ALIBABA CLOUD

Alibaba Cloud

Virtual Private Cloud
Product Introduction

Document Version: 20220622

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

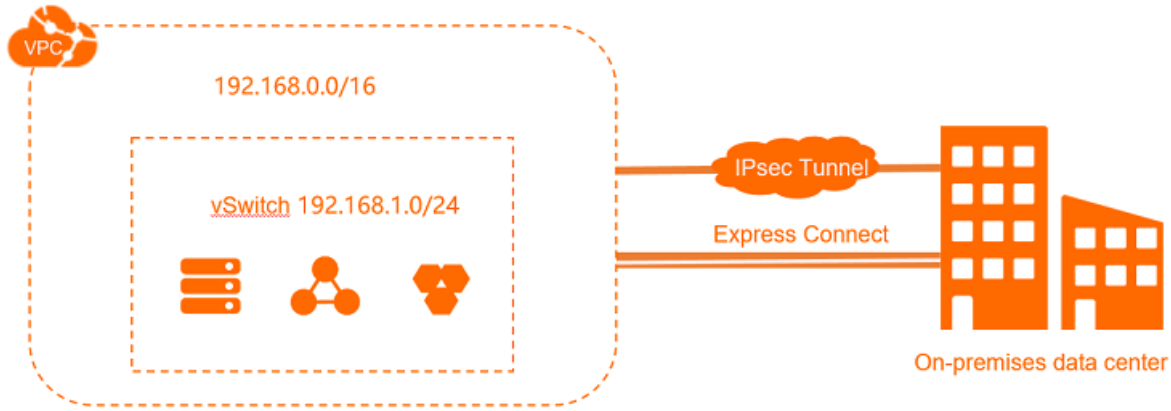
Style	Description	Example
Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	**Danger:** Resetting will result in the loss of user configuration data.
Warning	A warning notice indicates a situation that may cause major 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.What is a VPC?

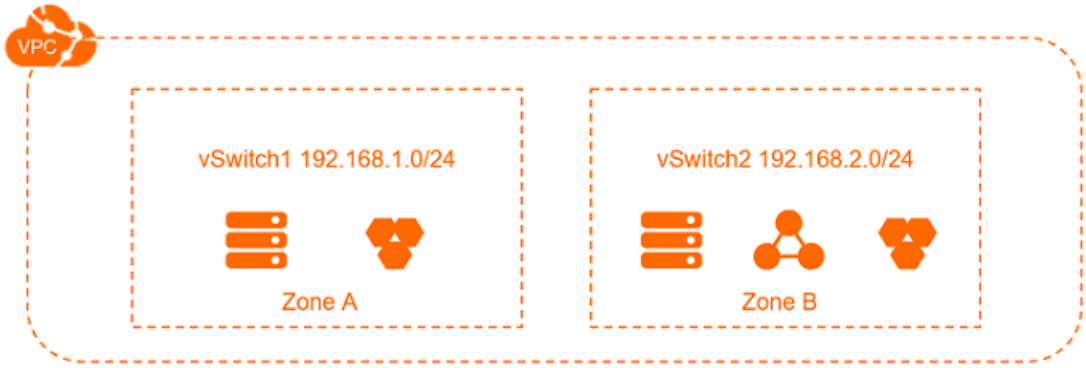
A virtual private cloud (VPC) is a private network dedicated for your use. You have full control over your VPC. For example, you can specify the CIDR block and configure route tables and gateways. In a VPC, you can deploy Alibaba Cloud resources, such as Elastic Compute Service (ECS) instances, ApsaraDB RDS instances, and Server Load Balancer (SLB) instances.

Furthermore, you can connect your VPC to other VPCs or on-premises networks through Express Connect circuits to create a custom network environment. This way, you can migrate applications to the cloud and extend data centers.



Components

Each VPC consists of at least one private CIDR block, a vRouter, and at least one vSwitch.



- Private CIDR blocks

  When you create a VPC and a vSwitch, you must specify the private IP address range for the VPC in CIDR notation.

