Alibaba Cloud
Virtual Private Cloud

Quick Start

Issue: 20190820

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 Plan a VPC network

Before you create VPCs and VSwitches, you must plan the quantity and CIDR block of VPCs and VSwitches according to your specific business needs.

A VPC is a private network in Alibaba Cloud. VPCs are logically isolated from each other. VPCs have the following characteristics:

- Isolated network environment

  Based on the tunneling technique, VPC isolates the data link layer and provides an independent, isolated, and safe network. VPCs cannot communicate with each other unless they are interconnected through an EIP or a NAT IP address.
- Controllable network configurations

  You can specify its IP address range or configure route tables and gateways for secure and easy access to resources. Furthermore, you can connect your VPC to a traditional data center through a leased line or VPN to create a custom network environment. This allows you to smoothly migrate your applications to Alibaba Cloud and expand your data center.

  For more information, see Virtual Private Cloud.

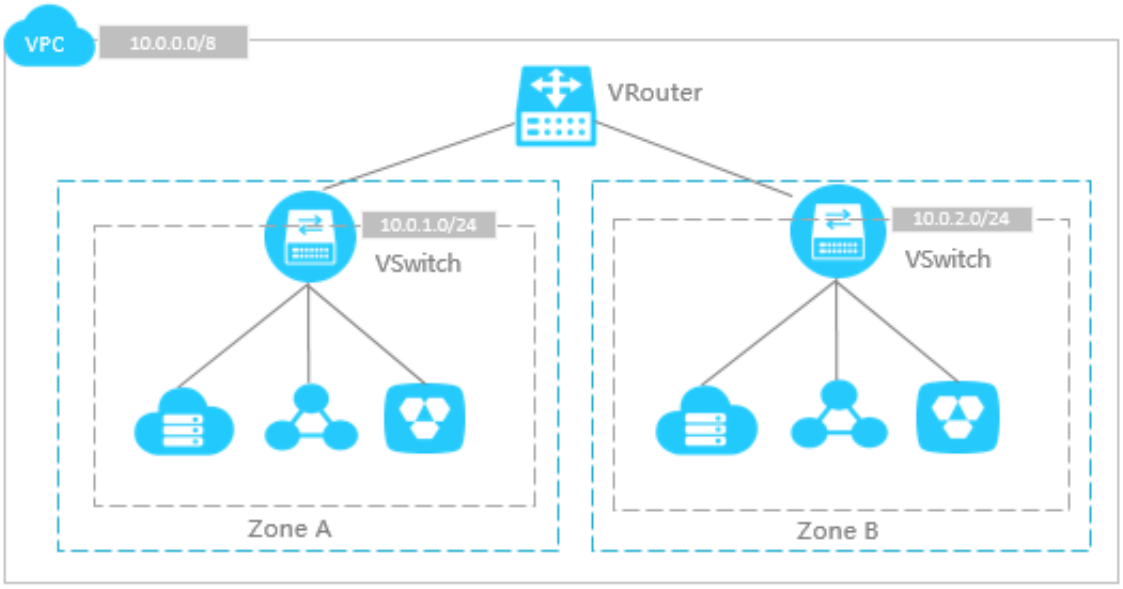
To use a VPC, you must first plan a VPC network. We recommend that you consider the following questions:

- #unique_4/unique_4_Connect_42_section_ocz_5j5_sdb
- #unique_4/unique_4_Connect_42_section_ak2_sm5_sdb
- #unique_4/unique_4_Connect_42_section_yzq_tm5_sdb
- #unique_4/unique_4_Connect_42_section_wn4_tm5_sdb

Question 1: How many VPCs are required?

- One VPC

  We recommend that you create one VPC if you do not need to deploy your business systems in multiple regions or isolate these systems by using VPCs. Currently, a VPC can accommodate up to 15,000 cloud product instances.

