ALIBABA CLOUD

Alibaba Cloud

Elastic IP Address

Best practices

Document Version: 20211125

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.Use BGP (Multi-ISP) Pro EIPs to access web services with low latency

Compared with BGP (Multi-ISP), You can associate a BGP (Multi-ISP) Pro elastic IP address (EIP) with an Elastic Compute Service (ECS) instance. Then, users in mainland China can access web services deployed in the China (Hong Kong) region with low latency.

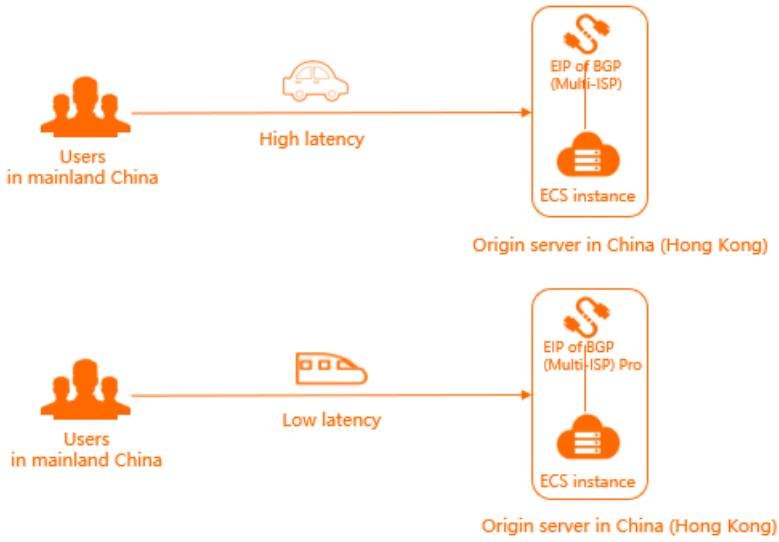
Prerequisites

A web service is deployed on an ECS instance in the China (Hong Kong) region. For more information, see Create an instance by using the wizard.

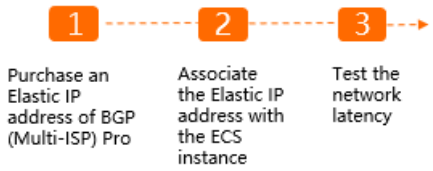
Context

The following scenario is used as an example in this topic. A web service is deployed on an ECS instance in the China (Hong Kong) region. The ECS instance is associated with a BGP (Multi-ISP) EIP. Network latency is high when users in mainland China access the web service deployed in the China (Hong Kong) region.

You can associate a BGP (Multi-ISP) Pro EIP with the ECS instance. Then, users in mainland China can access the web service deployed in the China (Hong Kong) region without using international ISP services. This reduces network latency.



Procedure



Step 1: Purchase a BGP (Multi-ISP) Pro EIP

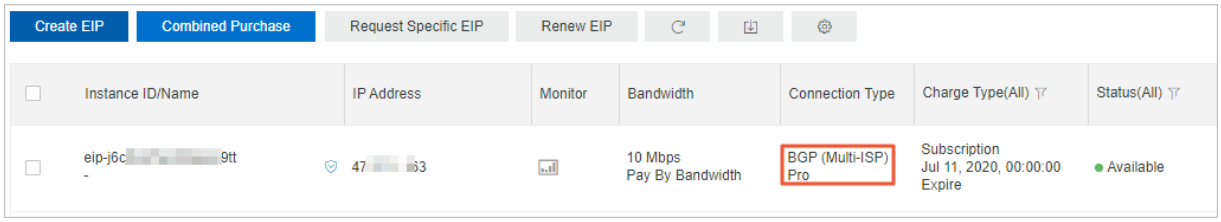
The following example describes how to purchase a BGP (Multi-ISP) Pro EIP that is billed on a subscription basis.

1. Log on to the Elastic IP Address console .
2. On the **Elastic IP Addresses** page, click **Create EIP**.
3. On the buy page, select **Subscription**, and set the following parameters.
   - **Region**: Select the region where you want to create the EIP. In this example, **China (Hong Kong)** is selected.
   - **Connection Type**: Select the line type.

     In this example, **BGP (Multi-ISP) Pro** is selected.
   - **Network Type**: Select a network type. **Internet** is selected in this example.
   - **Bandwidth value**: Select the maximum bandwidth value as needed. **10 Mbit/s** is selected in this example.
   - **Name**: Enter a name for the EIP.

     The name must be 2 to 128 characters in length, and can contain letters, digits, periods (.), underscores (_), and hyphens (-). It must start with a letter.
   - **Resource Group**: Select the resource group to which the EIP belongs.
   - **Quantity**: Select the number of EIPs that you want to buy.
   - **Service Time**: Select a subscription duration.
4. Click **Buy Now** and complete the payment.
5. Click **Console** and return to the **Elastic IP Addresses** page.

After you return to the **Elastic IP Addresses** page, you can find the EIP that you created. The **Connection Type** of the EIP is **BGP (Multi-ISP) Pro**.



Step 2: Associate the EIP with an ECS instance

You can associate the EIP with an ECS instance that is deployed in a virtual private cloud (VPC). ECS instances can communicate with the Internet after they are associated with elastic IP addresses.

Perform the following steps to associate the EIP with an ECS instance:

1. On the **Elastic IP Addresses** page, find the EIP that you created in Step 1: Purchase a BGP (Multi-ISP) Pro EIP, and click **Bind Resource** in the **Actions** column.
2. In the **Bind Elastic IP Address to Resources** dialog box, set the following parameters.
   - **Instance Type**: Select the type of the instance that you want to associate with the EIP. **ECS Instance** is selected in this example.
   - **Binding Mode**: Select a binding mode.

     Only Normal is supported. In Normal mode:

     - Both the private and public IP addresses of the ECS instance are available.

- The EIP is not displayed in the operating system. You must call the DescribeInstances operation to query the public IP address of the ECS instance. For more information, see DescribeInstances.
- The EIP does not support NAT application layer gateway (ALG) protocols such as H.323, Session Initiation Protocol (SIP), Domain Name System (DNS), Real Time Streaming Protocol (RTSP), or Trivial File Transfer Protocol (TFTP).

- **Select an Instance to Bind**: Select an ECS instance to be associated with the EIP.

