ALIBABA CLOUD

Alibaba Cloud

Virtual Private Cloud

Quick Start

Document Version: 20201126

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.Plan and design a VPC

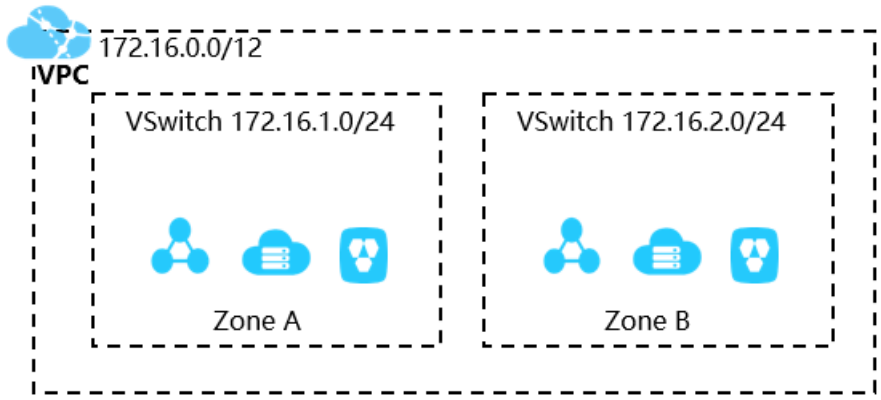
Before you create virtual private clouds (VPCs) and VSwitches, you need to plan the quantity and Classless Inter-domain Routing (CIDR) blocks of VPCs and VSwitches.

- How many VPCs are required?
- How many VSwitches are required?
- How do I specify CIDR blocks?
- How do I specify CIDR blocks if I want to connect a VPC to other VPCs or on-premises data centers?

How many VPCs are required?

- One VPC

  We recommend that you create one VPC if you do not need to deploy systems in multiple regions or separate VPCs.