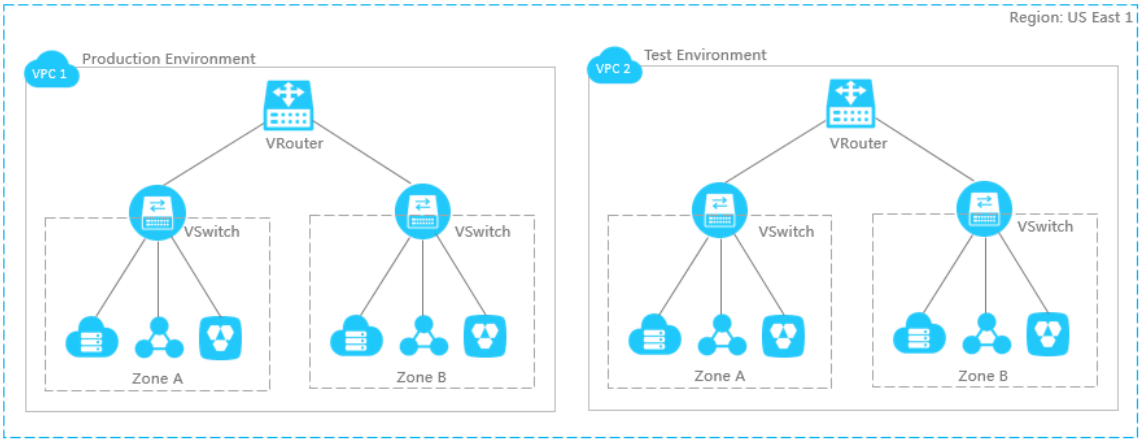


- Multiple VPCs

  We recommend that you create multiple VPCs if you need to:

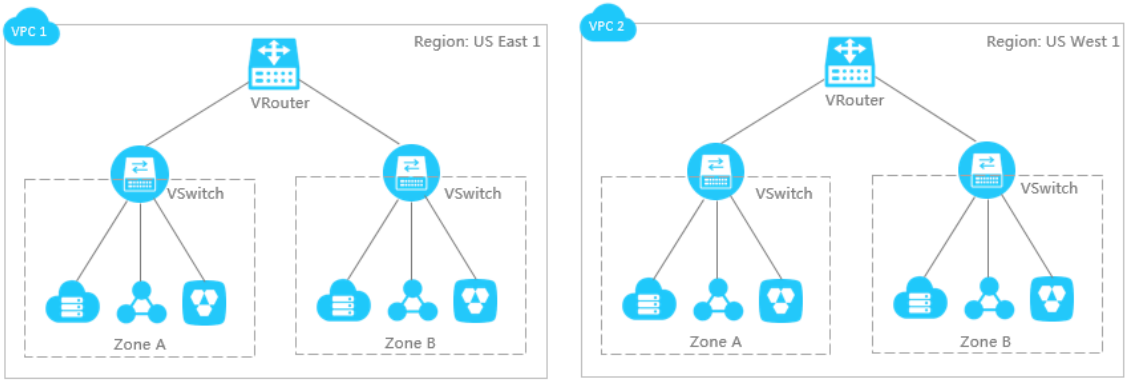
  - Deploy your business systems in multiple regions.

    VPCs are resources that cannot be deployed across regions. If you want to deploy your business systems in different regions, you must create multiple VPCs. You can use Express Connect, VPN Gateway, and CEN to connect VPCs.



  - Isolate multiple business systems.

    To isolate multiple business systems, for example, isolate the production environment from the test environment, you must create multiple VPCs, as shown in the following figure.



Question 2: How many VSwitches are required?

We recommend that you create at least two VSwitches for each VPC and deploy them in two different zones for cross-region disaster tolerance.

We also recommend that you check the network latency between different zones in the same region after you deploy your business systems. This is because the network latency may be higher than expected due to complicated system calls or cross-zone

calls. We recommend that you optimize and adjust your systems accordingly to keep a balance between high availability and low latency.

The number of VSwitches used also relates to the system size and system planning. If your front-end systems can be accessed by the Internet and you want them to access the Internet, you can deploy these systems under different VSwitches. At the same time, you can deploy the backend system in other VSwitches. This helps provide better disaster tolerance.

Question 3: How do I specify the private IP address range?

When you create VPCs and VSwitches, you must specify the private IP address range for these VPCs in the form of a Classless Inter-Domain Routing (CIDR) block.

