Alibaba Cloud
Virtual Private Cloud

Product Introduction

Issue: 20181129

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

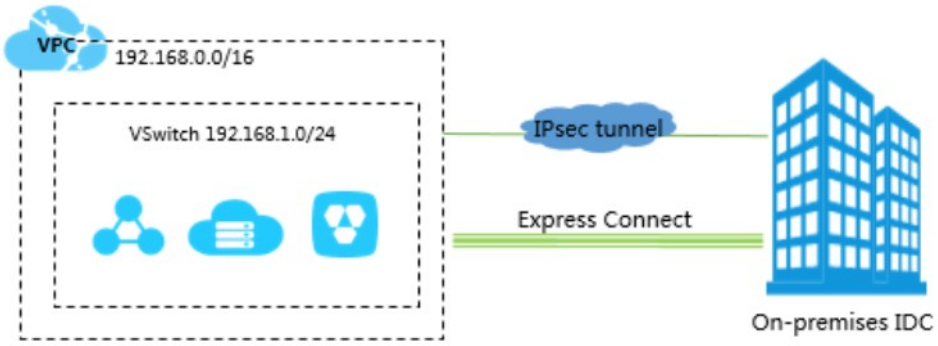
Contents

1 What is VPC?

Virtual Private Cloud (VPC) is a private network established in Alibaba Cloud. VPCs are logically isolated from other virtual networks in Alibaba Cloud.

VPC is a private network dedicated to you in Alibaba Cloud. You have full control over your VPC, such as specifying its IP address range, and configuring route tables and network gateways. You can also use Alibaba Cloud resources such as ECS, RDS, and SLB in your own VPC.

Additionally, you can connect VPCs with a local network using a dedicated connection or VPN Gateway to form an on-demand customizable network environment. This allows you to smoothly migrate applications to the cloud with little effort.



Components

Each VPC consists of a private CIDR block, a VRouter and at least a VSwitch.

- CIDR block

  When creating a VPC or a VSwitch, you must specify the private IP address range in the form of Classless Inter-Domain Routing (CIDR) block. For more information, see *Classless Inter-Domain Routing*.

  You can use any of the following standard CIDR blocks and their subnets as the IP address range of the VPC. For more information, see *Plan and design VPC*.

  Note:
  To use a subnet of a standard CIDR block, you must use the *CreateVpc* API to create a VPC.

CIDR block	Number of available private IPs (system reserved ones not included)
192.168.0.0/16	65,532

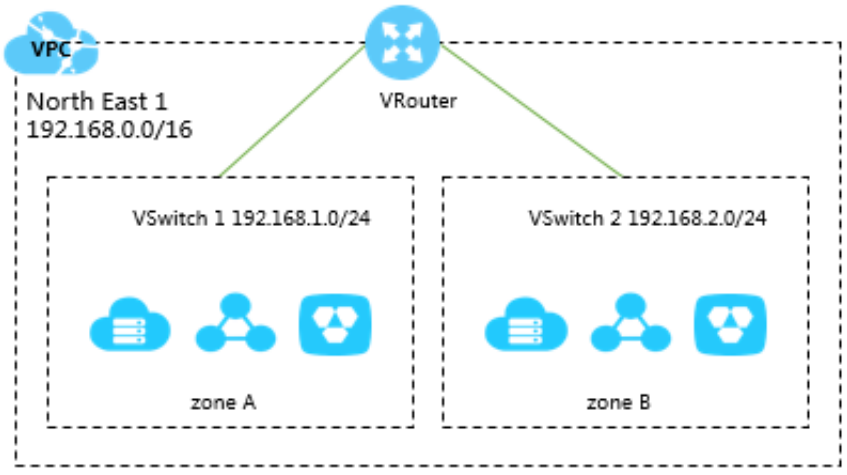
CIDR block	Number of available private IPs (system reserved ones not included)
172.16.0.0/12	1,048,572
10.0.0.0/8	16,777,212

- VRouter

  VRouter is the hub of a VPC. As an important component of a VPC, it connects VSwitches in a VPC and serves as the gateway connecting the VPC with other networks. Alibaba Cloud automatically creates VRouter after you create a VPC. A VRouter associates with a route table by default. For more information, see *Routing*.