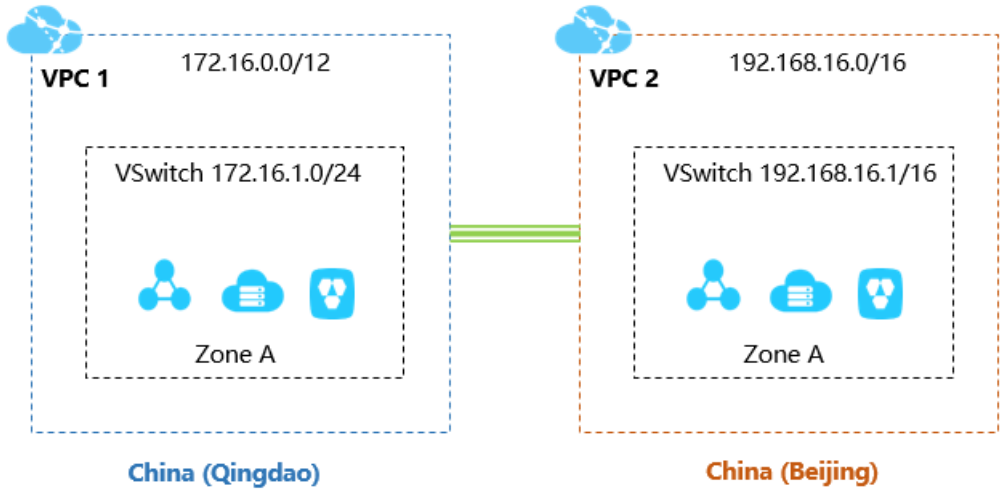


- Multiple VPCs

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

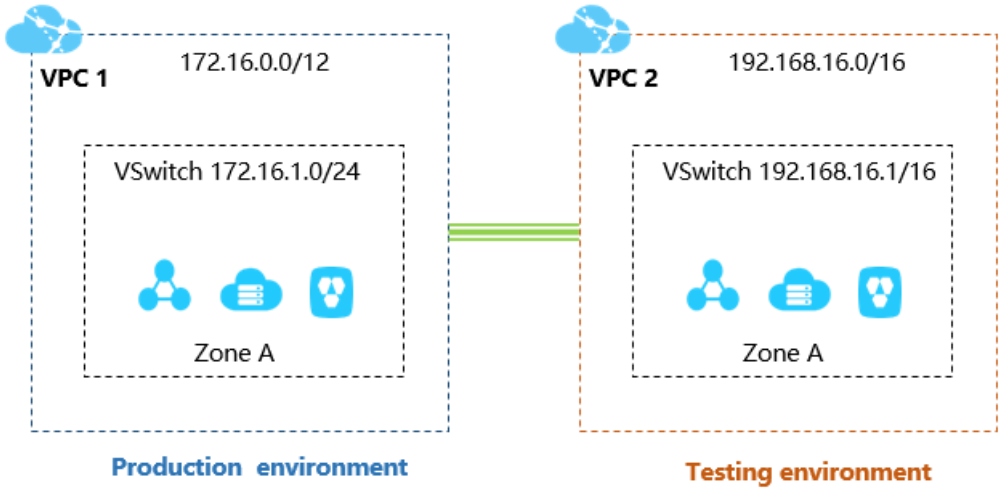
- Deploy application systems across regions.

  A VPC cannot be deployed across regions. If you want to deploy your application systems in different regions, you must create multiple VPCs. You can use Cloud Enterprise Network (CEN), Express Connect and VPN Gateway to connect VPCs.



- Separate IT systems

  To separate IT systems, you must create multiple VPCs. The following figure shows an example of isolating a production environment from a test environment by deploying them in separate VPCs.



How many VSwitches are required?

We recommend that you create at least two VSwitches for each VPC and deploy these VSwitches in different zones to achieve zone-disaster recovery.

After you deploy your applications in different zones within a region, you must measure the network latency between these applications. This is because the cross-zone network latency may be higher than expected due to complex data processing or cross-zone calls. An ideal approach is to optimize and adjust your systems to strike a balance between availability and latency.

In addition, the sizes and designs of your IT systems must also be taken into consideration when you create VSwitches. If you allow traffic from the Internet to be routed to and from the frontend systems, you can deploy the front-end systems in different VSwitches and the backend systems in other VSwitches to create a robust disaster recovery strategy.

How do I specify CIDR blocks?

When you create VPCs and VSwitches, you must specify their private IP address ranges in the form of CIDR blocks.

- VPC CIDR blocks

  You can use 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8, or their subsets as the CIDR blocks of your VPCs. To specify CIDR blocks for VPCs, follow these rules:

  - If you have only one VPC and this VPC does not need to communicate with any on-premises data center, you can use one of the preceding CIDR blocks or one of their subsets as the CIDR block of the VPC.
  - If you have multiple VPCs, or you need to build a hybrid cloud to integrate VPCs and on-premises data centers, we recommend that you use the subsets of the preceding CIDR blocks for your VPCs. In this case, the mask cannot be longer than 16 bits.
  - You must check whether a classic network is used before you specify the CIDR block for your VPC. If you plan to connect Elastic Compute Service (ECS) instances in a classic network to your VPC, we recommend that you do not use 10.0.0.0/8 as the CIDR block for your VPC, since 10.0.0.0/8 is the IP range of classic networks.

- VSwitch CIDR blocks

  The CIDR block of a VSwitch must be a subset of the CIDR block of the VPC this VSwitch resides in. For example, if the CIDR block of a VPC is 192.168.0.0/16, the CIDR block of a VSwitch in the VPC must be a segment from 192.168.0.0/17 to 192.168.0.0/29.