3. Click **OK**.

Step 3: Test the network latency

After you associate the EIP with the ECS instance, you can test the network latency between a client in mainland China and the ECS instance that is deployed in the China (Hong Kong) region.

1. Open the CLI on an on-premises machine that is deployed in mainland China.
2. Run the `ping` command to `ping` the EIP that is associated with the ECS instance.

   The test result shows that the network latency is reduced when users in mainland China use the BGP (Multi-ISP) Pro EIP to access the ECS instance.

   Network latency between the BGP (Multi-ISP) Pro EIP and the ECS instance

```
[root@iZbp1e1ke70d9k3tli17czZ ~]# ping 47.[redacted].46
PING 47.[redacted].46 (47.[redacted].46) 56(84) bytes of data.
64 bytes from 47.[redacted].46: icmp_seq=1 ttl=45 time=33.2 ms
64 bytes from 47.[redacted].46: icmp_seq=2 ttl=45 time=33.2 ms
64 bytes from 47.[redacted].46: icmp_seq=3 ttl=45 time=33.2 ms
64 bytes from 47.[redacted].46: icmp_seq=4 ttl=45 time=33.2 ms
64 bytes from 47.[redacted].46: icmp_seq=5 ttl=45 time=33.2 ms
^C
--- 47.[redacted].46 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 33.238/33.247/33.256/0.163 ms
```

   Network latency between the BGP (Multi-ISP) EIP and the ECS instance

```
[root@iZbp1e1ke70d9k3tli17czZ ~]# ping 8.[redacted].38
PING 8.[redacted].38 (8.[redacted].38) 56(84) bytes of data.
64 bytes from 8.[redacted].38: icmp_seq=1 ttl=45 time=112 ms
64 bytes from 8.[redacted].38: icmp_seq=2 ttl=45 time=111 ms
64 bytes from 8.[redacted].38: icmp_seq=3 ttl=45 time=111 ms
64 bytes from 8.[redacted].38: icmp_seq=4 ttl=45 time=104 ms
64 bytes from 8.[redacted].38: icmp_seq=5 ttl=45 time=109 ms
^C
--- 8.[redacted].38 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 104.208/109.888/112.068/2.983 ms
```

> **Note** The preceding test result is for reference only. The actual network latency varies based on the network quality of the ISP.

Why am I unable to associate an EIP with an ECS instance?

Possible causes:

- You can associate an EIP with only one ECS instance that is deployed in a VPC. If the ECS instance is not deployed in a VPC, you cannot associate an EIP with the ECS instance.

- The EIP and ECS instance are deployed in different regions.
- The ECS instance is in a state that does not allow you to associate an EIP with the ECS instance. You can associate an EIP with only an ECS instance that is in the Running or Stopped state.
- The ECS instance is assigned a public IP address or another EIP is associated with the ECS instance.

2.Associate multiple EIPs with an ECS instance in NAT mode

This topic describes how to associate multiple elastic IP addresses (EIPs) with a secondary elastic network interface (ENI) in NAT mode, and then associate the ENI with an Elastic Compute Service (ECS) instance.

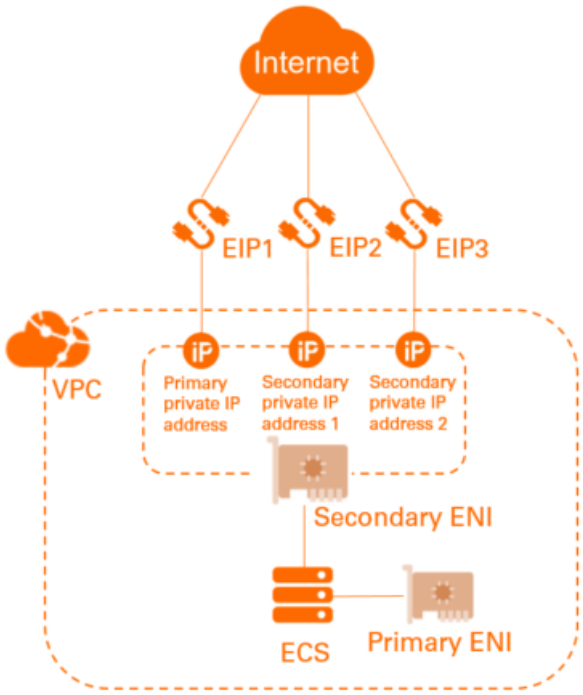
Context

- You can assign multiple secondary private IP addresses to a secondary ENI. If a secondary ENI is in the Available state, you can assign up to 10 secondary private IP addresses to the secondary ENI.
- Each secondary private IP address can be associated with an EIP in NAT mode. For more information about the NAT mode, see Association modes.
- ECS instances can communicate with the Internet only if they have public IP addresses. If you do not use a secondary ENI, each ECS instance can be assigned only one static public IP address or associated with only one EIP. To assign multiple public IP addresses to an ECS instance, you can associate EIPs with a secondary ENI, and then associate the secondary ENI with the ECS instance. If the ECS instance hosts multiple applications, each application uses an independent public IP address to communicate with the Internet. This way, you can improve the utilization of the ECS instance.

Scenarios

This scenario in the following figure is used an as example. A company has created an ECS instance on Alibaba Cloud and associated an EIP with the ECS instance. To meet business requirements, the company needs to associate three EIPs with the ECS instance.

You can assign two secondary private IP addresses to a secondary ENI. In this case, the secondary ENI has one primary private IP address and two secondary private IP addresses. Then, associate EIPs with the private IP addresses in NAT mode, and associate the secondary ENI with the ECS instance. This way, the ECS instance is associated with multiple EIPs.

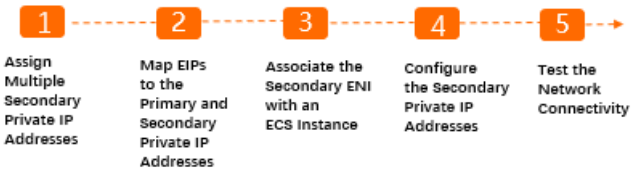


Prerequisites

- An ECS instance is created. For more information, see Create an instance by using the wizard.
- A secondary ENI is created and meets the following requirements:
  - The secondary ENI and the ECS instance to be associated with the secondary ENI are deployed in the same virtual private cloud (VPC).
  - The vSwitch of the secondary ENI and the vSwitch of the ECS instance to be associated with the secondary ENI are deployed in the same zone.

