Alibaba Cloud
Virtual Private Cloud

Product Introduction

Issue: 20190908

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]*

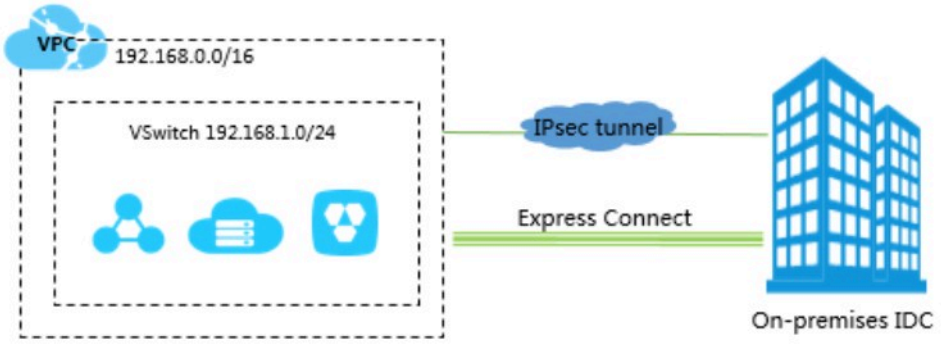
Style	Description	Example
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich {stand | slave}`

Contents

1 What is a VPC?

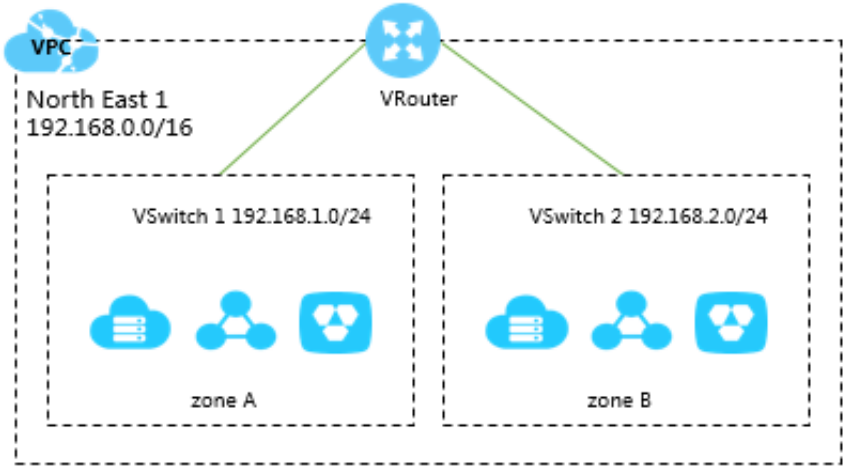
A VPC is a private network in Alibaba Cloud. You can specify the IP address range, configure route tables and gateways, and use Alibaba Cloud resources such as ECS, RDS, and SLB in your VPC.

Furthermore, you can connect your VPC to other VPCs or local networks to create a custom network environment. In this way, you can smoothly migrate applications to the cloud and extend on-premises data centers.



Components

Each VPC consists of a private CIDR block, a VRouter, and one or more VSwitches.



- Private CIDR block

  When you create a VPC or a VSwitch, you must specify the private IP address range in the form of a CIDR block.

  You can use the standard private CIDR blocks listed in the following table and their subnets as CIDR blocks of your VPCs. For more information, see #unique_4. For more information, see *the "Plan a VPC network" chapter of the User Guide* .

CIDR block	Number of available private IP addresses (excluding those reserved by the system)
192.168.0.0/16	65,532
172.16.0.0/12	1,048,572
10.0.0.0/8	16,777,212

- VRouter

  A VRouter is a hub that connects all VSwitches in a VPC and serves as a gateway between the 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 #unique_5.

  For more information, see *the "Route table overview" chapter of the User Guide* .

- VSwitch

  A VSwitch is a basic network device that connects different cloud resources in a VPC. After you create a VPC, you can create one or more subnets in the VPC by creating VSwitches. The VSwitches within a VPC are interconnected. You can deploy your applications on VSwitches that belong to different zones to improve service availability.

  For more information, see Create a VSwitch.

  For more information, see *the "Create a VSwitch" chapter of the User Guide* .

2 VPC connections

Alibaba Cloud provides a wide range of solutions that can connect your VPC to other VPCs, the Internet, or 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_8.	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_11.	· 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_12.	· 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.

3 Architecture

Based on the tunneling technique, VPCs isolate virtual networks. Each VPC has a unique tunnel ID, and each tunnel ID corresponds to only one VPC.