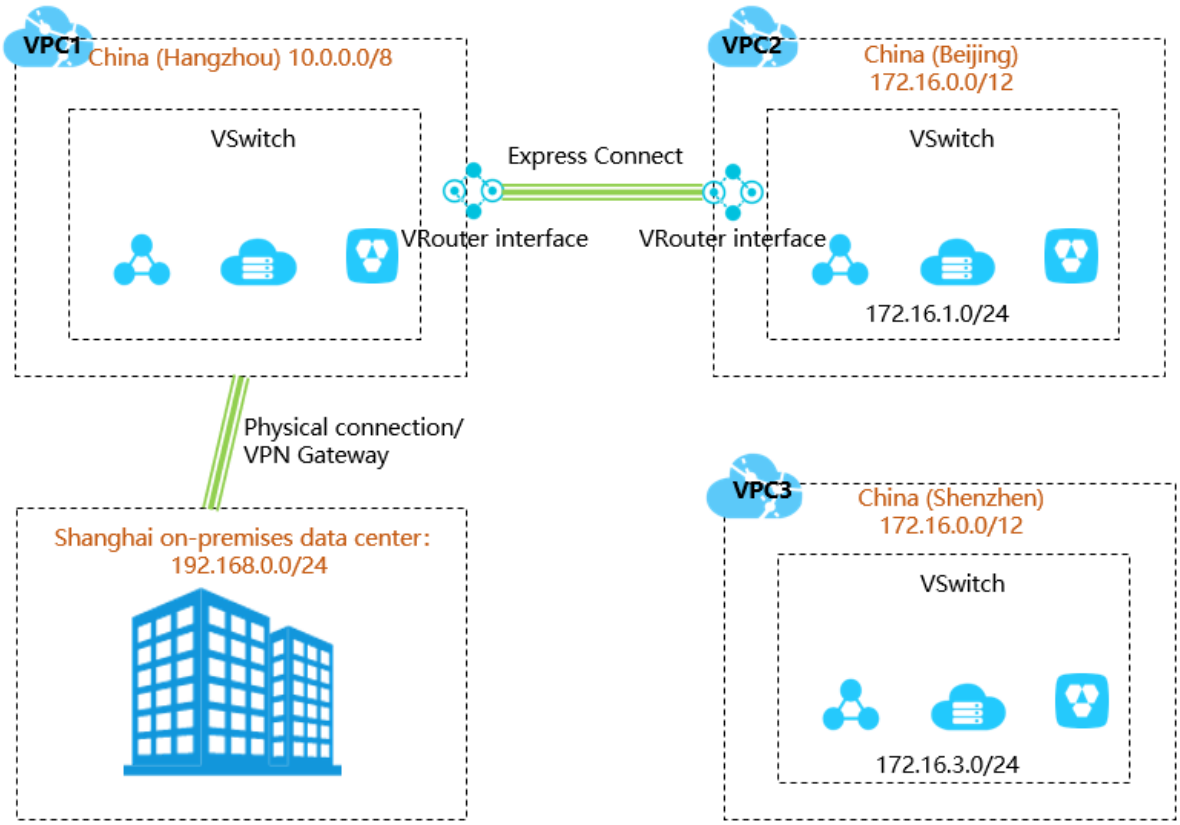
  To specify CIDR blocks for VSwitches, follow these rules:

  - The CIDR block size for a VSwitch is between a 16-bit mask and a 29-bit mask. It means that 8 to 65,536 IP addresses can be provided. This range is set because a 16-bit host address space provides addressing for 65,534 ECS instances, which can meet your needs in most cases, while a mask smaller than 29 bits can only allow very few usable host addresses.
  - The first and the last three IP addresses in each VSwitch CIDR block 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 ECS instances in classic networks can communicate with the ECS instances in VPCs by using ClassicLink. However, the CIDR block of each VPC must be 192.168.0.0/16, 10.0.0.0/8, or 172.16.0.0/12. For example, if you want to connect an ECS instance in a VSwitch of a VPC to an ECS instance in a classic network, and the IP address range of the VPC is 10.0.0.0/8, the IP address range of the VSwitch must be 10.111.0.0/16. For more information, see Overview.
  - You must check the number of ECS instances in the VSwitch before you specify the CIDR block of a VSwitch.

How do I specify CIDR blocks if I want to connect a VPC to other VPCs or on-premises data centers?

Before you connect your VPC to another VPC or an on-premises data center, you must make sure that the CIDR block of your VPC does not conflict with that of the peer network.