  For more information, see Create an ENI.
- Three EIPs are created in the same region as the ENI. For more information, see Apply for an EIP.

Procedure



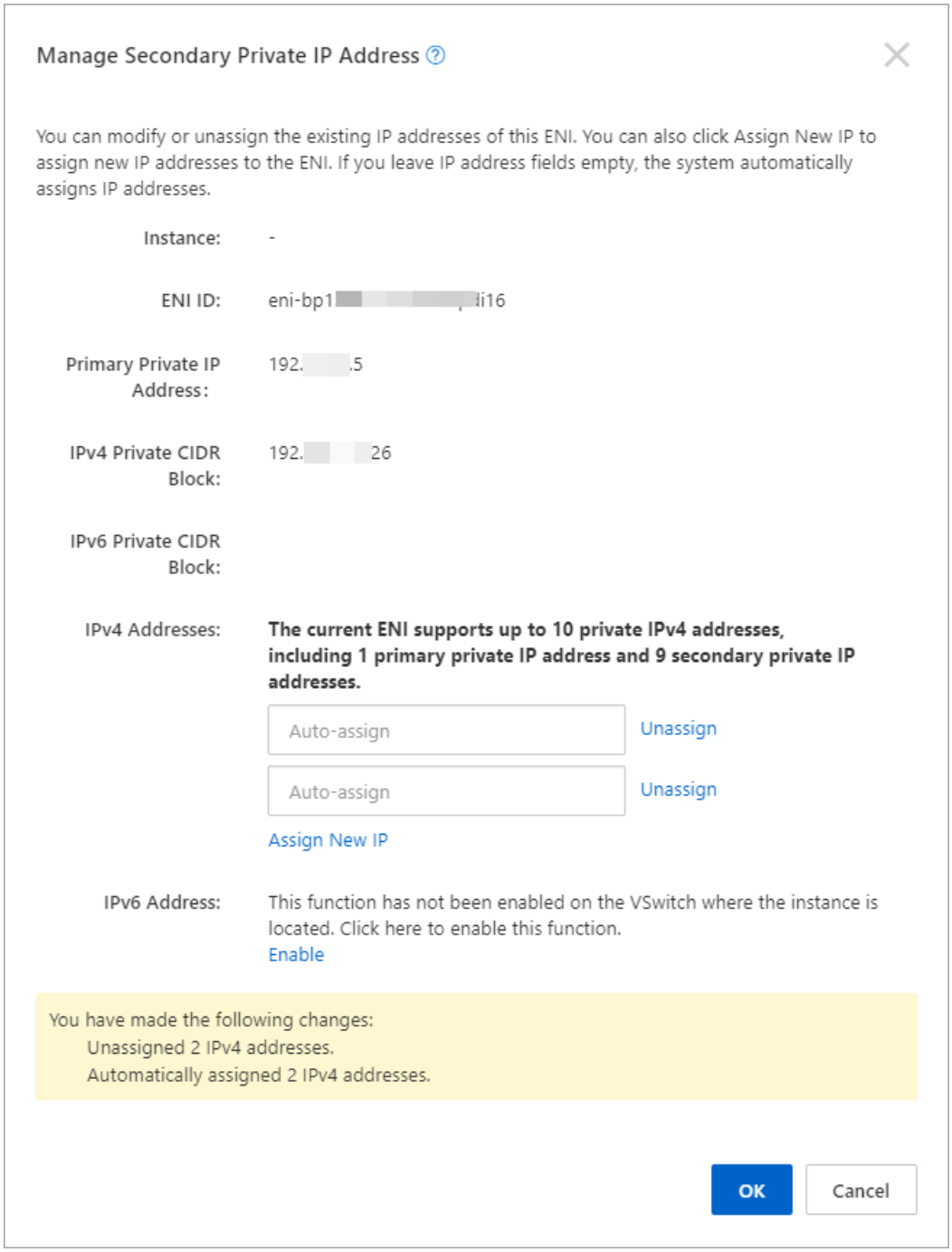
Step 1: Assign multiple secondary private IP addresses to a secondary ENI

You can assign multiple secondary private IP addresses to a secondary ENI and associate the secondary ENI with an ECS instance. This ensures high utilization and service availability of the ECS instance.

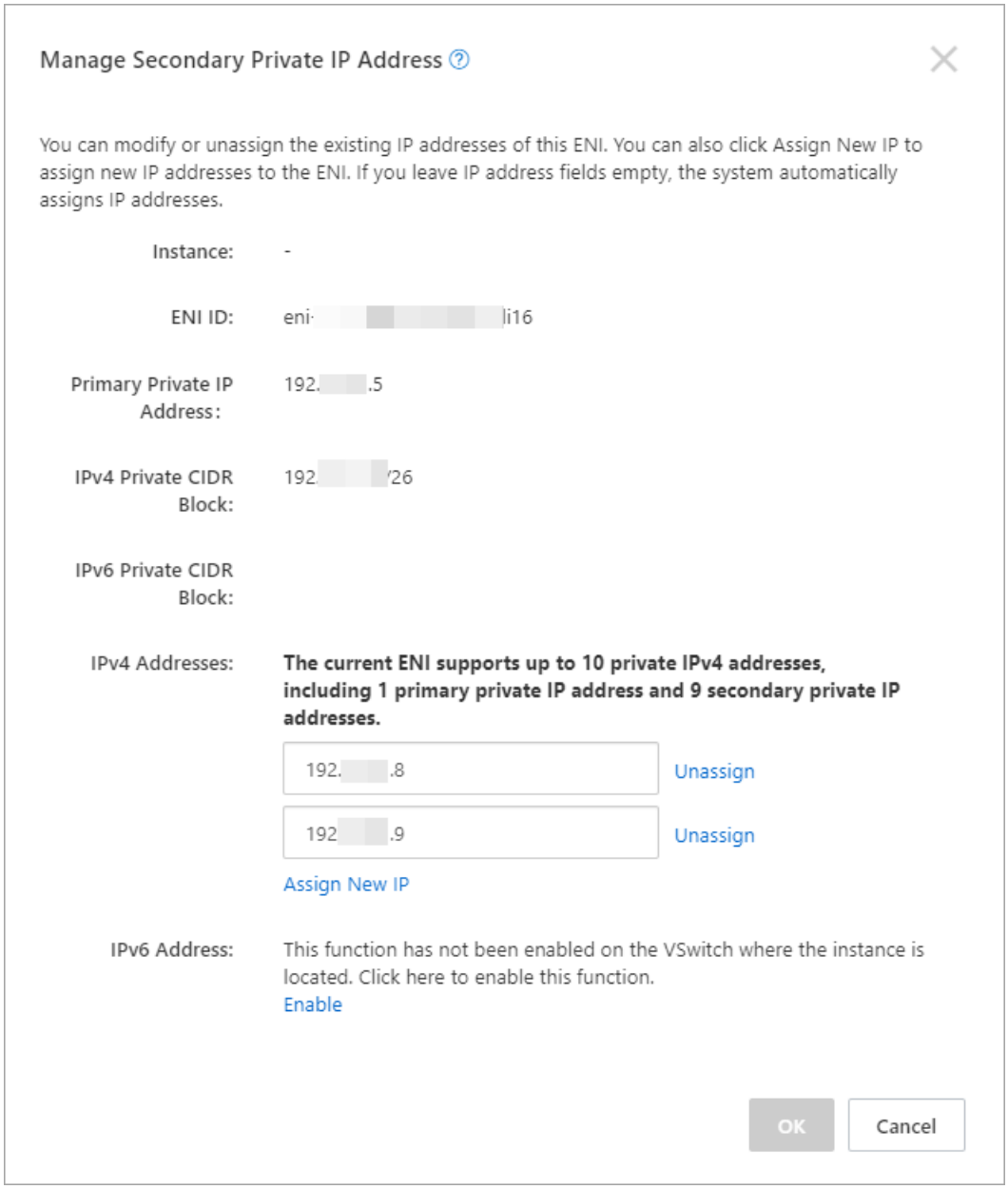
1. Log on to the ECS console.
2. In the left-side navigation pane, choose **Network & Security > ENIs**.
3. In the upper-left corner, select the region where the secondary ENI is deployed.
4. On the **Network Interfaces** page, find the ENI that you want to manage and click **Manage Secondary Private IP Address** in the **Actions** column.
5. In the **Manage Secondary Private IP Address** dialog box, click **Assign New IP** and click **OK**.

