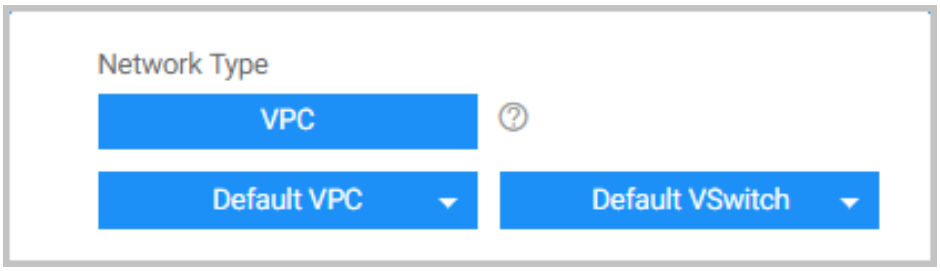
Virtual Private Cloud

User Guide

User Guide

Alibaba Cloud provides a default VPC and VSwitch for you in the situation that you do not have any existing VPC and VSwitch to use when creating a cloud product instance. A default VPC and VSwitch will be created along with the creation of the instance.



Default VPC and VSwitch feature list

Default VPC	Default VSwitch
The default VPC in each region is unique.	The default VSwitch in each Availability Zone is unique.
The netmask for a default VPC is /16 such as 172.31.0.0/16, which provides up to 65536 private IP addresses.	The netmask for a default VSwitch is /20 such as 172.31.0.0/20, which provides up to 4096 private IP addresses.
The default VPC does not occupy the VPC quota that the Alibaba Cloud allocates to you.	The default VSwitch does not occupy the VSwitch quota that the Alibaba Cloud allocates to you.
The default VPC is created by the system, all the VPCs created by you are non-default VPCs.	The default VSwitch is created by the system, all the VSwitches created by you are non-default VSwitches.
The operations and restrictions for default and non-default VPCs are the same.	The operations and restrictions for default and non-default VSwitches are the same.

Build VPC

Prerequisite

Before creating a VPC, refer to Plan and design VPC network to design your private network.

Procedure

Log on to the VPC console.

In the left navigation bar, click **VPC**.

Choose the region where the VPC is located.

Click **Create VPC** in the upper-right corner.

In the pop-up dialog, provide the following information:

Configuration	Description
VPC Name	Enter the name of the VPC.
Description (optional)	Add a description for the VPC.
CIDR block	Specify the IP address range for the VPC in the form of a Classless Inter-Domain Routing (CIDR) block. Note the following when selecting a CIDR block: - Use the standard private CIDR blocks (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/1) or their subsets as the IP address ranges. Note: If you want to use the subset of the provided CIDR blocks as the IP address range, use the Open API to create a VPC. For details, refer to Create a VPC. - If you have multiple VPCs, or you want to build a hybrid cloud consisting of multiple VPCs and on-premises IDCs, we recommend that you use the subset of the provided CIDR blocks, and ensure that the network mask is no larger than /16. - If you just have one VPC and the VPC does not need to communicate with the on-premises data center, you can

	use any of the provided CIDR blocks. - You also need to consider the use of the classic network. If you plan to connect the cloud product instances in the classic network with a VPC, we recommend that you do not use the CIDR block 10.0.0.0/8, which is also used as CIDR block by the classic network. - **Note**: If you have special requirements on the IP address range, submit a ticket or contact your customer manager.

Click **Create VPC**.

Related operations

Create a VSwitch

A VSwitch is a basic network device in a VPC network, which is used to connect the cloud product instances in the VPC. You can further segment your virtual networks into subnets by adding VSwitches. For more details, see Create a VSwitch.

Delete a VPC

On the VPC list page, locate the target VPC and click **Delete**.

> **Note**: Before you delete the VPC, make sure you have released or transferred all the instances in the VSwitches of the VPC and the VSwitches have been deleted.

Modify the name of a VPC

On the VPC list page, hover the mouse pointer to the ID of the target VPC. A pencil icon appears. Click the pencil icon to modify the name of VPC.

Reference API

Create a VPC

Delete a VPC

Check the VPC list

Modify the VPC attribute

Prerequisite

Create a VPC.

Procedure

Log on to the VPC console.

In the left navigation bar, click **VPC**.

Click the region of the VPC where the VSwitch to be created is located.

Click the ID of the target VPC.

Then you are directed to the **VPC Details** page.

Click **VSwitch** and then click **Create VSwitch**.