For example, assume you have three VPCs: VPC1 in China (Hangzhou), VPC2 in China (Beijing), and VPC3 in China (Shenzhen), as shown in the following figure. Express Connect circuit is used for VPC1 and VPC2 to communicate with each other. VPC3 does not communicate with other VPCs, but may need to communicate with VPC2 in the future. Additionally, you have an on-premises data center in Shanghai, and you need to connect it to VPC1 by using an Express Connect circuit.



In this example, the CIDR block of VPC2 is different from the CIDR block of VPC1, but is the same with the CIDR block of VPC3. However, considering that VPC2 and VPC3 may need to communicate with each other later in the private network, the VSwitches in these VPCs are assigned with different CIDR blocks. This example demonstrates that VPCs communicating with each other can have identical CIDR blocks, but their VSwitches must have different CIDR blocks.

When you specify CIDR blocks for multiple VPCs that need to communicate with each other, follow these rules:

- The preferred practice is to specify different CIDR blocks for different VPCs. You can use the subsets of the standard CIDR blocks to increase the number of available CIDR blocks.
- If you cannot assign different CIDR blocks for VPCs, try to specify different CIDR blocks for the VSwitches in these VPCs.
- If you cannot assign different CIDR blocks for all VSwitches in these VPCs, make sure that different CIDR blocks are configured for the VSwitches communicating with each other.

2.Create an IPv4 VPC network

This topic describes how to create a Virtual Private Cloud (VPC) network with an IPv4 CIDR block. After you create a VPC network, you can create Elastic Compute Service (ECS) instances in the VPC network, and associate elastic IP addresses (EIPs) with the ECS instances to enable the ECS instances to access the Internet.

Prerequisites

To deploy cloud resources in a VPC network, you must first set up network connections. For more information, see Plan and design a VPC.

Step 1: Create a VPC network and a VSwitch

To create a VPC network and a VSwitch, perform the following steps:

1. Log on to the VPC console.
2. In the top navigation bar, select the region where you want to deploy the VPC network.

   The VPC network and the cloud resources that you want to deploy must be created in the same region. **China (Qingdao)** is selected in this topic.
3. On the **VPCs** page, click **Create VPC**.
4. In the **Create VPC** dialog box, set the following parameters of the VPC network and the VSwitch, and click **OK**.

Parameter	Description
VPC	
Region	The region where the VPC is deployed.
Name	Enter a name for the VPC that you want to create. The name must be 2 to 128 characters in length and can contain letters, digits, underscores (_), and hyphens (-). It must start with a letter.
IPv4 CIDR Block	Select the primary IPv4 CIDR block for the VPC. Valid values: ○ **Recommended CIDR Block**: Enter 192.168.0.0/16, 172.16.0.0/12, or 10.0.0.0/8. ○ **Custom CIDR Block**: Enter 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8, or a subset of these CIDR blocks as the primary IPv4 CIDR block of the VPC. The subnet mask must be 8 to 24 bits in length. Example: 192.168.0.0/16. To use a public CIDR block as the primary CIDR block of the VPC,submit a ticket. **Note** After you create a VPC, you cannot change its primary IPv4 CIDR block. However, you can add a secondary IPv4 CIDR block to the VPC. For more information, see Add a secondary IPv4 CIDR block.