- VSwitch

  VSwitch is a basic network module in a VPC to connect different cloud product instances. After creating a VPC, you can further segment your virtual private network to one or more subnets by creating VSwitches. The VSwitches within a VPC are interconnected by default. Therefore, you can deploy different applications to VSwitches that are located in different zones to improve the service availability. For more information, see *Manage VSwitches*.



2 Architecture

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

Background information

With the continuous development of cloud computing, virtual network requirements are getting higher and higher, such as scalability, security, reliability, privacy, and higher requirements of connection performance. This gives a rise to a variety of network virtualization technologies.

The earlier solutions combined the virtual machine's network with the physical network to form a flat network architecture, such as the large layer-2 network. With the increase of virtual network scalability, problems are getting more serious for the earlier solutions. These problems include ARP spoofing, broadcast storms, host scanning, and more. Various network isolation technologies emerged to resolve these problems by completely isolating the physical networks from the virtual networks. One technology isolates users with VLAN, but VLAN only supports up to 4096 nodes. It cannot support the huge amount of users in the cloud.

VPC theory

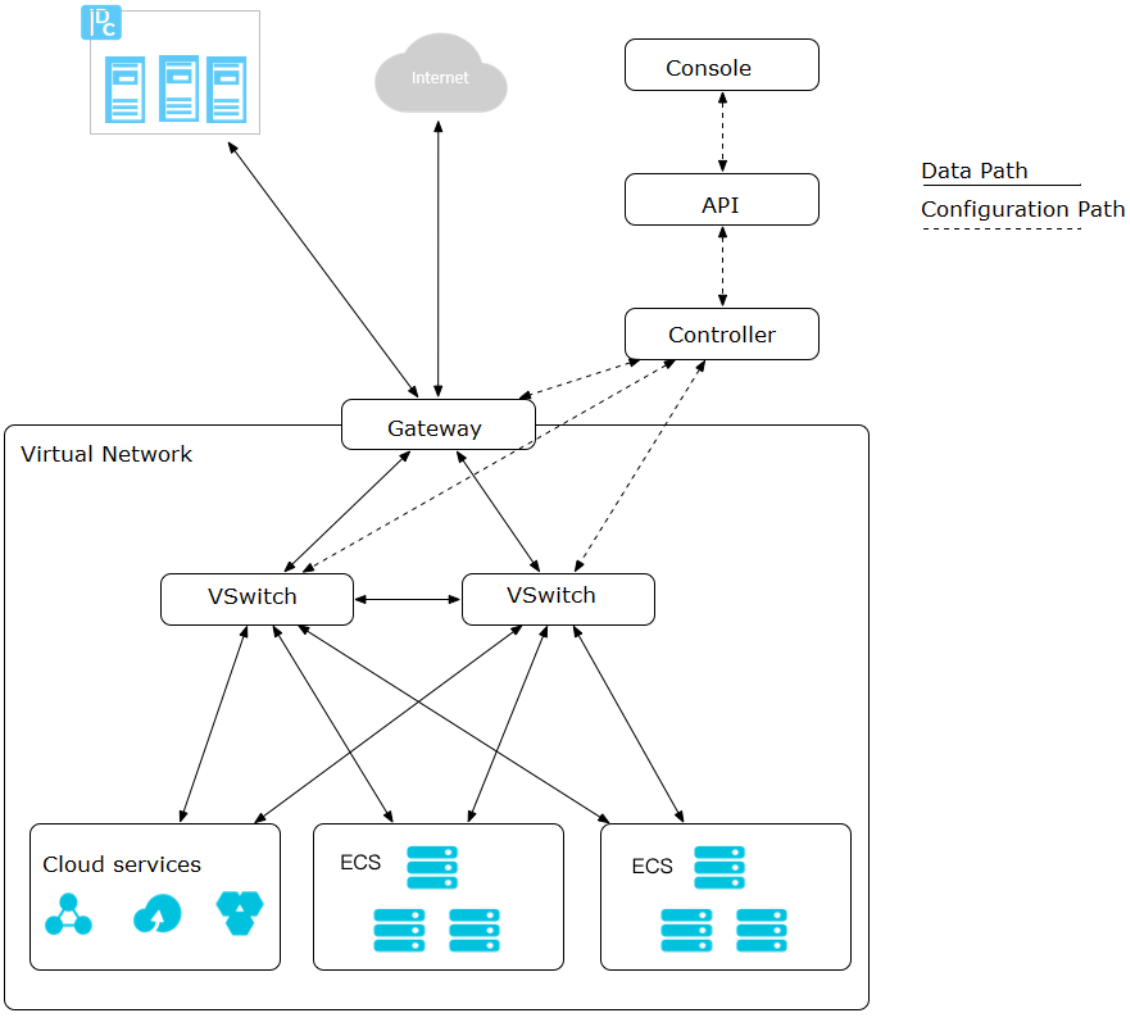
Based on mainstream tunneling technologies, VPCs isolate virtual networks. Each VPC has a unique tunnel ID, and a tunnel ID corresponds to only one VPC. A tunnel encapsulation carrying a unique tunnel ID is added to each data packet transmitted between the ECS instances within a VPC. Then, the data packet is transmitted over the physical network. Because the tunnel IDs are different for ECS instances in different VPCs and the ECS instances are located on two different routing planes, the ECS instances from different VPCs cannot communicate with each other and are isolated by nature.