In the **Create VSwitch** dialog, provide the following information:

Configuration	Description
VPC	The ID of the VPC where the VSwitch is located.
VPC CIDR block	The CIDR block of the VPC. Click **Display Binary** to view the CIDR block in binary format.
Name	Enter the name of the VSwitch.
Zone	Select a zone of the VSwitch. Zones are physical areas with independent power grids and networks

	in one region. Zones in the same region are intranet connected. We recommend creating different VSwitches in different zones to achieve disaster recovery.
CIDR block	Specify the IP address of the VSwitch in the form of a Classless Inter-Domain Routing (CIDR) block. Note the following when specifying a VSwtich CIDR block: - The allowed block size for a VSwitch is between a /16 netmask and /29 netmask, which can provide 8 to 65,536 IP addresses. - The CIDR block of the VSwitch can be the same as that of the VPC that it belongs to, or the subset of the VPC CIDR block. **Note**: If the CIDR block of the VSwitch is the same as that of the VPC, you can only create one VSwitch. - The first and the last three IP addresses are reserved by the system. Take the CIDR block 192.168.1.0/24 as an example, the IP addresses 192.168.1.0, 192.168.1.253, 192.168.1.254 and 192.168.1.255 are reserved by the system. - You also need to consider the number of the cloud product instances running in the VSwitch.
Number of Available Private IPs	The number of available IP addresses in the VSwitch.
Description (optional)	Add a description for the VSwitch.

7. Click **OK**.

Related operations

Create cloud product instances in a VPC

On the **VSwitch List** page, click **Create an Instance** to create an ECS, SLB or RDS instance. For more details, refer to Create cloud service instance in a VPC.

Modify a VSwtich

On the **VSwitch List** page, find the target VSwitch and then click **Edit**. Or hover your mouse pointer over the VSwitch name to change the name of the VSwitch.

Delete a VSwitch

On the **VSwitch List** page, find the target VSwitch and then click **Delete**.

Note: Before deleting a VSwitch, ensure that you have released or transferred all the cloud product instances under it.

Reference API

Create a VSwitch

Delete a VSwitch

Check the VSwitch list

Modify the VSwitch attribute

Route table basics

A VRouter is a hub in a VPC that connects all VSwitches in the VPC and also serves as a gateway device that connects the VPC with other networks.

A VRouter and a route table are automatically created after you create a VPC. Each entry in the route table is a ***route entry***, which defines the next hop of the network traffic destined for a specific destination CIDR block. The network traffic is routed based on the configurations of the route entries in the route table.

> **Note**: You cannot create or delete a VRouter or a route table directly. They will be deleted automatically along with the deletion of the VPC. But you can add route entries to the route table to route network traffic.

There are two types of route entries:

System route entry

A system route entry is created by the system and cannot be deleted.

After you create a VPC, a system route entry will be automatically created.

The destination CIDR block of this system route entry is 100.64.0.0/10, which is used for the communication within the VPC.

After you create a VSwitch, a system route entry will be automatically created.

The destination CIDR block of this system route entry is the CIDR block of the VSwitch, which controls the routing for the VSwitch.

Custom route entry

You can create or delete custom route entries, and you can create up to 40 custom route entries in a route table.

> **Note**: In general, system route entries can meet your needs. But in some particular cases, you still need to add custom route entries. Before adding custom route entries, ensure that you have completed your network plan.

Routing policy

The longest prefix match algorithm is used to route the network traffic when more than one route entries match the destination IP address. That is, the route entry with the longest netmask (the most specific route) is used to determine the next hop.

Here is an example of a route table.

Destination CIDR block	Next Hop Type	Next Hop	Type
100.64.0.0/10			System
192.168.0.0/24			System
0.0.0.0/0	Instance	i-12345678	Custom
10.0.0.0/24	Instance	i-87654321	Custom

In this example, route entries with the destination CIDR blocks100.64.0.0/10 and 192.168.0.0/24 are

the system route entries. Route entries with the destination CIDR blocks0.0.0.0/0 and 10.0.0.0/24 are custom route entries.

All traffic destined for 0.0.0.0/0 is routed to the ECS instance with the IDi-12345678 and all traffic destined for 10.0.0.0/24 is routed to the ECS instance with the IDi-87654321.

According to the longest prefix match algorithm, the traffic destined for 10.0.0.1 is routed to ECS instance with the IDi-87654321, while the traffic destined for 10.0.1.1 is routed to the ECS instance with the IDi-12345678.