Background information

With the development of cloud computing, a variety of network virtualization techniques have been developed to meet the increasing demands for virtual networks with higher scalability, security, reliability, privacy, and connectivity.

Earlier solutions combined the virtual network with the physical network to form a flat network, for example, the large layer-2 network. However, with the increase of virtual network scale, problems such as ARP spoofing, broadcast storms, and host scanning are becoming more serious. To resolve these problems, various network isolation techniques are developed to completely isolate the physical network from the virtual network. One of these techniques can isolate users with a VLAN. However, a VLAN only supports up to 4,096 nodes, which are insufficient for the large number of users in the public cloud.

Principles

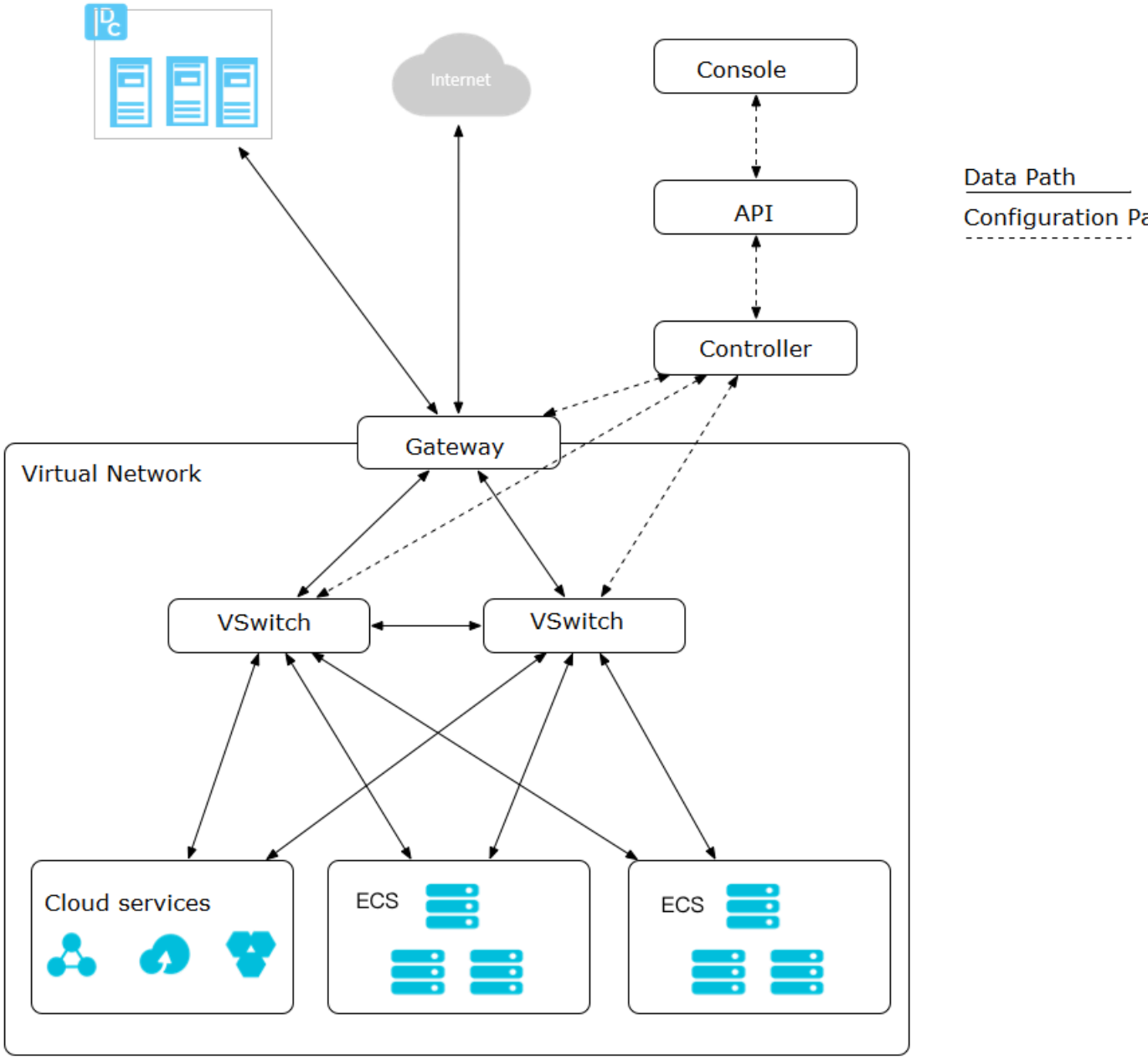
Based on the tunneling technique, VPCs isolate virtual networks. Each VPC has a unique tunnel ID, and each tunnel ID corresponds to only one VPC. A tunnel encapsulation carrying a unique tunnel ID is added to each data packet transmitted over the physical network between ECS instances in a VPC. In different VPCs, ECS instances with different tunnel IDs are located on two different routing planes. Therefore, these ECS instances cannot communicate with each other.