  You can use one of the standard private CIDR blocks listed in the following table or their subnets as the private CIDR block of a VPC, or use a custom CIDR block. For more information, see Plan networks.

CIDR blocks	Description
192.168.0.0/16	Number of available private IP addresses (excluding IP addresses reserved by the system): 65,532

CIDR blocks	Description
172.16.0.0/12	Number of available private IP addresses (excluding IP addresses reserved by the system): 1,048,572
10.0.0.0/8	Number of available private IP addresses (excluding IP addresses reserved by the system): 16,777,212
Custom CIDR block	Custom CIDR blocks except 100.64.0.0/10, 224.0.0.0/4, 127.0.0.0/8, 169.254.0.0/16, and their subnets

- vRouters

  A vRouter is the hub of a VPC. As a core component, it connects the vSwitches in a VPC and serves as a gateway between a VPC and other networks. After a VPC is created, a vRouter is automatically created for the VPC. Each vRouter is associated with a route table.

  For more information, see Route table overview.

- vSwitches

  A vSwitch is a basic network component that connects different cloud resources in a VPC. After you create a VPC, you can create vSwitches to divide the VPC into one or more subnets. vSwitches deployed in a VPC can communicate with each other over the private network. You can deploy your applications in vSwitches that belong to different zones to improve service availability.

  For more information, see vSwitches.

2.Service architecture

Virtual private clouds (VPCs) are isolated from each other based on a tunneling technology. Each VPC is identified by a unique tunnel ID, which corresponds to a virtualized network.

Background information

The development of cloud computing technologies leads to higher requirements for virtual networks, such as scalability, security, reliability, privacy, and robust connectivity performance. This speeds up the development of various technologies about network virtualization.

In earlier solutions, virtual and physical networks are merged to generate a flat network architecture, such as large-scale Layer 2 networks. As the scale of virtual networks grows, these solutions encounter problems such as Address Resolution Protocol (ARP) spoofing, broadcast storms, and host scanning. To resolve these problems, various network isolation technologies emerged. With these technologies, physical networks are isolated from virtual networks. One of these technologies adopts virtual local area networks (VLANs) to isolate networks. However, VLANs support at most 4096 VLAN IDs and do not apply to large-scale networks.

How VPC works

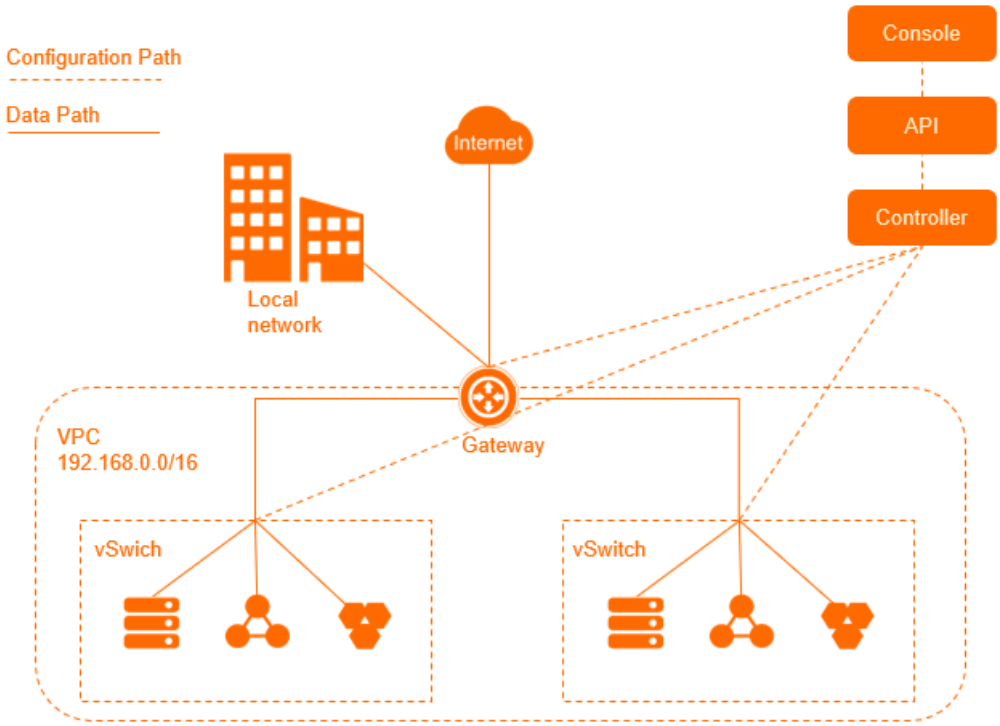
VPCs are isolated from each other based on a tunneling technology. Each VPC is identified by a unique tunnel ID, which corresponds to a virtual network.