   Click **Assign New IP** twice in this example. This way, two secondary private IP addresses are automatically assigned to the secondary ENI.

   > **Note** You can also manually enter a secondary private IP address that falls within the **IPv4 private CIDR clock**. If you do not manually enter a secondary private IP address, the system assigns an idle IP address from the **IPv4 private CIDR block**.



6. On the **Network Interfaces** page, find the secondary ENI, and click **Manage Secondary Private IP Address** in the **Actions** column to view the assigned secondary private IP addresses.



Step 2: Associate EIPs with the secondary private IP addresses

1. Log on to the Elastic IP Address console .
2. In the upper-left corner, select the region where the EIPs are created.
3. On the **Elastic IP Addresses** page, find the EIP that you want to manage and click **Bind Resource** in the **Actions** column.
4. In the **Bind Elastic IP Address to Resources** dialog box, set the following parameters and click **OK**.
   - **Instance Type**: Select **Secondary ENI**.
   - **Mode**: Select **NAT Mode**.
   - **Select an instance to bind**: Select the secondary ENI with which you want to associate the EIP.

     In this example, the primary private IP address of the secondary ENI is selected.

5. Repeat the preceding steps to associate the other two EIPs with the secondary private IP addresses of the secondary ENI. Make sure that each EIP is associated with a separate secondary private IP address.

Step 3: Associate the secondary ENI with the ECS instance

1. Log on to the ECS console.
2. In the left-side navigation pane, choose **Instances & Images > Instances**.
3. In the top navigation bar, select the region where the ECS instance is deployed.
4. On the **Instances** page, find the ECS instance, and choose **More > Network and Security Group > Bind Secondary ENI** in the **Actions** column.
5. In the **Bind Secondary ENI** dialog box, select the secondary ENI to be associated and click **OK**.

Step 4: Configure the secondary private IP addresses

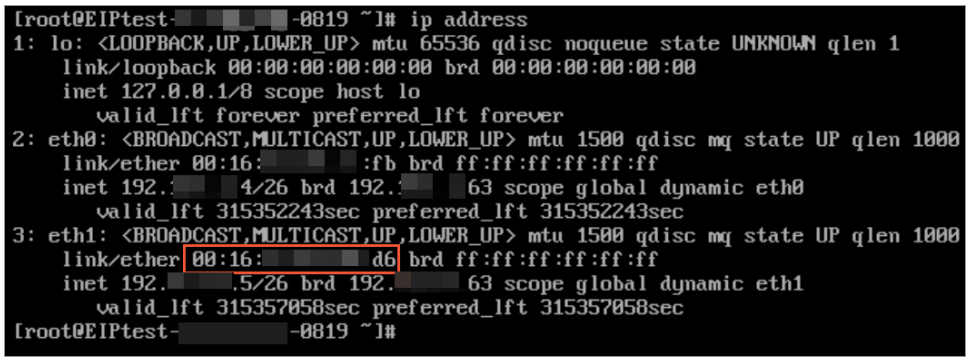
After you associate the secondary ENI with the ECS instance, you must configure the secondary private IP addresses for the ECS instance.

An ECS instance that runs CentOS 7 is used in the following example to describe how to configure the secondary private IP addresses for the ECS instance. For more information about how to configure ECS instances that run other operating systems, see Configure secondary private IPv4 addresses in a Windows instance and Configure secondary private IPv4 addresses in a Linux instance.

1. Log on to the ECS instance.

   For more information about how to connect to an ECS instance, see Overview.

2. Run the `ip address` command to view the media access control (MAC) address of the secondary ENI.



3. Configure the secondary private IP addresses for the secondary ENI.
   i. Run the following command to open the configuration file of the secondary ENI:

      `vi /etc/sysconfig/network-scripts/ifcfg-eth1`

ii. Press the **i** key to enter the edit mode. Modify the configuration file based on the following information.

```
DEVICE=eth1 # indicates that this is the configuration file of eth1, the newly configured secondary ENI.
BOOTPROTO=no
ONBOOT=yes
TYPE=Ethernet
USERCTL=yes
PEERDNS=nol
IPV6INIT=no
PERSISTENT_DHCLIENT=yes
HWADDR=00:16:**:**:fd:d6 # Configure the MAC address of the secondary ENI.
IPADDR0=192.xx.xx.5    # Configure the primary private IP address of the secondary ENI.
IPADDR1=192.xx.xx.8    # Configure one of the secondary private IP address of the secondary ENI.
IPADDR2=192.xx.xx.9    # Configure the other secondary private IP address of the secondary ENI.
DEFROUTE=no # indicates that the ENI is not the default route. To prevent changing the default route of the ECS instance when you bring up the secondary ENI, do not specify eth1 as the default route.
```

After you modify the configuration file, press the **Esc** key. Then, enter `:wq!` and press the **Enter** key to save the configuration file and exit the edit mode.