Based on the tunneling and Software Defined Network (SDN) techniques, Alibaba Cloud has developed VPCs that are integrated with gateways and VSwitches.

Logical architecture

As shown in the following figure, a VPC consists of a gateway, a controller, and one or more VSwitches. The VSwitches and gateway form a key data path. By using a protocol developed by Alibaba Cloud, the controller distributes the forwarding table to the gateway and VSwitches to provide a key configuration path. In the overall architecture, the configuration path and data path are separated from each other. The VSwitches are distributed nodes, the gateway and controller are deployed in

clusters, and all links are equipped with disaster recovery. These features improve the availability of the VPC.



4 Benefits

This topic describes the benefits of using VPCs.

High security

Each VPC has a unique tunnel ID, and each tunnel ID corresponds to a virtual network. Different VPCs are isolated by tunnel IDs:

- Similar to traditional networks, VPCs can also be divided into subnets. 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 and can only be interconnected by mapping an EIP or a NAT IP address.
- ECS IP packets are encapsulated by using the tunneling technique. Therefore, information about the data link layer (layer-2 MAC address) of ECS does not go to the physical network. As a result, the layer-2 network between different ECS instances or between different VPCs is isolated.
- ECS instances in a VPC use security groups as firewalls to control traffic going to and from ECS instances. This is layer-3 isolation.

High flexibility

You can use security groups or whitelists to flexibly control traffic going to and from the cloud resources in a VPC.

Ease of use

You can quickly create and manage VPCs in the VPC console. After a VPC is created, the system automatically creates a VRouter and a route table for the VPC.

High scalability

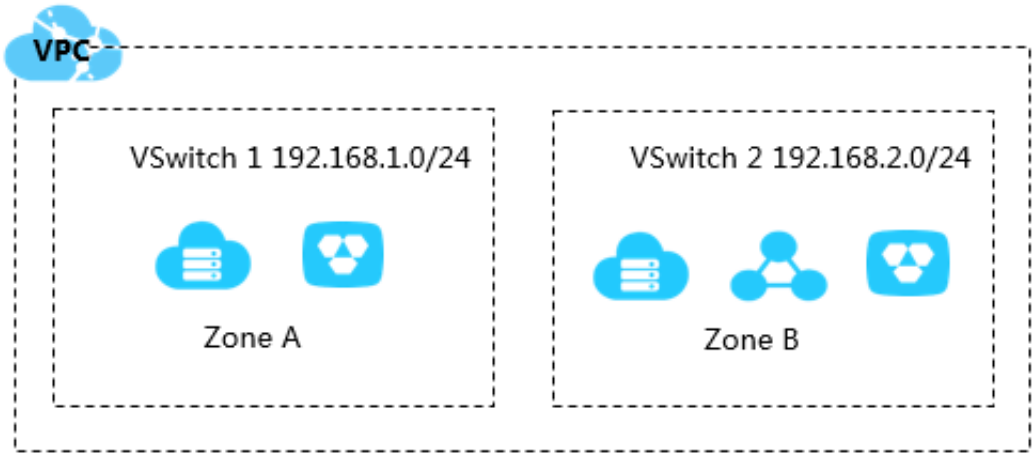
You can create multiple subnets in a VPC to deploy different services. Additionally , you can connect a VPC to other VPCs or on-premises data centers to expand your network.

5 Scenarios

This topic describes the scenarios in which VPCs are used to guarantee a high level of data security and service availability.