- Data packets are encapsulated with a unique tunnel ID and transmitted over a physical network between Elastic Compute Service (ECS) instances in a VPC.
- Data packets transmitted over ECS instances in different VCPs have different tunnel IDs. Therefore, ECS instances in different VPCs cannot communicate with each other.

Alibaba Cloud developed VPCs that are integrated with gateways and vSwitches by adopting the tunneling and Software Defined Network (SDN) technologies.

Logical architecture of VPCs

A VPC contains a gateway, a controller, and one or more vSwitches, as shown in the following figure. The vSwitches and gateway form a data path where data is transferred. The controller uses a protocol developed by Alibaba Cloud to form a configuration path. The data path is isolated from the configuration path. vSwitches in VPCs are distributed nodes while gateways and controllers are deployed in clusters in multiple data centers. All VPC connections support disaster recovery, which ensures the high availability.


Configuration Path
Data Path
Console
API
Controller
Internet
Local network
Gateway
VPC
192.168.0.0/16
vSwich
vSwitch

3.Benefits

This topic describes the benefits of virtual private clouds (VPCs). VPCs are secure, reliable, flexible, easy to use, and scalable.

Security and reliability

Each VPC is identified by a unique tunnel ID, which corresponds to a virtual network. Different VPCs are isolated by tunnel IDs:

- Similar to a traditional network, you can create vSwitches and vRouters to divide a VPC into multiple subnets. Elastic Compute Service (ECS) instances in the same subnet use the same vSwitch to communicate with each other, while ECS instances in different subnets use vRouters to communicate with each other.
- VPCs are completely isolated from each other. Cloud resources in different VPCs can communicate with each other by using elastic IP addresses (EIPs) or NAT IP addresses.
- The IP packets of an ECS instance are encapsulated by using the tunneling technology. Therefore, information at the data link layer (the MAC address) of the ECS instance is not transferred to the physical network. This way, ECS instances in different VPCs are isolated at Layer 2.
- ECS instances in a VPC use security groups as firewalls to control inbound and outbound traffic at Layer 3.

Flexible management

You can use security group rules and access control lists (ACLs) to manage inbound and outbound traffic to cloud resources in a VPC in a flexible manner.

Ease of use

You can easily create and manage VPCs in the VPC console. When you create a VPC, the system automatically creates a vRouter and a route table for the VPC.

High scalability

You can create different subnets in a VPC to deploy different services. Additionally, you can connect a VPC to a data center or another VPC to extend the network architecture.

4.Common scenarios

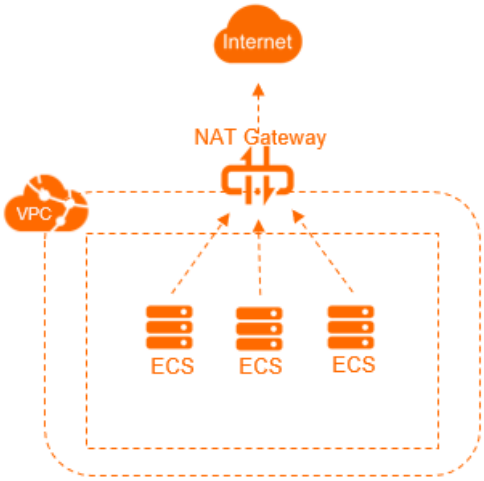
Virtual private clouds (VPCs) are virtual networks that are isolated from each other. VPCs support flexible configurations to meet requirements of different scenarios.