4. Run the following command to restart the network service:

   `service network restart`

After you configure the secondary private IP addresses, you can run the `ip address` command to view the configured secondary private IP addresses.

```
[root@EIPtest -0819 ~]# service network restart
Restarting network (via systemctl):                        [  OK  ]
[root@EIPtest- -0819 ~]# ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
    link/ether 00:16: fb brd ff:ff:ff:ff:ff:ff
    inet 192. .4/26 brd 192. .63 scope global dynamic eth0
       valid_lft 315359976sec preferred_lft 315359976sec
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
    link/ether 00:16 d6 brd ff:ff:ff:ff:ff:ff
    inet 192 .5/24 brd 192. .255 scope global eth1
       valid_lft forever preferred_lft forever
    inet 192. .8/24 brd 192. .255 scope global secondary eth1
       valid_lft forever preferred_lft forever
    inet 192 .9/24 brd 192. .255 scope global secondary eth1
       valid_lft forever preferred_lft forever
[root@EIPtest -0819 ~]#
```

Step 5: Verify network connectivity

An ECS instance that runs CentOS 7 is used in the following example to describe how to test the connectivity between the ECS instance and the destination network.

1. Log on to the ECS instance.

   For more information about how to connect to an ECS instance, see Overview.

2. Run the following command to configure a static route in which the source IP address is set to one

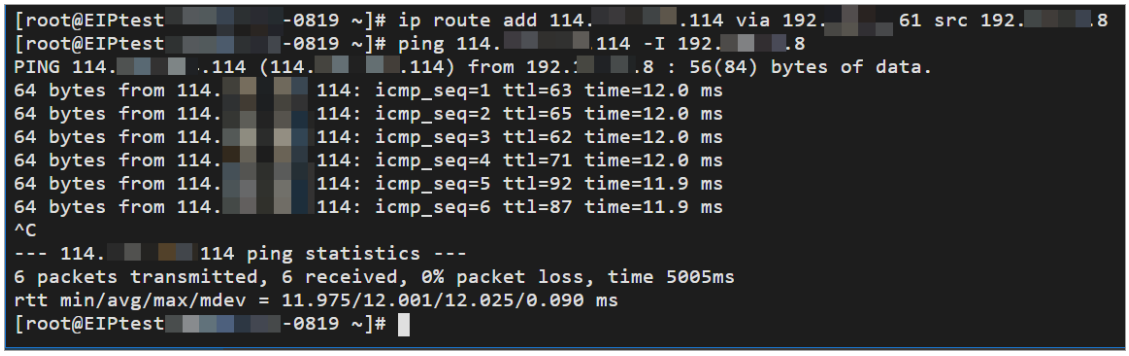
of the secondary private IP addresses:

```
ip route add <destination network>/<prefix length of the subnet> via <gateway of the secondary private IP address> src <secondary private IP address>
```

3. Run the following command to verify the connectivity between the secondary private IP address and the destination network:

   ```
   ping <destination network> -I <secondary private IP address>
   ```

   The test result shows that packets sent from the secondary private IP address can reach the destination network. This means that the ECS instance can access the Internet by using the EIPs associated with the private IP addresses.



Related information

- AssociateEipAddress

3.Bring your public IP address range to Alibaba Cloud

This topic describes how to bring your public IP address range from your on-premises network to Alibaba Cloud.

Context

Before you bring your public IP address range from your on-premises network to Alibaba Cloud, take note of the following limits:

- The public IP address range must be registered with a Regional Internet Registry (RIR).
- You must go to the corresponding Regional Internet Registry (RIR) platform to update the routing information by changing the autonomous system number (ASN) of the public IP address range to **AS45102**.
- You can bring only IP addresses in regions of North America, Asia Pacific, Europe, and Australia to Alibaba Cloud. Regions in mainland China are not supported. The following table lists the regions where you can bring the public IP address range of your on-premises network to Alibaba Cloud.

Area	Region
North America	US (Silicon Valley) and US (Virginia)
Asia Pacific	China (Hong Kong), Singapore (Singapore), Malaysia (Kuala Lumpur), Japan (Tokyo), Indonesia (Jakarta), and India (Mumbai)
Europe	Germany (Frankfurt) and UK (London)
Australia	Australia (Sydney)

- You can bring only public IPv4 addresses to Alibaba Cloud.
- The minimum prefix length of the IP address range is /23.
- The waiting time of bringing a public IP address range to the cloud:

  You can bring a public IP address range to Alibaba Cloud after you authorize an Internet service provider (ISP) to advertise the IP address range on the Internet. It may take up to one month.

- The waiting time of withdrawing a public IP address range:

  It may take one month for an ISP to withdraw an advertised IP address range.

- If you want your public IP address range to use EIP bandwidth plans, take note of the following limits:
  - The minimum bandwidth of an EIP bandwidth plan is 1,000 Mbit/s. You can add a maximum of 100 elastic IP addresses (EIPs) to each EIP bandwidth plan. If your workload requires bandwidth lower than 1,000 Mbit/s, we recommend that you directly use your public IP address range. Do not add the public IP address range to an EIP bandwidth plan.