- Private IP address range of VPCs

  You can use 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8, or their subsets as the private IP address range for your VPC. When you plan the private IP address range of your VPC, note the following:

  - If you have only one VPC and it does not need to communicate with on-premises data centers, you can use any of the preceding IP address ranges or their subnets.
  - If you have multiple VPCs, or you want to build a hybrid cloud consisting of VPCs and on-premises data centers, you can use a subset of the preceding IP address ranges as the IP address range for your VPC. In this case, the netmask cannot be longer than 16 bits.
  - You also need to consider whether a classic network is used when you select a CIDR block for your VPC. If you plan to connect ECS instances in a classic network with your VPC, we recommend that you do not use the IP address range 10.0.0.0/8. This is because the IP address range is also used by the classic network.

- Private IP address range of VSwitches

  A VSwitch can share the same IP address range with the VPC that the VSwitch belongs to. The VSwitch can also use a subnet of the IP address range of the VPC . For example, if the IP address range of the VPC is 192.168.0.0/16, the IP address

range of the VSwitch can be 192.168.0.0/16, or any IP address range between 192.168.0.0/17 and 192.168.0.0/29.

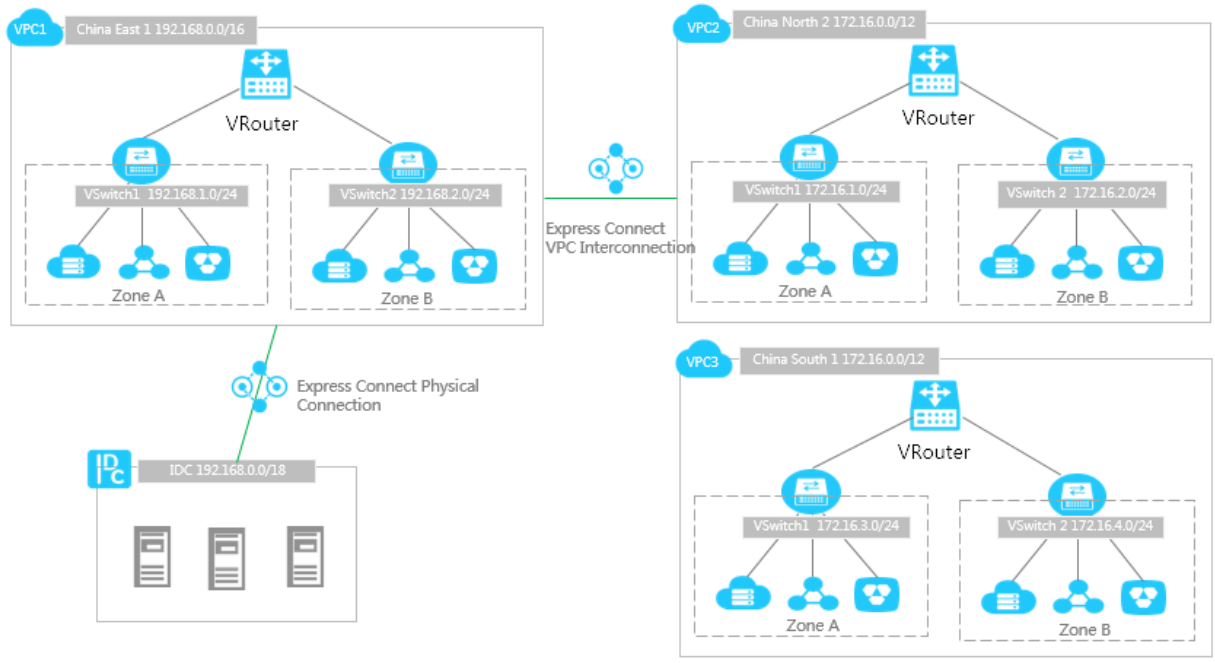
When you plan the IP address range of a VSwitch, note the following:

- The block size for a VSwitch is between a 16-bit netmask and a 29-bit netmask. It means that 8 to 65,536 IP addresses can be provided. This range is set because the 16-bit netmask can provide IP addresses to support 65,532 ECS instances, while a netmask smaller than 29 bits cannot provide sufficient IP addresses.
- The first IP address and the last three IP addresses of each VSwitch are reserved by the system. For example, if the CIDR block of a VSwitch is 192.168.1.0/24, the IP addresses 192.168.1.0, 192.168.1.253, 192.168.1.254, and 192.168.1.255 are reserved.
- The ClassicLink function allows ECS instances in a classic network to communicate with ECS instances in a VPC whose CIDR blocks are 192.168.0.0/16, 10.0.0.0/8, and 172.16.0.0/12. For example, if you want to connect an ECS instance of a VSwitch in a VPC to an ECS instance in the classic network, and the IP address range of the VPC is 10.0.0.0/8, then the IP address range of the VSwitch must be 10.111.0.0/16. For more information, see #unique_5.
- When you plan the IP address range of a VSwitch, you need to consider the number of ECS instances in the VSwitch.

Question 4: How do I specify the private IP address range if I need to connect a VPC to other VPCs or on-premises data centers?

To connect a VPC to other VPCs or on-premises data centers, make sure that the CIDR block of the VPC does not conflict with that of the target network.

For example, you have three VPCs: VPC1 in China (Hangzhou), VPC2 in China (Shanghai), and VPC3 in China (Beijing), as shown in the following figure. VPC1 and VPC2 can communicate with each other through Express Connect. VPC3 does not need to communicate with VPC1 or VPC2 currently, but may need to communicate with VPC2 later. Additionally, you have an on-premises data center in Shanghai, and you need to connect it to VPC1 by using the physical connection of Express Connect.



In this example, the CIDR blocks of VPC1 and VPC2 are different, but the CIDR blocks of VPC2 and VPC3 are the same. This is because VPC3 does not need to communicate with VPC1 or VPC2 currently. However, the VSwitches in VPC2 and VPC3 use different CIDR blocks so that these two VPCs can communicate with each other in future. VPCs that need to communicate with each other can have the same CIDR block, but their VSwitches cannot have the same CIDR block.

When you specify the IP address range for multiple VPCs to allow them to communicate with other VPCs or on-premises data centers, follow these rules:

- Try to specify different IP address ranges for different VPCs. You can use the subsets of the standard IP address ranges to increase the number of available VPC CIDR blocks.
- If you cannot specify different IP address ranges for different VPCs, try to use different CIDR blocks for VSwitches of different VPCs.
- If you cannot use different CIDR blocks for VSwitches of different VPCs, make sure that the VSwitches that need to communicate with each other use different CIDR blocks.

2 Create a VPC

This tutorial shows how to create an ECS instance in a VPC. This tutorial also shows how to attach an EIP to the ECS instance to enable the instance to access the Internet.

Step 1: Create a VPC and a VSwitch

To deploy cloud resources in a VPC, you must first plan the network, create a VPC and create at least one VSwitch. To plan the network, see Network planning.

To create a VPC and a VSwitch, follow these steps:

1. Log on to the VPC console.
2. Select a region.

   The VPC and the cloud resources to deploy must be in the same region. In this tutorial, select the China (Qingdao) region.
3. Configure the VPC and VSwitch. Descriptions about the configuration items are provided in the following table.

   Note:
   In this tutorial, do not select Assign IPv6 Address Free of Charge.