Deploy applications in a safe manner

Applications deployed in a VPC can provide services to the outside. To control access to the applications over the Internet, you can create security group rules and configure whitelists. You can also isolate application servers from databases to implement access control. For example, you can deploy web servers in a subnet that can access the Internet, and deploy databases in another subnet that cannot access the Internet.

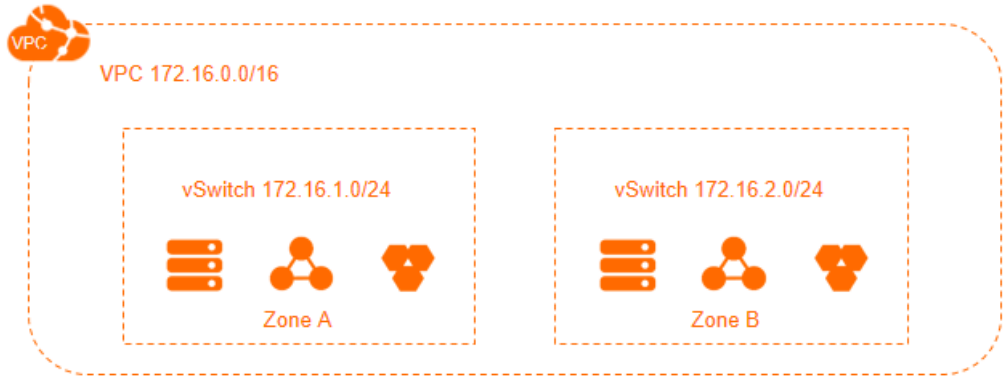
Deploy applications that require access to the Internet

You can deploy applications that require access to the Internet in a subnet of a VPC and use an Internet NAT gateway to route network traffic. You can configure SNAT entries to allow instances in the subnet to access the Internet without the need to expose the private IP addresses. In addition, you can change the elastic IP addresses (EIPs) specified in the SNAT entries to prevent attacks from the Internet.



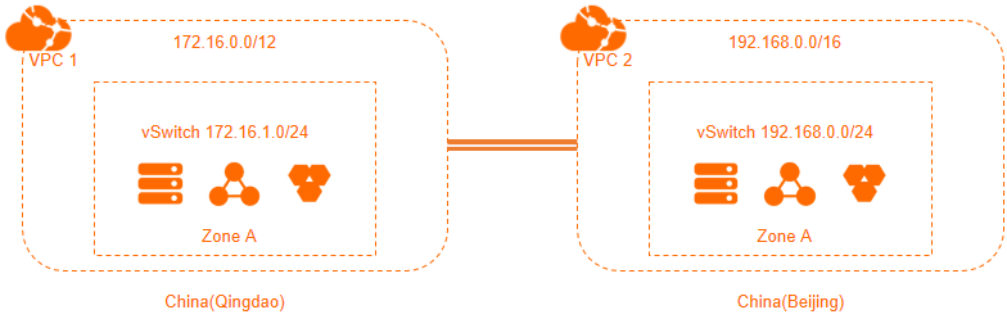
Implement cross-zone disaster recovery

You can create one or more vSwitches to create one or more subnets for the VPC. vSwitches within the same VPC can communicate with each other. To implement cross-zone disaster recovery, you can deploy resources across vSwitches in different zones.