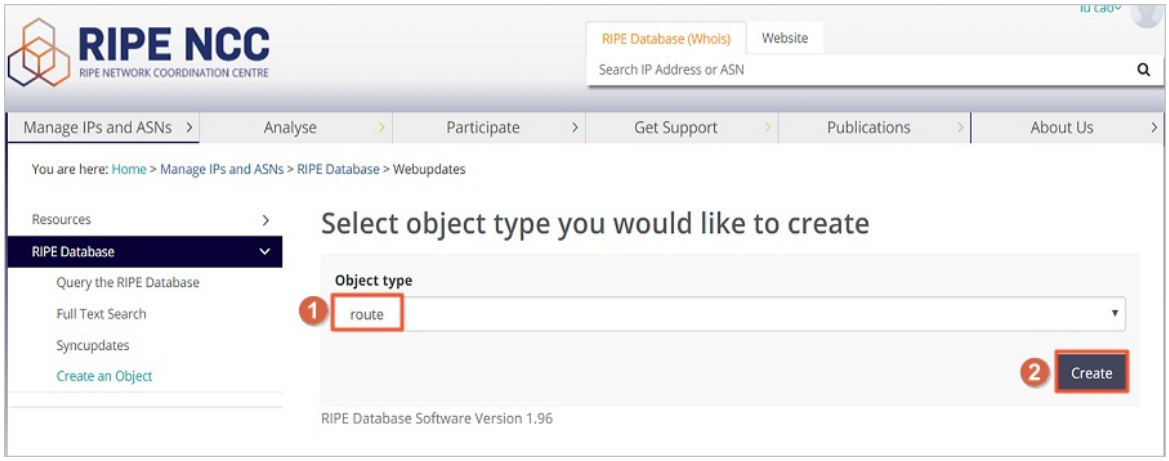
- Before you can add your public IP address range to an EIP bandwidth plan, the system checks where the maximum bandwidth of the plan meets the following requirements. Otherwise, you cannot add your public IP address range to the EIP bandwidth plan.
  - If a total of 1,000 public IP addresses are advertised to the Internet by Alibaba Cloud, the maximum bandwidth of the pay-by-bandwidth plan must be at least 1,000 Mbit/s. For every 1,000 additional pubic IP addresses, you must increase the maximum bandwidth by 1,000 Mbit/s.
  - If a total of 1,000 public IP addresses are advertised to the Internet by Alibaba Cloud, the maximum bandwidth of the pay-by-95th-percentile plan must be at least 1,000 Mbit/s. For every 1,000 additional pubic IP addresses, you must increase the maximum bandwidth by 1,000 Mbit/s.

Step 1: Update the routing information

You must go to the corresponding RIR platform to update the routing information by changing the ASN of the IP address range to **AS45102**.

The following example shows how to modify the ASN of an IP address range registered with Network Coordination Center (RIPE NCC).

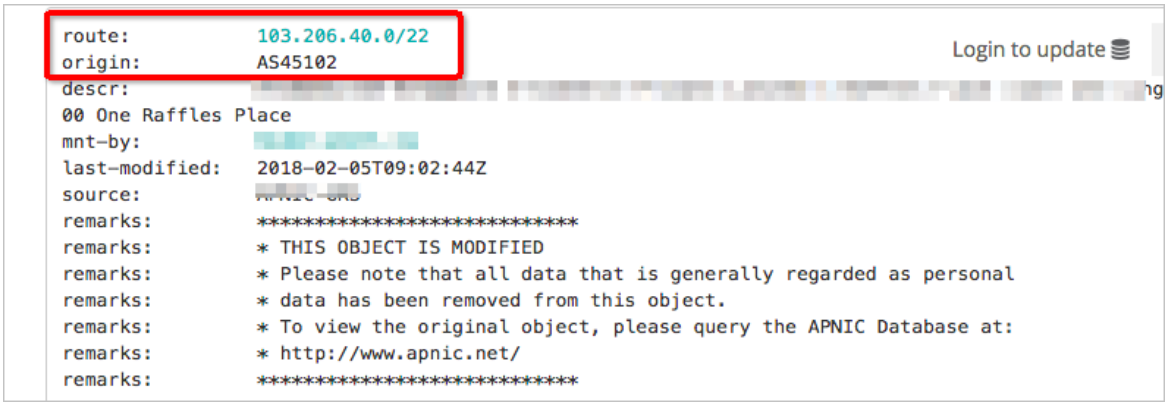
1. Log on to RIPE NCC Webupdates.
2. Select **route** from the **Object type** drop-down list and click **Create**.



3. On the **Create "route" object** page, select a role and maintainer pair from the drop-down list.
4. In the **Password authentication** field, enter the password and click **Submit**.
5. Configure the route reflector (RR) based on the following information, and then click **Submit**.

Parameter	Description
route	Enter the public IP address range.
origin	Enter the ASN. AS45102 is used in this example.

After you configure the route reflector, you can go to RADB to check whether the configuration takes effect.



Step 2: Apply for bringing the public IP address range to Alibaba Cloud

After you update the routing information, you must submit a ticket to bring the public IP address range of your on-premises network to Alibaba Cloud. Make sure that the following information is included in the ticket:

- The public IP address range.
- The region where the public IP address range is to be used.
- The updated routing information of the IP address range.

Step 3: Apply for an EIP

After you complete the preceding task, Alibaba Cloud will advertise the public IP address range from the specified region, and assign you a dedicated Service Provider Identification Number (SPIN). You will receive the SPIN within 20 business days. After you receive the SPIN, you can apply for EIPs that are brought to Alibaba Cloud on the buy page. For more information, see Apply for an EIP.

Step 4: Associate the EIP with a cloud resource

After you apply for an EIP, you can associate the EIP with an Alibaba Cloud resource, such as an Elastic Compute Service (ECS) instance, NAT gateway, internal-facing Server Load Balancer (SLB) instance, or elastic network interface (ENI). For more information, see the following topics:

- Associate an EIP with an ECS instance
- Associate an EIP with a NAT gateway
- Associate an EIP with an SLB instance
- Associate an EIP with an ENI