With the tunneling technology, Alibaba Cloud has developed VSwitch, Software Defined Network (SDN) and hardware gateway and thus created VPC.

Logical architecture

As shown in the following figure, the VPC architecture contains three main components: VSwitches, gateway, and controller. VSwitches and gateways form the key data path. Controllers use the self-developed protocol to forward the forwarding table to the gateway and VSwitches, completing the key configuration path. In the overall architecture, the configuration path and data path are separated from each other. VSwitches are distributed nodes, the gateway and controller

are deployed in clusters, and all links have redundant disaster recovery. This improves the overall availability of the VPC.



3 Benefits

VPC features high security and flexible configuration, and supports multiple connection methods.

Secure

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

- Using VSwitches and VRouters, you can segment your VPC into subnets as you would in the traditional network environment. Different cloud resources in the same subnet use the VSwitch to communicate with each other, while cloud resources in different subnets within a VPC use VRouters to communicate with each other.
- The intranet communication between different VPCs is completely isolated and can only be interconnected by mapping an external IP (Elastic IP and NAT IP).
- The IP packets of ECS are encapsulated with the tunneling ID, the data link layer (two-layer MAC address) will not transfer to the physical network. Therefore, the two-layer network of different ECS is isolated. That is, the two-layer networks between different VPCs are isolated.
- ECS instances in VPC use security groups as firewalls to control the traffic to and from ECS instances. This is the third-layer isolation.

Controllable

You can use security groups or whitelists to control the inbound and outbound traffic going through the cloud resources in a VPC.

Ease of use

You can quickly create and manage your private network on the VPC console. After a VPC is created, the system automatically creates a VRouter and a route table for it.

Scalable

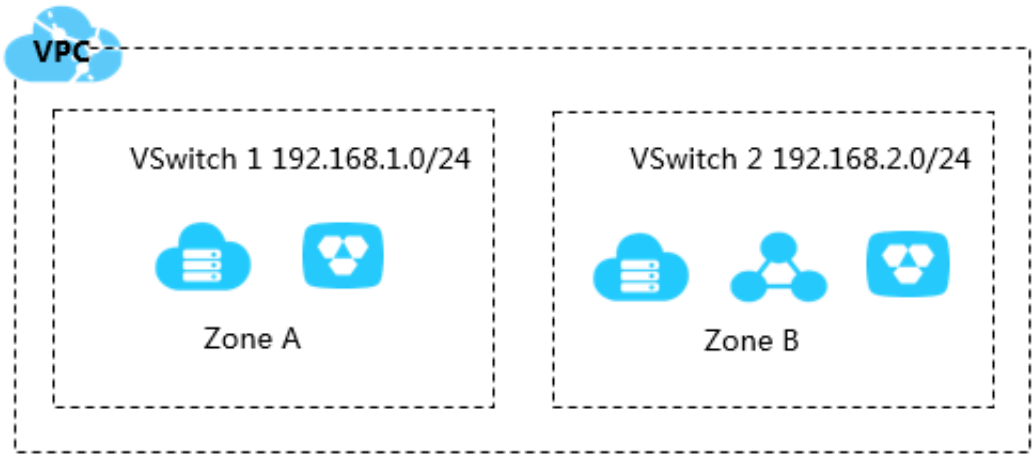
You can create multiple subnets in a VPC to deploy different services. Additionally, you can connect a VPC to a local data center or other VPCs to expand the network architecture.

