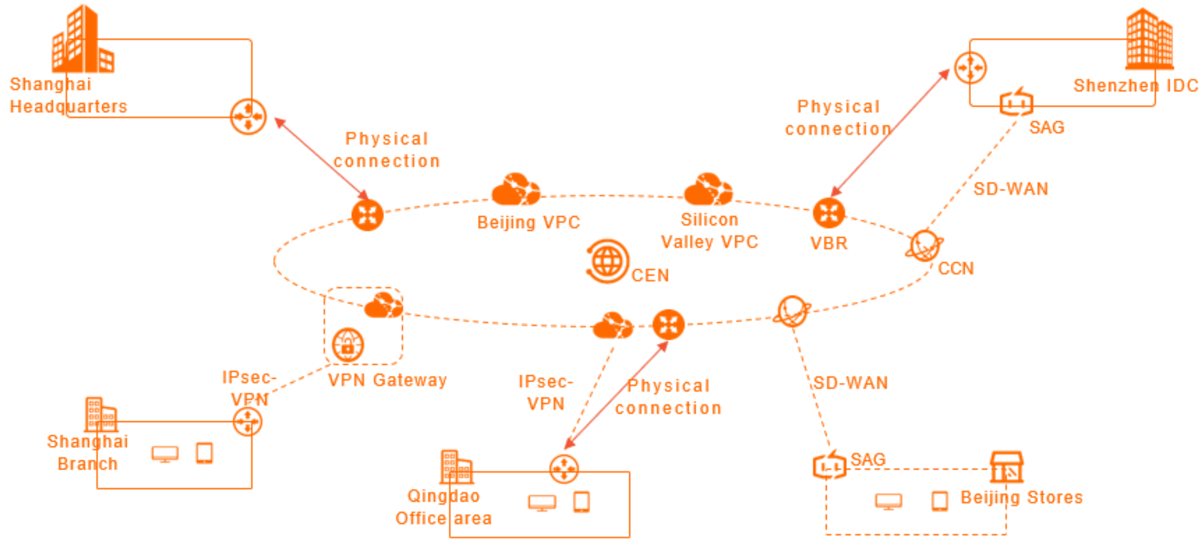
4.Connect a data center to a VPC

This topic describes how to build a hybrid cloud by connecting a data center to a virtual private cloud (VPC). You can connect a data center to a VPC through a VPN gateway, an Express Connect circuit, or Smart Access Gateway (SAG).

Overview

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

You can connect a data center to a VPC through a VPN gateway, an Express Connect circuit, or SAG. You can also use Cloud Enterprise Network (CEN) to connect networks around the world.



Solutions

Solution	Description
VPN gateways	You can use VPN gateways to establish IPsec-VPN connections between your data centers and VPCs. By default, VPN gateways support the active-active mode where two VPN gateways are used. In this mode, the system automatically performs a failover when one VPN gateway is not working as expected. IPsec-VPN connections are established over the Internet. Therefore, the network latency and availability are based on the Internet. If you do not require low network latency, we recommend that you use VPN gateways. For more information, see Connect a data center to a VPC.

Solution	Description
Express Connect circuits	You can use an Express Connect circuit provided by an Internet service provider (ISP) to connect your data center to an Alibaba Cloud access point. You can also apply for dedicated Express Connect circuits. Connections over Express Connect circuits provide low network latency and high bandwidth. We recommend that you use Express Connect circuits if you require low network latency. For more information, see Create a dedicated connection over an Express Connect circuit.
SAG	SAG is a one-stop solution for connecting private networks to Alibaba Cloud. You can use SAG to connect private networks to Alibaba Cloud over the Internet. The connections established by SAG are secure and reliable. SAG is easy to use and cost-effective. To connect multiple on-premises branch sites to Alibaba Cloud, we recommend that you use SAG. For more information, see Deploy an SAG device in inline mode.
Standby Express Connect circuits	You can establish high-quality and reliable connection between your data center and Alibaba Cloud by using standby Express Connect circuits. You can use up to four Express Connect circuits to achieve equal-cost multi-path routing (ECMP). For more information, see Establish active/active connections between a data center and Alibaba Cloud.
Active/standby connection	You can use an Express Connect circuit and a Cloud Enterprise Network (CEN) instance to connect a data center to VPCs in different regions. For more information, see Establish active/standby connections between a data center and Alibaba Cloud.
Express Connect circuits and standby connections	• After you connect your data center to Alibaba Cloud over an Express Connect circuit, you can use SAG 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 Layer 3 switch). • After you connect your data center to Alibaba Cloud over an Express Connect circuit, you can use a VPN gateway to establish a standby IPsec-VPN connection. This ensures the high availability of your hybrid cloud.