Scenarios of adding custom router entries

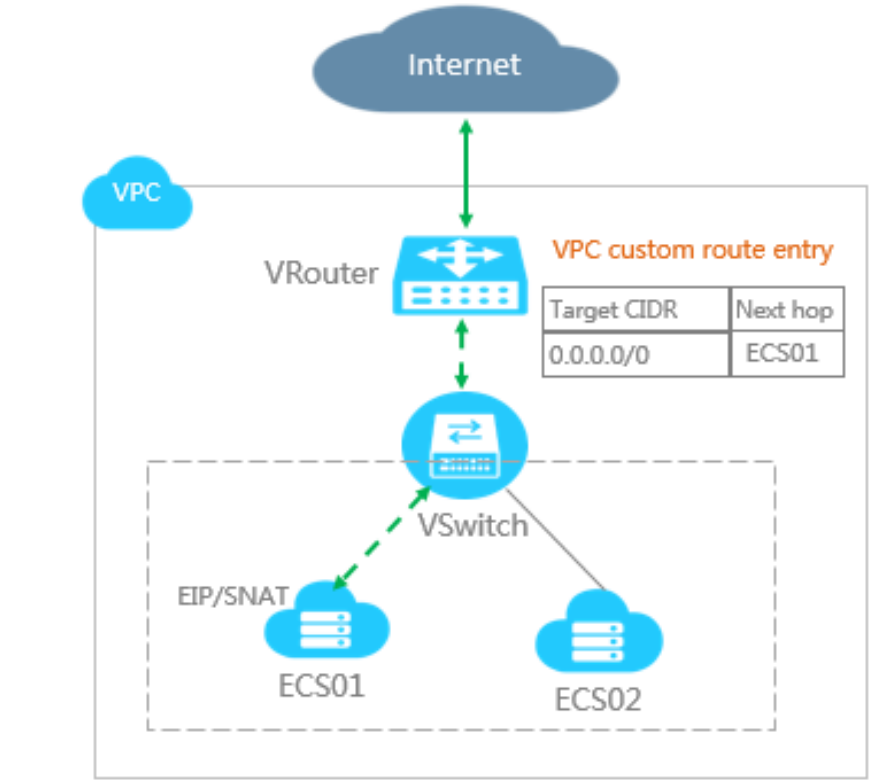
The custom route entries are needed in the following scenarios.

Traffic routing within a VPC

Assume that you have two ECS instances in your VPC: ECS01 and ECS02.

ECS01 is bounded with an Elastic IP (EIP) so that this ECS instance can communicate with the Internet. If you want ECS02 to communicate with the Internet without binding another EIP, you can add a custom route entry as follows.

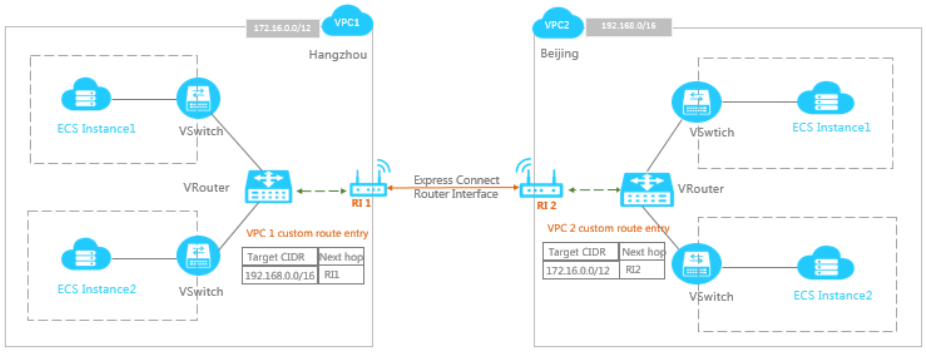
Destination CIDR	Next hop type	Next hop
0.0.0.0/0	ECS instance	ECS01



Interconnection between VPCs

Assume that you have two VPCs. VPC1 uses the CIDR block 172.16.0.0/12 and VPC2 uses the CIDR block 192.168.0.0/16.

By using the router interface function of the Express Connect product, you can create a connection between these two VPCs. Firstly, you need to create a router interface, and set VPC1 as the initiator and VPC2 as the receiver. Then, you need to add two custom route entries as follows.