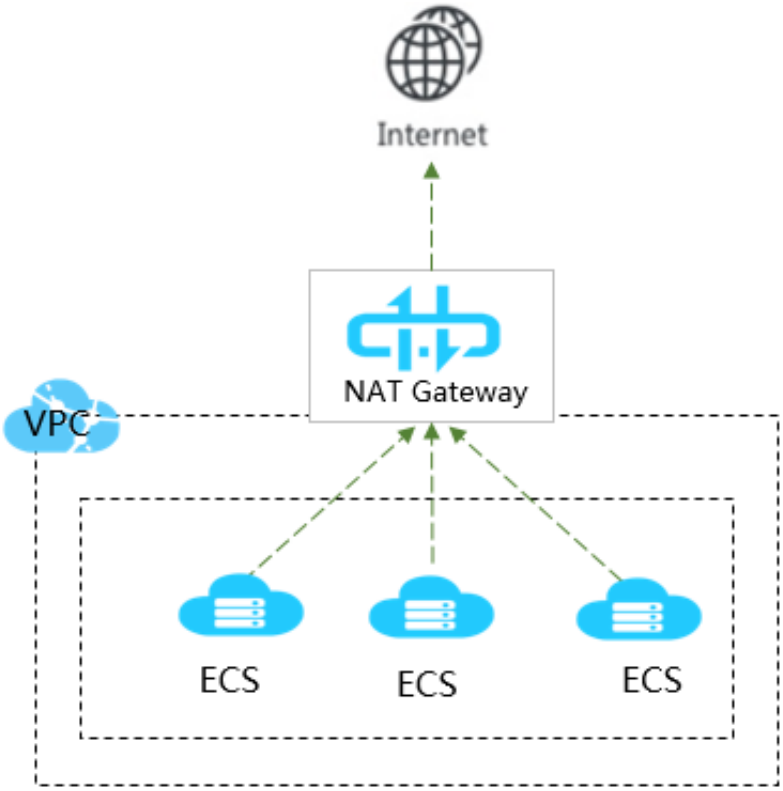
Host applications that provide external services

You can host applications that provide external services in a VPC and control access to these applications from the Internet by creating security group rules and access control whitelists. You can also isolate Internet-based mutual access between the application server and the database. For example, you can deploy the web server in a subnet that can access the Internet and deploy the application database in a subnet that cannot access the Internet.



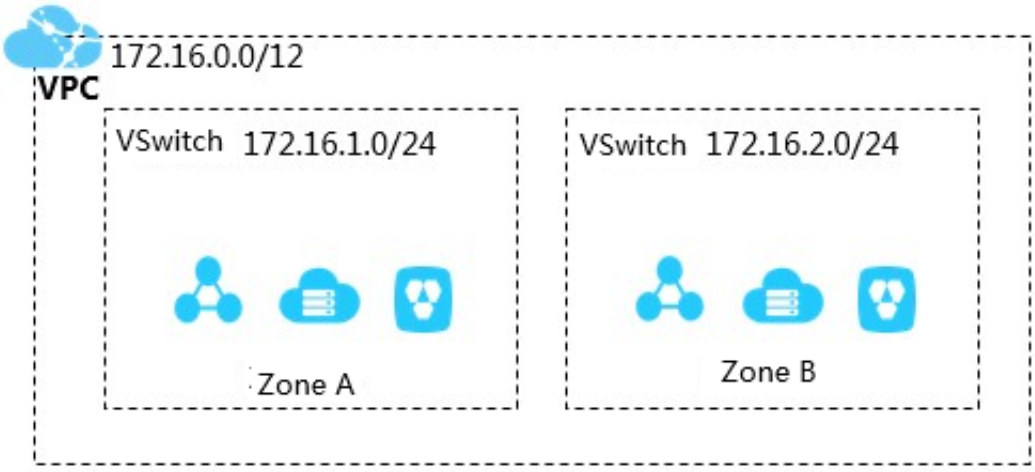
Host applications that require access to the Internet

You can host applications that require access to the Internet in a subnet of a VPC and route traffic through network address translation (NAT). After you configure SNAT rules, instances in the subnet can access the Internet without exposing their private IP addresses, which can be changed to public IP addresses any time to avoid external attacks.