4 Scenarios

VPC applies to scenarios with high requirement on communication security and service availability.

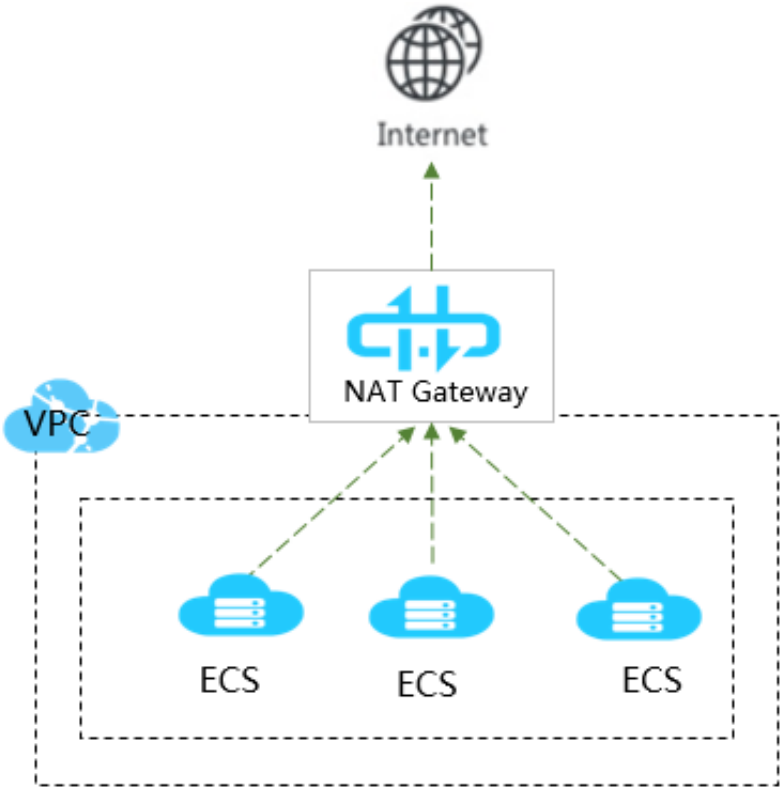
Host applications

You can host an application that provides external services in a VPC and control Internet access by creating security group rules and whitelist. You can also control the access by isolating the application server from the database. For example, deploy the web server in a subnet that can access the Internet and deploy the database of the application in a subnet without Internet access.



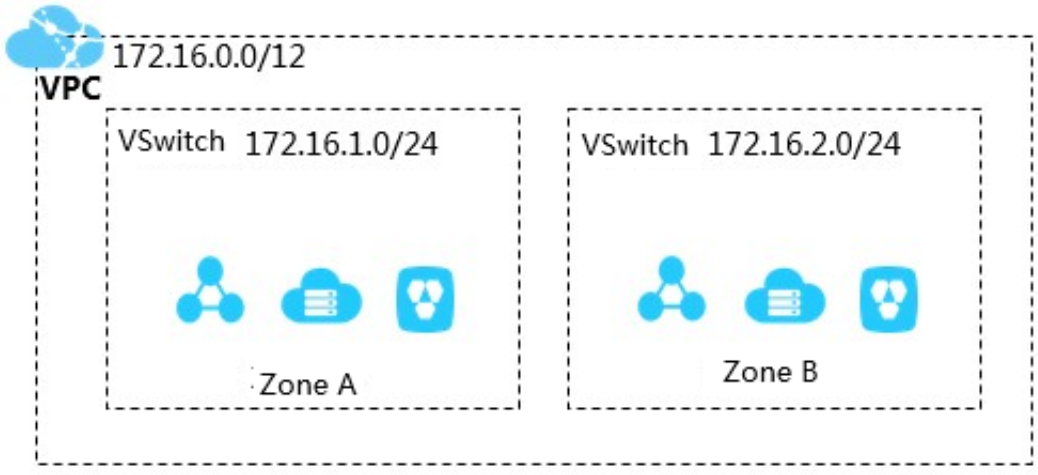
Host applications requiring the access to the Internet