- Custom route entry added in VPC1

Destination CIDR	Next hop type	Next hop

192.168.0.0/16	Route interface	RI1

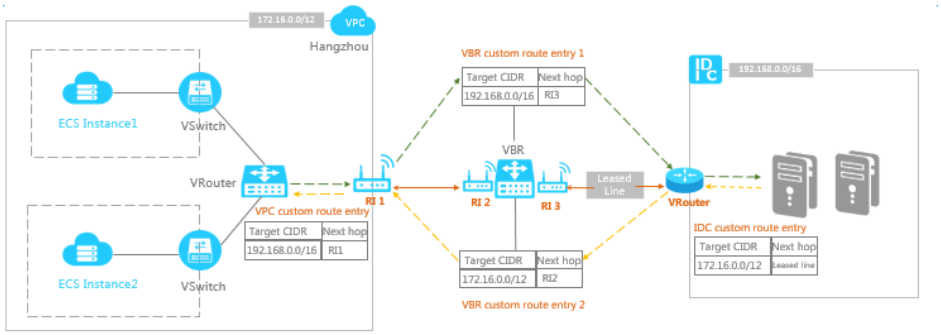
- Custom route entry added in VPC2

Destination CIDR	Next hop type	Next hop
172.16.0.0/12	Route interface	RI2

Interconnection between VPC and on-premises IDC

Assume that you have a VPC with the CIDR block 172.16.0.0/12, and an on-premises IDC with the CIDR block 192.168.0.0/16.

By using the physical connection (leased line) function of the Express Connect product, you can create a connection between the VPC and the IDC. Firstly, you need to create a Virtual Border Router (VBR) to connect the IDC with the VBR. Then, you need to create a router interface to connect the VBR with the VPC. Lastly, you need to add the following custom router entries:



- Custom route entry added in VPC

Destination CIDR block	Next hop type	Next hop
192.168.0.0/16	Route interface	RI1

- Custom route entry added in VBR

Destination CIDR	Next hop type	Next hop
192.168.0.0/16	Leased line	RI3
172.16.0.0/12	VPC	RI2

- Custom route entry added in IDC

Destination CIDR	Next hop type	Next hop

172.16.0.0/12	—	RI4

Add custom route entries

Log on to the VPC console.

In the left-side navigation pane, click **VPC**.

Choose the region where the VPC is created.

Click the ID of the target VPC.

In the left-side **VPC Details** pane, click **VRouter**, and then click **Add Route Entry**.

In the **Add Route Entry** dialog, provide the following information and click **OK**.

Configuration	Description
Destination CIDR Block	Enter the destination CIDR block. If you enter an IP address, the network mask /32 is used by default.
Next hop type	Choose a type of the next hop. - ECS instance: routes the traffic destined for the destination CIDR to an ECS instance. - Router interface: routes the traffic destined for the destination CIDR to a router interface. Then the router interface will route the traffic to its peer router interface.
Next hop	The next hop that receives the routed traffic. **Note**: If you select ECMP-Routing, you must add at least two router interfaces, and the corresponding peer router interface must be a Virtual Boarder Interface (VBR).

Instance management in VPC

Overview

You can directly create a cloud product instance such as ECS, SLB and RDS under a specific VSwitch in the VPC console.

Prerequisite

Ensure that you have created a VPC and VSwitch.

Procedure

Log on to the VPC console.

In the left-side navigation pane, click **VPC**.

Click a region and then click the ID of the VPC where the VSwitch is created.

On the **VPC Details** navigation pane, click **VSwitch**.

Click the **Create an Instance** option of the target VSwitch, and then click the instance that you want to create.

Complete the instance configuration on the corresponding purchase page. After the purchase is completed, an instance is created under this target VSwitch.

After creating a VPC ECS instance, you can change the private IP address and also can change the VSwitch of the ECS instance.

Procedure

Log on to the ECS console.

On the left-side navigation pane, click **Instances**.

Click a region and then click the ID of the target ECS instance.

On the **Instance Details** page, click **Stop** on the upper-right corner.

In the **Configuration Information** panel, click **More** > **Modify Private IP Address**.

In **Modify Private IP Address** dialog, modify the private IP by either of the following ways, and then click **Modify**.

VSwitch: Select a new VSwitch for the ECS instance from the list.

Because each VSwitch in a VPC has a unique CIDR block, the ECS instance's private IP address will be automatically changed along with the change of the VSwitch.

Private IP Address: Enter the new IP address if you do not want to change the VSwitch of the ECS instance.

Restart the ECS instance.

You can migrate an RDS instance from one VPC to another VPC. Firstly, you have to switch the network type of the RDS instance to the classic network, and then switch it to the VPC.

Note:

The VPC switch will cause an ephemeral disconnection for the RDS instance. Ensure that you have set an automatic reconnection mechanism for it.

Procedure

Log on to the RDS console.

Switch the network type to the classic network:

Click the ID of the target RDS instance.

On the left-side navigation pane, click **Database Connection**.

In the **Connection information** section, click **Switch to Classic**.

Click **OK** in the pop-up dialog.

Switch the network type to VPC:

Click **Refresh** to check the database status.