4.Deploy an FTP server by using an EIP

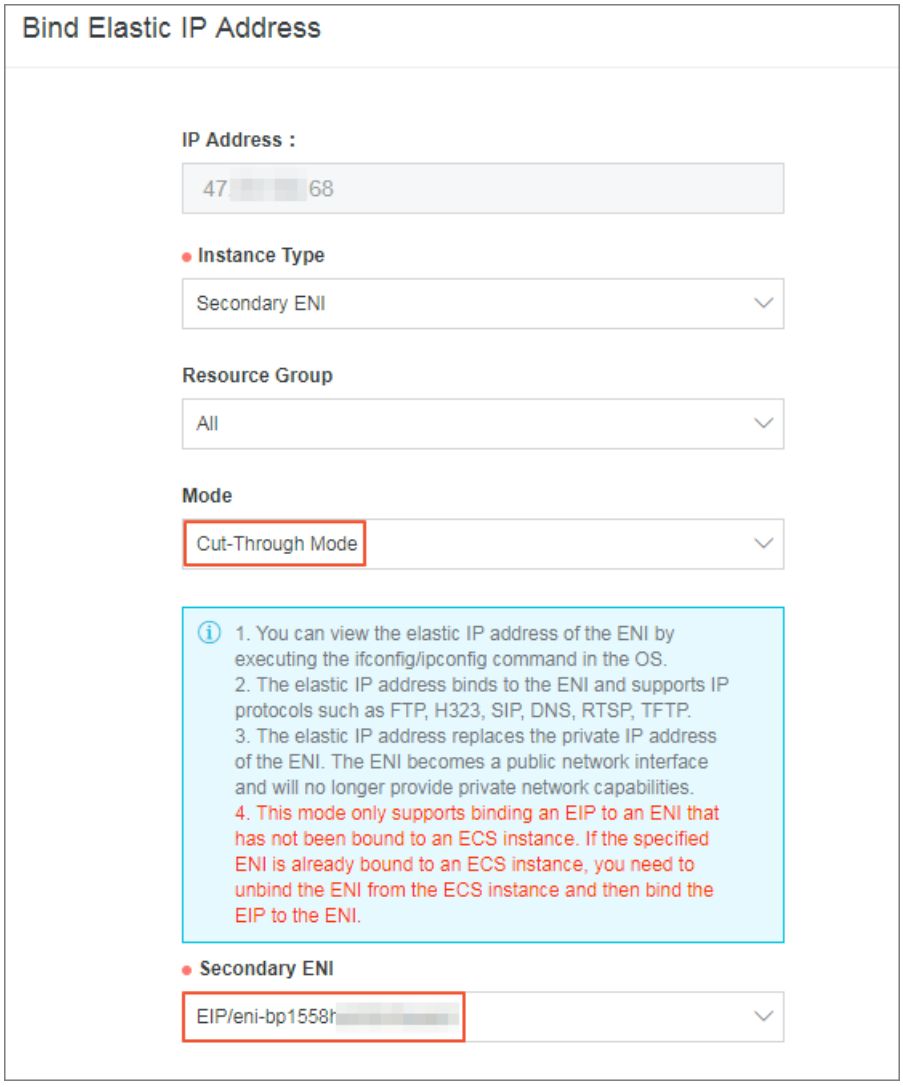
You can use the EIP cut-through mode to associate an Elastic IP Address (EIP) with an FTP server to provide FTP services. This topic takes an FTP server deployed with a Windows system as an example.

Procedure

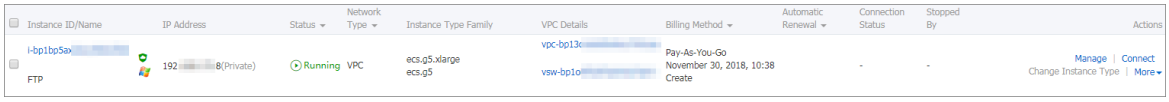
1. Apply for an EIP.
2. Associate the EIP with a secondary Elastic Network Interface (ENI) and select the EIP cut-through mode.

   > **Note** Make sure that the selected secondary ENI is not associated with any ECS instance.

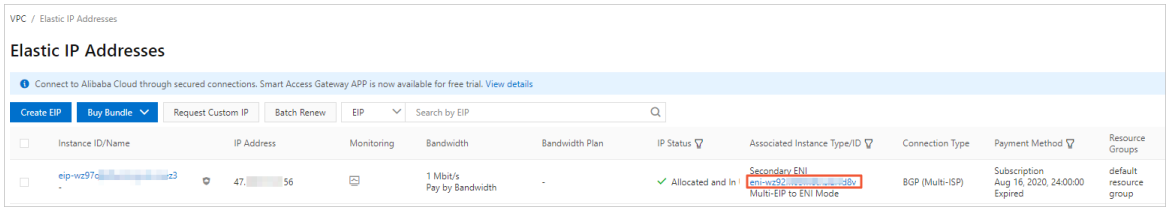
   For more information, see Associate an EIP with a secondary ENI in cut-through mode.



3. Purchase an ECS instance of the Windows Server 2016 system and deploy an FTP service.



4. On the page of EIP list, click the link of the associated ENI.

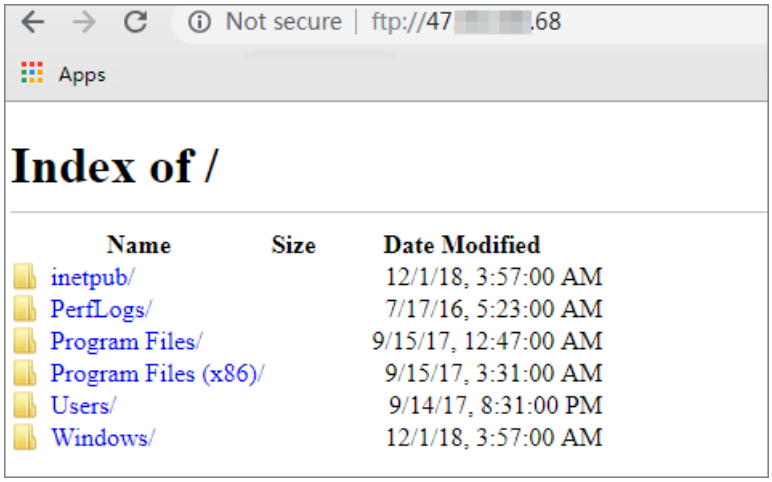


5. On the **Network Interfaces** page, find the ENI associated with the EIP and click **Bind to Instance** to associate the ENI with the ECS instance deployed with the FTP service.

Result

Use the EIP address associated with the ENI to access the FTP service.

> **Note** Make sure that the security group rules of the ECS instance allow access from the Internet.



5.Create an ECS instance in an IPv6 VPC

This topic describes how to create a virtual private cloud (VPC) with an IPv6 CIDR block and then create an Elastic Compute Service (ECS) instance that uses an IPv6 address. Then, the ECS instance can access other services over IPv6.

Step 1: Create a VPC and a vSwitch

Before you deploy cloud resources in a VPC, you must plan your networks. For more information, see Plan networks.

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

   The VPC and the cloud resources that you want to deploy must be in the same region. In this example, **China (Hohhot)** is selected.

   > **Note** Regions that support IPv6 CIDR blocks: .

3. On the **VPCs** page, click **Create VPC**.
4. On the **Create VPC** page, set the following parameters and click **OK**.