You can host an application that requires to access the Internet in a subnet of a VPC and route the traffic through NAT. By configuring SNAT rules, the instance in the subnet can access the Internet without exposing its private IP address and the private IP address can be changed to a public IP address any time to avoid external attacks.



Cross-zone disaster tolerance

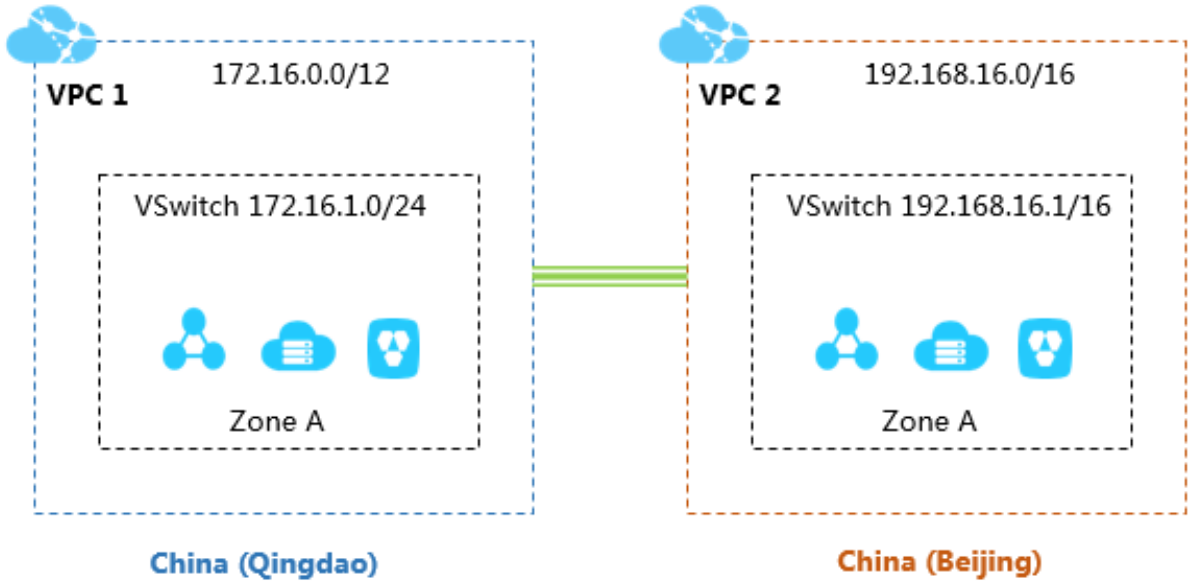
You can create one or multiple subnets in a VPC by creating VSwitches. Different VSwitches in a VPC can communicate with one another through the intranet. You can deploy resources in VSwitches of different zones to achieve cross-zone disaster tolerance.