After the network type is changed to the classic network, click **Switch to VPC**.

In the pop-up dialog, select a new VPC and VSwitch for the RDS instance and then click **OK**.

Connections from VPC to Internet

If a VPC ECS instance needs to access the Internet, you can choose to allocate a public IP for it when creating the ECS instance.

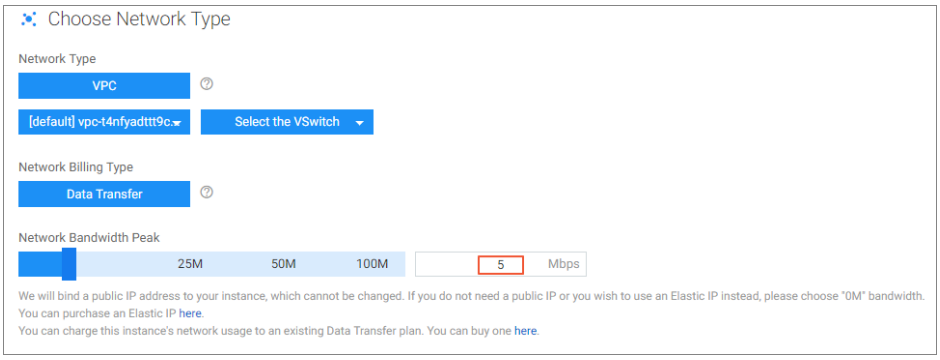
As shown in the following figure, after you have chosen the VPC and VSwitch where the ECS instance is created, you have to set a network bandwidth peak. The value must be larger than 0 so that a public IP will be allocated to the ECS instance after it is created.

Note:

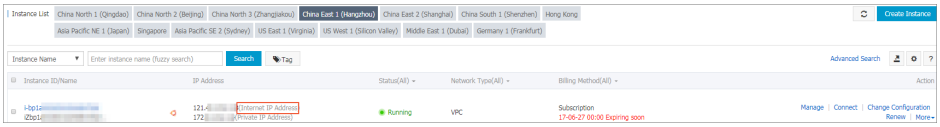
Only when the specified network bandwidth peak is larger than 0, a public IP will be allocated. Otherwise, no public IP is allocated. In this situation, you can bind an Elastic IP to the ECS instance as an alternative.

You cannot unbind the system allocated IP from the ECS instance.

For more details on creating an ECS instance, refer to Create an instance running Linux or Create an instance running Windows.



After the ECS instance is created, you can view the public IP on the **Instance List** page. You can use this public IP to access the ECS instance in the public network.



If the ECS instance does not have a system allocated public IP, you can bind an EIP to the ECS instance to access the Internet.

Elastic IP (EIP) is a public IP address resource that you can purchase and possess independently. It can be dynamically bound to a VPC ECS instance without restarting the ECS instance. For more details, refer to EIP overview.

Procedure

Log on to EIP console.

Click **Apply for Elastic IP**.

On the purchase page, configure the EIP and then click **Buy Now**.

Go back to the EIP console after completing the purchase, and click **Bind** next to the target EIP.

In the **Bind** dialog, select the ECS instance to be bound and then click **OK**.

> **Note**: Ensure the ECS instance is in the Running or Stopped status, and the ECS instance does not have a system allocated public IP or bound with any other EIPs.

After binding an EIP, the ECS instance can access the Internet through the EIP. You can unbind and release the EIP whenever the Internet access is not needed. For details, refer to Manage an EIP.

Access from Internet to VPC

If the ECS instance in a VPC needs to provide external services, you can choose to allocate a public IP for it when creating the ECS instance.

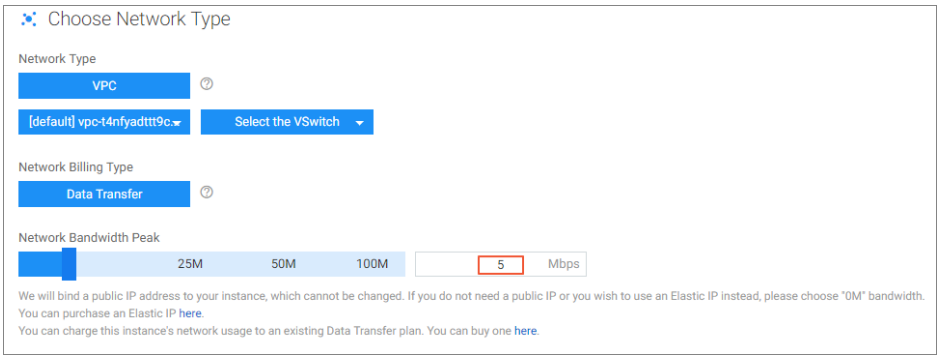
As shown in the following figure, after you have chosen the VPC and VSwitch where the ECS instance is created, you have to set a network bandwidth peak. The value must be larger than 0 so that a public IP will be allocated to the ECS instance after it is created.