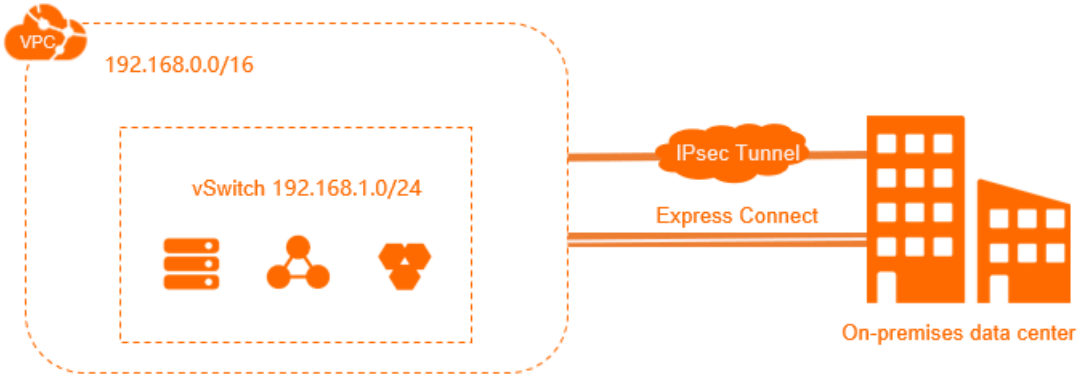
Isolate business systems

VPCs are logically isolated from each other. You can use multiple VPCs to isolate business systems in different environments such as production and test environments. If you want to enable a VPC to communicate with another one, you can attach the VPCs to a Cloud Enterprise Network (CEN) instance. For more information, see What is CEN?.



Build a hybrid cloud

To expand your on-premises network, you can establish a dedicated connection between a VPC and your data center. This allows you to seamlessly migrate the applications in your data center to the cloud. You do not need to change the access method for the applications.



5.Terms

This topic describes basic terms about Virtual Private Cloud (VPC).

Term	Description
VPC	A VPC is a private network deployed on Alibaba Cloud. VPCs are logically isolated from each other. You can create and manage cloud resources in your VPC, such as Elastic Compute Service (ECS), Server Load Balancer (SLB), and ApsaraDB RDS instances.
vSwitch	A vSwitch is a basic network device that connects different cloud resources. When you create a cloud resource in a VPC, you must specify a vSwitch to which the cloud resource is connected.
vRouter	A vRouter is a virtual router that connects all vSwitches in a VPC and serves as a gateway that connects the VPC to other networks. A vRouter also forwards network traffic based on the route entries in the route table.
Route table	A route table consists of route entries in a vRouter.
Route entry	Each item in a route table is a route entry. A route entry specifies the next hop address for the network traffic that is destined for a destination CIDR block. Route entries are classified into system route entries and custom route entries.

6.Manage VPC connections

You can connect a virtual private cloud (VPC) to the Internet, another VPC, or a data center.

7.Advanced VPC features

This topic describes the advanced features supported by Virtual Private Cloud (VPC). These features include network access control lists (ACLs), custom route tables, and Dynamic Host Configuration Protocol (DHCP) options sets. Some Elastic Compute Service (ECS) instance families do not support the advanced features. If a VPC contains one or more ECS instances that belong to these ECS instance families, you cannot use the advanced VPC features.

Overview

Advanced VPC features include network ACLs, custom route tables, and DHCP options sets. For more information, see the following topics:

- Network ACLs
- Custom route tables
- Overview of DHCP options sets

Limits on ECS instance families

Advanced VPC features have the following limits on ECS instance families:

- If a VPC contains one or more ECS instances that belong to one of the following instance families, you cannot use the advanced VPC features.

  > Note
  > - You can view information about advanced VPC features on the **Advanced Features** tab.
  >   - Information about whether the specified VPC supports advanced VPC features.
  >   - The advanced VPC features that the specified VPC supports.
  >   - The resources that do not support advanced VPC features in the specified VPC.
  >
  >   For more information, see View a VPC.
  > - When you configure an advanced VPC feature, the system automatically checks the ECS instances deployed in the VPC. If one or more ECS instances belong to one of the following instance families, you cannot configure the advanced VPC feature.

- If a VPC has an advanced VPC feature enabled, you cannot create an ECS instance that belongs to one of the following instance families. In addition, you cannot migrate such ECS instances from other VPCs to this VPC.

Most ECS instance families support advanced VPC features. The following table describes the ECS instance families that do not support advanced VPC features.