Step 2: Create an ECS instance

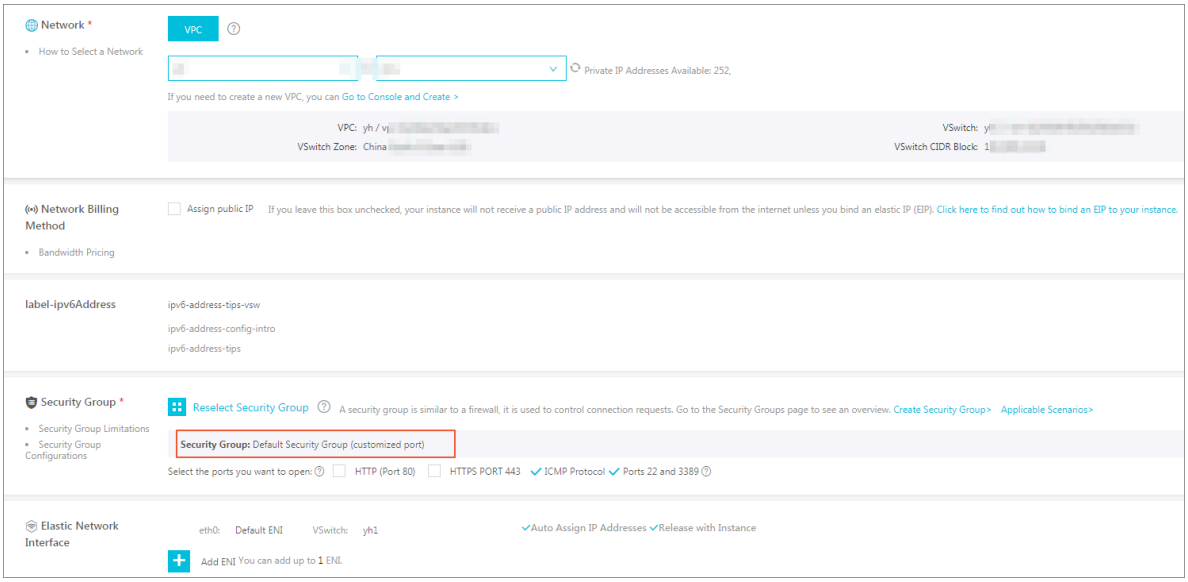
To create an ECS instance in the VPC, follow these steps:

1. In the left-side navigation pane, click VSwitches.
2. Select the target region. In this tutorial, select China (Qingdao).
3. Find the created VSwitch, and then click Purchase > ECS Instance.

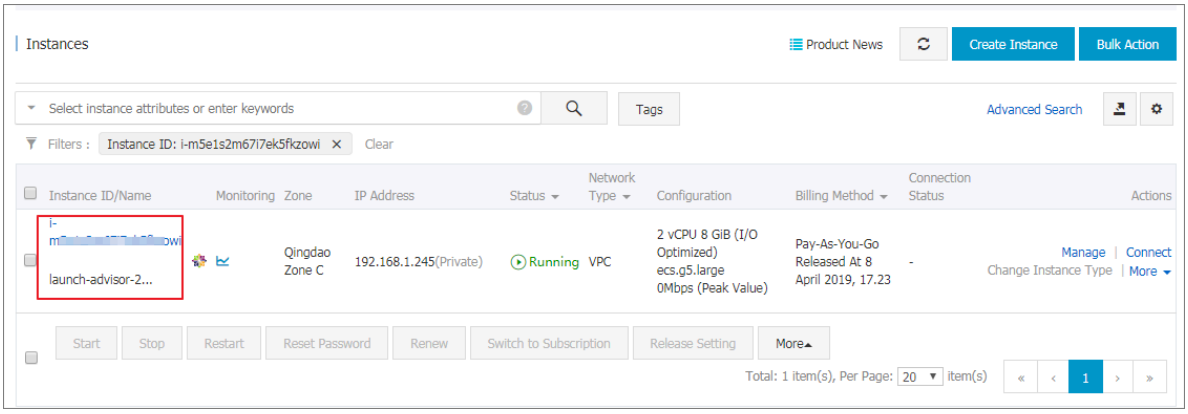
4. Configure the ECS instance and click Buy Now.

   For network configurations, the following are used in this tutorial:

   - Network: Select the created VPC and VSwitch.
   - Assign Public IP: Do not select.
   - Select Security Group: Select to use the default security group. For more information, see Default security group rules.



5. Go back to the ECS console to view the created ECS instance.



Step 3: Create and attach an EIP

An Elastic IP address (EIP) is a public IP address resource that you can purchase and use independently.

To create an EIP, follow these steps:

1. In the left-side navigation pane, click Elastic IP addresses.

2. Select the region of the EIP and click Create EIP. In this tutorial, select China (Qingdao).
3. Configure the EIP, and click Buy Now.

   For more information, see Pay-As-You-Go.
4. Find the created EIP and click Bind.
5. In the displayed dialog box, select ECS Instance as the Instance Type, select the created ECS instance and then click OK

\

Step 4: Test the Internet access

After the ECS instance is associated with an EIP, it can communicate with the Internet. You can use the associated EIP address to initiate a remote access to the ECS instance.

Note:
Make sure the security group rules of the ECS instance allow remote access. For more information, see Typical applications of commonly used ports.