Business system isolation

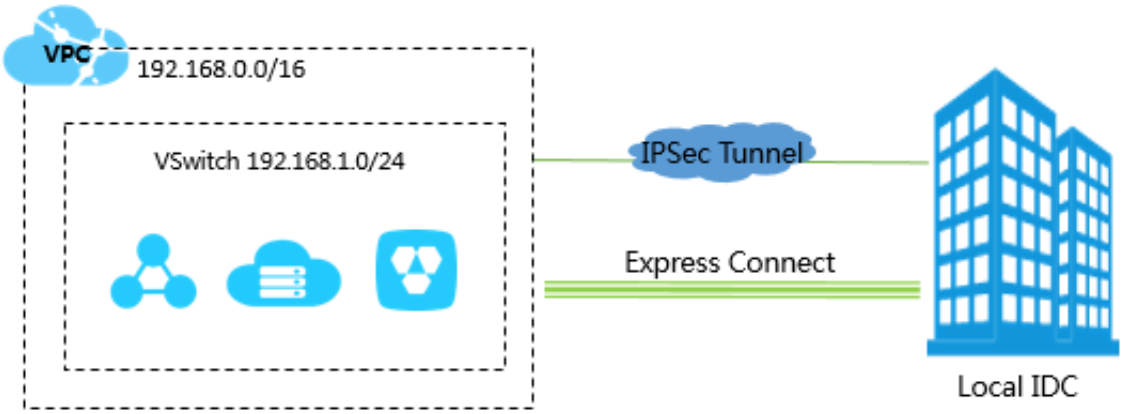
Different VPCs are logically isolated from one another. If you must isolate multiple business systems, such as isolating the production environment from the test environment, you can create

multiple VPCs. When the VPCs need to communicate with each other, you can create a peer connection between them.



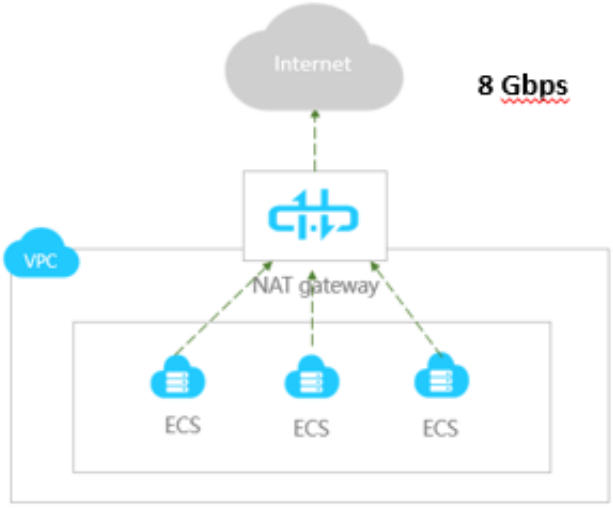
Build hybrid cloud

You can create a dedicated connection to connect your VPC to a local data center to expand your local network. With the dedicated connection, you can seamlessly migrate your local applications to the cloud without changing the way of the application access.



Great bandwidth fluctuation caused by multiple applications

If you applications experience great bandwidth fluctuation, you can configure DNAT forwarding rules through NAT Gateway and add EIPs to *Internet Shared Bandwidth*, so that the EIPs can share the bandwidth, the bandwidth fluctuation can be reduced and your cost can be saved.


Internet
8 Gbps
VPC
NAT gateway
ECS
ECS
ECS

5 Terms

Term	Description
Virtual Private Cloud (VPC)	VPC is a private network established in Alibaba Cloud. It is logically isolated from other virtual networks in Alibaba Cloud. Alibaba Cloud VPC enables you to create and use the Alibaba Cloud resources in your own VPC, such as ECS, SLB, and RDS.
VSwitch	A VSwitch is a basic network device of a VPC and used to connect different cloud product instances. When creating a cloud product instance in a VPC, you must specify the VSwitch that the instance is located.
VRouter	A VRouter is a hub in the VPC that connects all VSwitches in the VPC and serves as a gateway device that connects the VPC to other networks. VRouter routes the network traffic according to the configurations of route entries.
Route Table	A route table is a list of route entries in a VRouter.
Route Entry	Each entry in a route table is a route entry. A route entry specifies the next hop address for the network traffic destined to a CIDR block. It has two types of entries: system route entry and custom route entry.

6 Limits

Resource	Default limits	Ticket submission permits exemption
Maximum number of VPCs per region	10	Submit a ticket to apply for more quota
Available CIDR blocks	192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8, and their subsets	Submit a ticket to apply for more quota
Maximum number of VRouters in a VPC	1	Unsupported
Maximum number of VSwitches in a VPC	24	Submit a ticket to apply for more quota
Maximum number of route tables in a VPC	1	Unsupported
Maximum number of route entries in a route table	48	Submit a ticket to apply for more quota
Maximum number of cloud product instances that can run in a VPC	15,000	Unsupported