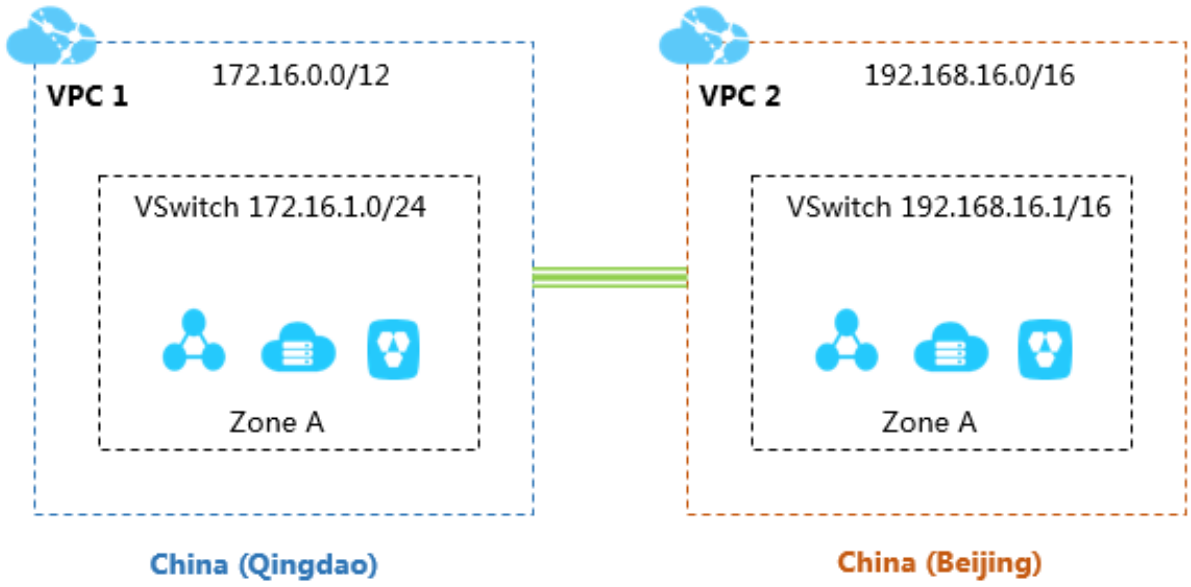
Implement disaster tolerance across zones

You can create one or multiple subnets in a VPC by creating VSwitches. VSwitches in a VPC can communicate with each other. You can deploy resources on VSwitches in different zones for disaster tolerance.



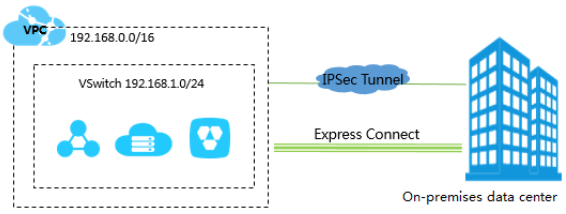
Isolate business systems

VPCs are logically isolated from each other. Therefore, you can create multiple VPCs to isolate multiple business systems, for example, isolate the production environment from the test environment. You can also create a peering connection between two VPCs if they need to communicate with each other.



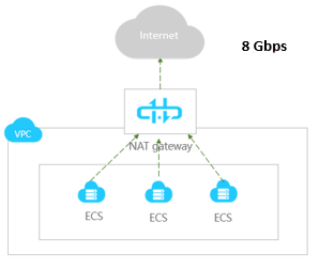
Build a hybrid cloud

You can create a dedicated connection to connect your VPC to an on-premises data center to expand your local network. By doing so, you can seamlessly migrate your local applications to the cloud without changing the method of access to these applications.



Control big bandwidth fluctuations caused by multiple applications

If your applications generate big bandwidth fluctuations, you can configure DNAT forwarding rules through the NAT Gateway. Then, you can add EIPs to Internet Shared Bandwidth so that these EIPs can share the bandwidth. This can reduce bandwidth fluctuations and save your cost.



6 Terms

This topic describes the terms about VPCs.

Term	Description
Virtual Private Cloud (VPC)	A VPC is a private network established in Alibaba Cloud . VPCs are logically isolated from each other. You can create and manage cloud resources in your VPC, such as ECS, SLB, and RDS.
VSwitch	A VSwitch is a basic network device that connect different cloud resources in a VPC. When you create a cloud resource in a VPC, you must specify the VSwitch to which the cloud resource is connected.
VRouter	A VRouter is a hub 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 according to the route entries in its route table.
Route table	A route table is a list 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 directed to a destination CIDR block. Route entries are divided into system route entries and custom route entries.

7 Limits

The following table describes the limits that apply to VPCs.

Resource	Limit	Quota increase supported?
Maximum number of VPCs per region	10	Yes. Open a ticket.
Available CIDR blocks	192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8, and their subnets	Yes. Open a ticket.
Maximum number of VRouters per VPC	1	No.
Maximum number of VSwitches per VPC	24	Yes. Open a ticket.
Maximum number of route tables per VPC	10	Yes. Open a ticket.
Maximum number of custom route entries per route table	48	Yes. Open a ticket.
Maximum number of network addresses used by a single VPC to support cloud products For example, if an ECS instance has only one private IP address, the ECS instance uses one network address. If an ECS instance is associated with multiple NICs or an NIC is configured with multiple IP addresses, the number of network addresses used by the ECS instance is the sum of the VPC addresses assigned to these NICs.	15,000	No.