Parameter	Description
Description	The description of the VPC. The description must be 2 to 256 characters in length and cannot start with `http://` or `https://`.
VSwitch	
Name	Enter a name for the VSwitch. The name must be 2 to 128 characters in length, and can contain digits, underscores (_), and hyphens (-). It must start with a letter.
Zone	Select a zone for the VSwitch. In a VPC, VSwitches in different zones can communicate with each other.
Zone Resource	Displays the cloud instances that can be created in the specified zone. The supported cloud resources vary based on the zone and the time when you create cloud resources. The buy page displays whether the cloud instances are available. Only Elastic Compute Service (ECS), Relational Database Service (RDS), and Server Load Balancer (SLB) instances can be queried on the buy page.
IPv4 CIDR Block	Specify an IPv4 CIDR block for the VSwitch. Note the following limits when you specify an IPv4 CIDR block: ○ The CIDR block of a VSwitch must be a subset of the CIDR block of the VPC to which the VSwitch belongs. For example, if the CIDR block of the VPC is 192.168.0.0/16, the CIDR block of the VSwitch in the VPC can be one CIDR block from 192.168.0.0/17 to 192.168.0.0/29. ○ The first and last three IP addresses in the VSwitch CIDR block are reserved. For example, if the VSwitch CIDR block 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. ○ If a VSwitch needs to communicate with the VSwitches in other VPCs or on-premises networks, make sure that the related CIDR blocks do not conflict with each other. **Note** After you create a VSwitch, you cannot modify the CIDR block.
Number of Available Private IPs	Displays the number of available IP addresses.

Parameter	Description
Description	Enter a description for the VSwitch. The description must be 2 to 256 characters in length and cannot start with `http://` or `https://`.

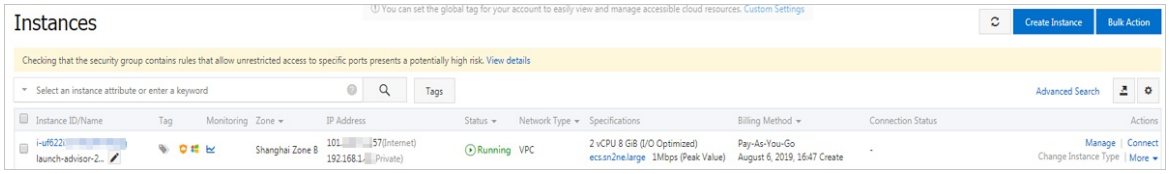
Step 2: Create an ECS instance

To create an ECS instance in the created VPC network, perform the following steps:

1. Log on to the VPC console.
2. In the left-side navigation pane, click **VSwitches**.
3. In the top navigation bar, select the region where the VSwitch is deployed. **China (Qingdao)** is selected in this topic.
4. On the **VSwitches** page, find the target VSwitch, and choose **Create > ECS Instance** in the **Actions** column.
5. On the **Custom Launch** tab, set the following parameters of the ECS instance.

   For more information about how to configure an ECS instance, see Create an instance by using the provided wizard.

   - **Network Type**: Select the VPC network and VSwitch that you have created.
   - **Public IP Address**: Clear the check box.
   - **Security Group**: Use the default security group.
6. Click **Create Order** and complete the payment.
7. Log on to the ECS console. In the left-side navigation pane, click **Instances**. On the **Instances** page, view details of the created ECS instance.



Step 3: Create an EIP and associate it with the ECS instance

An EIP is a public IP address resource that can be purchased and held as an independent resource. You can associate EIPs with ECS instances in a VPC network to enable the ECS instances to access the Internet.

To create an EIP and associate it with the ECS instance, perform the following steps:

1. Log on to the VPC console.
2. In the left-side navigation pane, choose **Elastic IP Addresses > Elastic IP Addresses**.
3. On the **Elastic IP Addresses** page, click **Create EIP**.
4. On the **Elastic IP** page, set the parameters of the EIP, click **Buy Now**, and complete the payment.For more information, see Apply for new EIPs.
5. On the **Elastic IP Addresses** page, find the target EIP, and click **Bind Resource** in the **Actions** column.

6. In the **Bind Elastic IP Address to Resources** dialog box, set the following parameters and click **OK**.
   - **Instance Type**: Select **ECS Instance** from the drop-down list.
   - **Binding mode**: Select a mode in which the EIP is associated with the ECS instance.

     Only Normal is supported.
   - **Select an instance to bind**: Select the ECS instance to be associated.

Step 4: Test the network connectivity

To test the network connectivity of the ECS instance, perform the following steps:

1. Log on to the ECS instance that is associated with the EIP.
2. Run the `ping` command to test the network connectivity between the ECS instance and the Internet.The test result indicates that the ECS instance can access the Internet.