   > **Note** In this example, Assign is selected in the IPv6 CIDR Block section. After you create the VPC, the system automatically assigns an IPv6 CIDR block whose prefix is /56 to the VPC and creates a free IPv6 gateway. You can use the IPv6 gateway to process IPv6 traffic.

Parameter	Description
VPC	
Region	Displays the region where you want to deploy the VPC.
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 digits, underscores (_), and hyphens (-). It must start with a letter.

Parameter	Description
IPv4 CIDR Block	Enter an IPv4 CIDR block for the VPC. ◦ You can specify one of the following CIDR blocks or their subsets as the primary IPv4 CIDR block of the VPC: 192.168.0.0/16, 172.16.0.0/12 and 10.0.0.0/8. These three CIDR blocks are standard private CIDR blocks as defined by Request for Comments (RFC) documents. The subnet mask must be 8 to 24 bits in length. For example, enter 192.168.0.0/24. ◦ You can also use a custom CIDR block other than 100.64.0.0/10, 224.0.0.0/4, 127.0.0.0/8, 169.254.0.0/16, or their subnets as the primary IPv4 CIDR block of the VPC. ◦ In scenarios where multiple VPCs are used or in hybrid cloud scenarios where data centers and VPCs are used, we recommend that you use standard RFC CIDR blocks as VPC CIDR blocks with subnet masks no more than 16 bits in length. Make sure that the CIDR blocks of the VPCs and data centers do not overlap. **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.
IPv6 CIDR Block	Specify whether to assign an IPv6 CIDR block to the VPC. By default, no IPv6 CIDR block is allocated. If you set this parameter to Assign, the system automatically creates a free IPv6 gateway for this VPC, and assigns an IPv6 CIDR block with the subnet mask /56, such as 2xx1:db8::/56. By default, IPv6 addresses can only be used to communicate within private networks. If you want to use the IPv6 address to access the Internet or to be accessed by IPv6 clients over the Internet, you must purchase an Internet bandwidth plan for the IPv6 address. For more information, see Purchase a public bandwidth plan for an IPv6 address. **Note** ◦ The following regions support IPv6 CIDR blocks: China (Qingdao), China (Beijing), China (Zhangjiakou), China (Hohhot), China (Ulanqab), China (Hangzhou), China (Shanghai), China (Shenzhen), China (Heyuan), China (Guangzhou), China (Chengdu), China (Hong Kong), Singapore (Singapore), US (Virginia), and Germany (Frankfurt).. ◦ After you create a VPC, you cannot change its IPv6 CIDR block.

Parameter	Description
Description	Enter a description for the VPC. The description must be 2 to 256 characters in length and cannot start with `http://` or `https://`.
Resource Group	Select the resource group to which the VPC belongs.
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 the same VPC, vSwitches in different zones can communicate with each other.
Zone Resources	Displays the cloud resources 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 instances provided in this topic are for reference only. The actual instances on the buy page shall prevail. Only Elastic Compute Service (ECS), 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. When you specify an IPv4 CIDR block for the vSwitch, take note of the following limits: ○ 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 a VPC is 192.168.0.0/16, the CIDR block of a vSwitch in the VPC must be a subset of 192.168.0.0/16. In this example, the CIDR block of the vSwitch can range from 192.168.0.0/17 to 192.168.0.0/29. ○ The first IP address and last three IP addresses of a vSwitch CIDR block are reserved. For example, if a 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 is required to communicate with vSwitches in other VPCs or with data centers, make sure that the CIDR block of the vSwitch does not overlap with the destination CIDR blocks. **Note** After you create a vSwitch, you cannot modify its CIDR block.

Parameter	Description
Available IP Addresses	Displays the number of available IP addresses.
IPv6 CIDR Block	Enter an IPv6 CIDR block for the vSwitch. By default, the subnet mask for the IPv6 CIDR block of a vSwitch is /64. You can enter a decimal number from 0 to 255 to define the last 8 bits of the IPv6 CIDR block. For example, if the IPv6 CIDR block of the VPC is 2xx8:4004:c0:b900::/56, you can specify 255 to define the last 8 bits of the IPv6 CIDR block. In this case, the IPv6 CIDR block of the vSwitch is 2xx8:4004:c0:b9ff::/64. ff is the hexadecimal value of 255.
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

After you create a VPC with an IPv6 CIDR block and a vSwitch, create an ECS instance and assign an IPv6 address to the ECS instance. You must allocate the IPv6 address to the network interface controller (NIC) of the ECS instance.

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

   In this example, the following parameters are set for Networking:

   - **Public IP Address**: **Assign Public IPv4 Address** and **Pay-By-Bandwidth** are selected and the bandwidth limit is set to 1 Mbit/s. You can also use an elastic IP address (EIP) instead of assigning a public IP address to the ECS instance.
   - **IPv6**: **Assign IPv6 Address Free of Charge** is selected.
6. Return to the **Instances** page and click the ID of the ECS instance that you created to view the IPv6 address that is assigned to the ECS instance.
7. Assign a static IPv6 address to the ECS instance.

Step 3: Purchase an IPv6 public bandwidth plan

By default, IPv6 addresses are used only for communication within private networks. If you want to allow an ECS instance that is assigned an IPv6 address to access the Internet or receive requests from IPv6 clients over the Internet, you must purchase a public bandwidth plan.

1. Log on to the IPv6 gateway console.

2. In the top navigation bar, select the region of the IPv6 gateway. In this topic, **China (Hohhot)** is selected.
3. On the **IPv6 Gateway** page, find the IPv6 gateway that you want to manage and click **Manage** in the **Actions** column.
4. On the **IPv6 Internet Bandwidth** tab, find the IPv6 address that you want to manage and click **Enable IPv6 Internet Bandwidth** in the **Actions** column.
5. Specify the billing method and a bandwidth limit, click **Buy Now**, and then complete the payment.

Step 4: Configure security group rules

Services that are assigned IPv4 addresses and services that are assigned IPv6 addresses cannot communicate with each other. If the current security group rules do not support your IPv6 services, you must configure IPv6 security group rules for the ECS instance.

For more information, see Add security group rules.

Step 5: Verify network connectivity

Log on to the ECS instance and run the `ping` command to `ping` an IPv6 service over the Internet to verify network connectivity. If the ECS instance can receive echo reply packets, it indicates that the connection is reachable.

The test result shows that the ECS instance can access the Internet over IPv6.