Instance type	Instance family
General purpose	sn2 (discontinued)
Compute-optimized	sn1 (discontinued)
Memory-optimized	se1
Big data	d1

Instance type	Instance family
Local SSD	i1
High clock rate	• c4 (discontinued) • ce4 (discontinued) • cm4 (discontinued)
GPU-optimized	• gn4 • gn5
GPU-accelerated	ga1 (discontinued)
Shared	• n1 (discontinued) • n2 (discontinued) • e3 (discontinued) • xn4 • n4 • mn4 • e4
Generation I	• t1 (discontinued) • s1 (discontinued) • s2 (discontinued) • s3 (discontinued) • m1 (discontinued) • m2 (discontinued) • c1 (discontinued) • c2 (discontinued)

Upgrade or release an ECS instance

If a VPC contains ECS instances of the preceding instance families, you can upgrade or release these instances. After you upgrade or release the ECS instances, you can use advanced VPC features.

- For more information about how to upgrade an ECS instance, see Upgrade the instance types of subscription instances and Change the instance type of a pay-as-you-go instance.
- For more information about how to release an ECS instance, see Release an instance.

Disable advanced VPC features

You can disable advanced VPC features for a VPC. After you disable advanced VPC features, you can create ECS instances of the preceding families in the VPC. For more information, see:

- Delete a network ACL
- Delete a custom route table
- Delete a DHCP options set

8.Regions that support VPC features

This topic describes the regions that support Virtual Private Cloud (VPC) features, and how to apply for participation in a public preview.

In the following table, "√" indicates that a feature is supported in a region, whereas "-" indicates that a feature is not supported in a region. To use a feature during a public preview, you must apply for participation in the public preview. To apply for participation in a public preview, you must use an Alibaba Cloud account.

Region	Custom route table	DHCP options set	VPC sharing	Flow log(submit a ticket)	Network access control list (ACL)	High-availability virtual IP address (HAVIP) (submit a ticket)	IPv4/IPv6 dual-stack	Traffic mirroring
China (Hangzhou)	√	√	√	√	√	√	√	√
China (Shanghai)	√	√	√	√	√	√	√	√
China (Qingdao)	√	√	√	√	√	√	√	√
China (Beijing)	√	√	√	√	√	√	√	√
China (Zhangjiakou)	√	√	√	√	√	√	√	√
China (Hohhot)	√	√	√	√	√	√	√	√
China (Ulanqab)	√	√	√	√	√	√	√	-
China (Shenzhen)	√	√	√	√	√	√	√	√

Region	Custom route table	DHCP options set	VPC sharing	Flow log(submit a ticket)	Network access control list (ACL)	High-availability virtual IP address (HAVIP) (submit a ticket)	IPv4/IPv6 dual-stack	Traffic mirroring
China (Heyuan)	√	√	√	√	√	√	√	√
China (Guangzhou)	√	√	√	√	√	√	√	√
China (Chengdu)	√	√	√	√	√	√	√	√
China (Hong Kong)	√	√	√	√	√	√	√	√
Japan (Tokyo)	√	√	√	√	√	√	-	√
South Korea (Seoul)	√	√	√	-	√	√	-	-
Singapore (Singapore)	√	√	√	√	√	√	√	√
Australia (Sydney)	√	√	√	√	√	√	-	√
Malaysia (Kuala Lumpur)	√	√	√	√	√	√	-	-
Indonesia (Jakarta)	√	√	√	√	√	√	-	-
Philippines (Manila)	√	-	√	-	√	√	√	-

Region	Custom route table	DHCP options set	VPC sharing	Flow log(submit a ticket)	Network access control list (ACL)	High-availability virtual IP address (HAVIP) (submit a ticket)	IPv4/IPv6 dual-stack	Traffic mirroring
Thailand (Bangkok)	√	√	√	-	√	√	-	√
India (Mumbai)	√	√	√	√	√	√	-	-
Germany (Frankfurt)	√	√	√	√	√	√	√	√
UK (London)	√	√	√	√	√	√	-	√
US (Virginia)	√	√	√	√	√	√	√	√
US (Silicon Valley)	√	√	√	√	√	√	-	√
UAE (Dubai)	√	√	√	√	√	√	-	-