Note:

Only when the specified network bandwidth peak is larger than 0, a public IP will be allocated. Otherwise, no public IP is allocated. In this situation, you can bind an Elastic IP to the ECS instance as an alternative.

You cannot unbind the system allocated IP from the ECS instance.

For more details on creating an ECS instance, refer to Create an instance running Linux or Create an instance running Windows.



After the ECS instance is created, you can view the public IP on the **Instance List** page. You can resolve this public IP to a domain name to provide external services.

If the ECS instance does not have a system allocated public IP, you can bind an EIP to the ECS instance to provide external services.

Elastic IP (EIP) is a public IP address resource that you can purchase and possess independently. It can be dynamically bound to a VPC ECS instance without restarting the ECS instance. For more details, refer to EIP overview.

Procedure

Log on to EIP console.

Click **Apply for Elastic IP**.

On the purchase page, configure the EIP and then click **Buy Now**.

Go back to the EIP console after completing the purchase, and click **Bind** next to the target EIP.

In the **Bind** dialog, select the ECS instance to be bound and then click **OK**.

> **Note**: Ensure the ECS instance is in the Running or Stopped status, and the ECS instance does not have a system allocated public IP or bound with any other EIPs.

After binding an EIP, the ECS instance can access the Internet through the EIP. You can unbind and release the EIP whenever there is no need to provide external services. For details, refer to Manage an EIP.

Server Load Balancer (SLB) is a traffic distribution control service that distributes traffic based on the forwarding rules and scheduling algorithms to multiple backend servers.

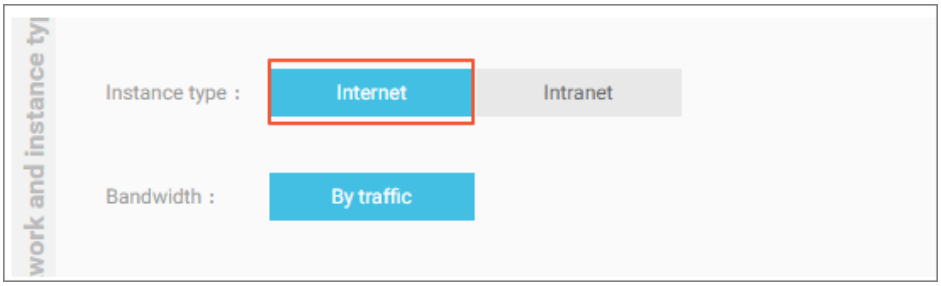
You can create an Internet-facing SLB instance, and add VPC ECS instances as the backend servers to process the distributed requests from the Internet. In this way, the VPC ECS instances can provide external services.

> Two ECS instances with Apache static web pages deployed are used in this tutorial.

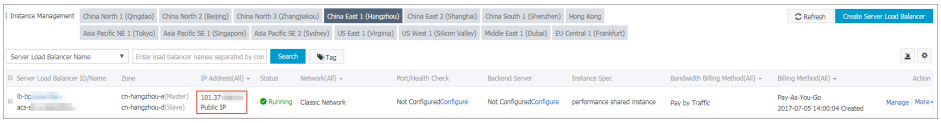
Procedure

Log on to the Server Load Balancer console and click **Create Server Load Balancer** to create an Internet-facing SLB instance.

Note: Ensure that the selected instance type is **Internet**.



A public IP address is allocated to the SLB instance after it is created. You can use this IP address to provide external services.



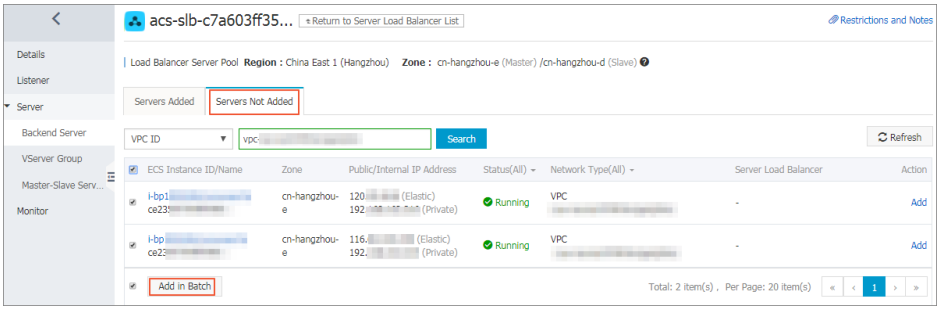
Add backend servers.

Click the ID of the created SLB instance.

In the left-side **Details** pane, click **Server** > **Backend Server**.

Click the **Servers Not Added** tab.

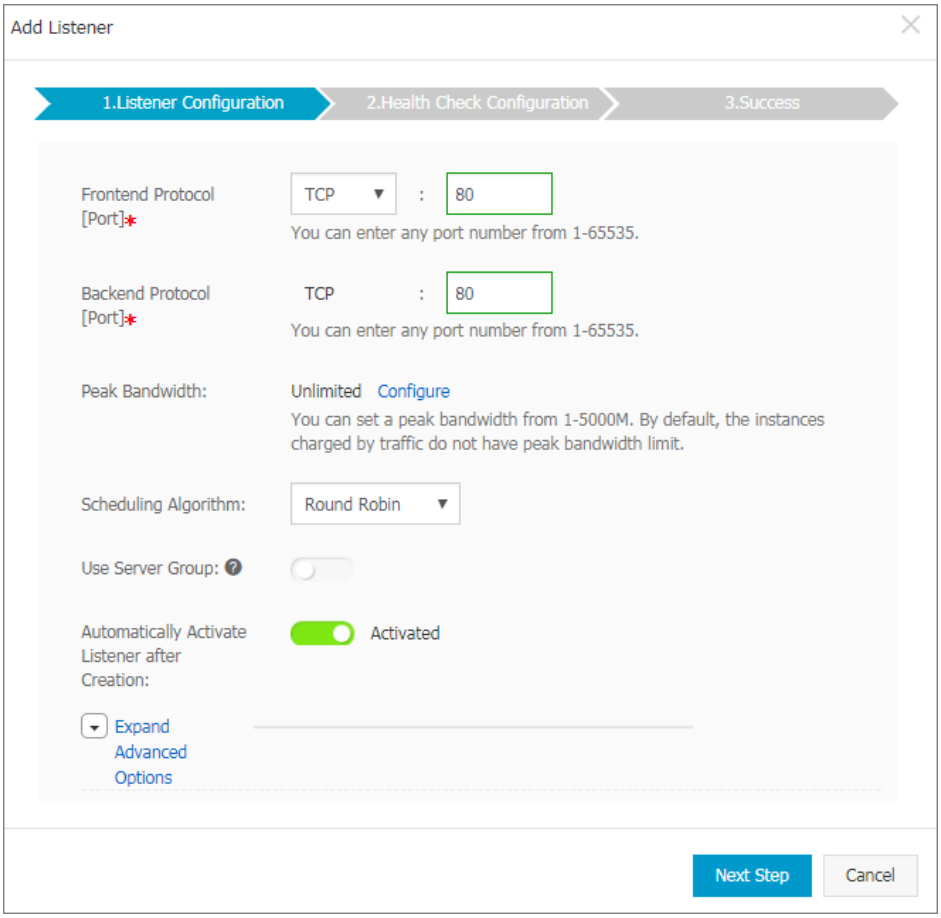
Select the checkboxes next to the VPC ECS instances and then click **Add in Batch**. In the pop-up dialog, set the weight to 100 and click **Confirm** to add.



Add a listener.

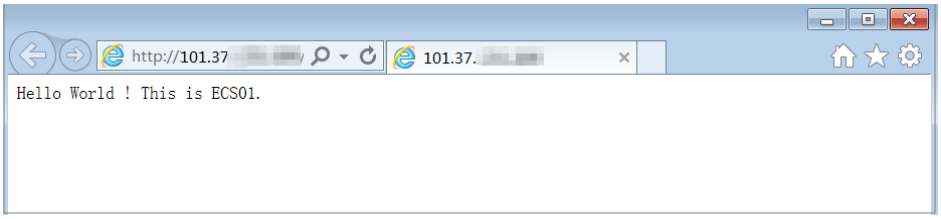
In the left-side **Details** pane, click **Listener**, and then click **Add Listener**.

In the **Add Listener** dialog, configure a TCP listener as shown in the following figure.



Click **Next Step** to configure the health check and select **TCP** with other settings unchanged. Click **Confirm** twice to finish the configuration.

Go back to the Server Load Balancer list page and refresh the page to check the instance status. When the instance is running and the health check is normal, you can use the public IP address of the SLB instance to provide external services.

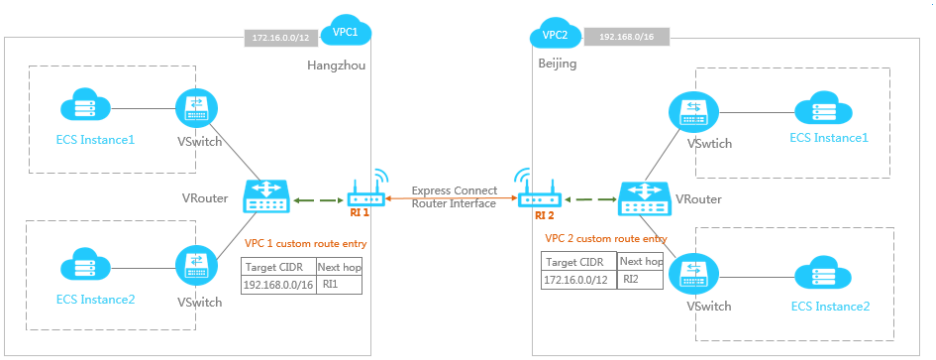


Interconnection between VPCs

Alibaba Cloud Express Connect can establish a dedicated private connection between two VPCs in any regions. The connection does not go over the Internet. This allows Express Connect to offer a fast, stable, secure and dedicated network communication.

As shown in the following figure, assume that you have two VPCs, VPC1 with the CIDR block 172.16.0.0/16, and VPC2 with the CIDR block 192.168.0.0/16.

To establish a connection between VPC1 and VPC2, you need to use the router interface function of Express Connect. Firstly, you need to create a router interface, and set VPC1 as the initiator and VPC2 as the receiver. Then, you need to add two custom route entries.



- Custom route entry added in VPC1

Destination CIDR	Next hop type	Next hop
192.168.0.0/16	Route interface	RI1

- Custom route entry added in VPC2

Destination CIDR	Next hop type	Next hop
172.16.0.0/12	Route interface	RI2

For more details, refer to:

Establish a connection between VPCs under the same account

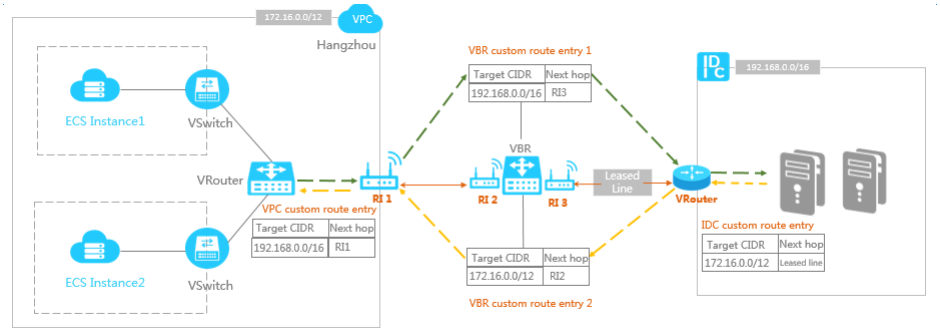
Establish a connection between VPCs under different accounts

Interconnection between VPC and On-

premises IDC

You can use the physical connection function of Express Connect to establish a connection between a VPC and an on-premises IDC.

Assume that you have a VPC with CIDR block 172.16.0.0/12, and an on-premises data center with CIDR block 192.168.0.0/16. When the cloud services needs to access the on-premises data center, you can apply for a leased line to create a connection between them.



Procedure

Apply for a leased line

A leased line is used to connect the IDC with the access point of Alibaba Cloud.

Create a virtual border router

Virtual border router (VBR) is a bridge between the IDC and the VPC for forwarding your data from your VPC to IDC.

After creating the VBR, the system will automatically establish a connection between the router interface (RI3 in the figure) and the IDC through the leased line.

Create a router interface

Create a router interface to connect the VPC and the VBR. When creating the router interface, set the router interface of the VBR as the local side, and the VPC as the peer side.

After creating the router interface, the system will automatically establish a connection between the VPC and VBR through two router interfaces (RI2 and RI3 in the figure).

Add route entries

At last, you need to add route entries to route the network traffic between the VPC and IDC.

Custom route entries added in VPC

Destination CIDR block	Next hop type	Next hop
192.168.0.0/16	Router interface	RI1

Custom route entries added in VBR

Destination CIDR block	Next hop type	Next hop
192.168.0.0/16	Leased line	RI3
172.16.0.0/12	VPC	RI2

Route in IDC

Add a route pointing to the leased line in the IDC router.

For more details, see Leased line access.