ALIBABA CLOUD

Alibaba Cloud

Elastic Compute Service

Network

Document Version: 20200917

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.Network types 05
2.Instance IP addresses 07
2.1. IP addresses of ECS instances within VPCs 07
2.2. Elastic IP Addresses 08
3.Change IPv4 addresses 10
3.1. Change the private IP address of an instance 10
3.2. Change the public IP address of an ECS instance 11
3.3. Convert the public IP address of a VPC-type instance to... 13
3.4. Convert the public IP address of a classic network-type... 14
4.Elastic Network Interfaces 17
4.1. ENI overview 17
4.2. Create an ENI 19
4.3. Attach an ENI 20
4.4. Configure an ENI 22
4.5. Assign secondary private IP addresses 30
4.6. Revoke secondary private IP addresses 35
4.7. Modify an ENI 36
4.8. Detach an ENI from an instance 38
5.Change the VPC of an ECS instance 39
6.Configure NIC multi-queue 41
7.Network FAQ 44

1.Network types

Alibaba Cloud ECS provides two network types: Virtual Private Cloud (VPC) and classic network.

network classic network VPC nat ip

VPC

VPC is an isolated virtual network environment built on Alibaba Cloud public cloud. VPCs are logically isolated from each other. You can customize the topology and IP addresses in a VPC. VPC is suitable for users who have high network security requirements and network management capabilities.

For more information, see What is a VPC?.

Classic network

Services that use the classic network are deployed in the public infrastructure of Alibaba Cloud, and planned and managed by Alibaba Cloud. The classic network is suitable for users who have high requirements for network usability.

> Note If you purchased your first ECS instance after 12:00:00 (UTC+8) on June 16, 2017, you cannot select the classic network.

Differences

The following table shows differences between VPCs and the classic network.

Item	VPC	Classic network
Layer 2 logical isolation	Supported.	Not supported.
Custom private CIDR block	Supported.	Not supported.
Private IP address planning	Private IP addresses must be unique within a single VPC, but can be duplicate across VPCs.	Private IP addresses must be unique in the classic network.
Instance communication within or between private networks	Instances in the same VPC can communicate with each other. However, instances in different VPCs are isolated.	Instances in the classic network can communicate with each other if they belong to the same region and the same account.
Tunneling	Supported.	Not supported.
Custom router	Supported.	Not supported.
Routing table	Supported.	Not supported.
VSwitch	Supported.	Not supported.
SDN	Supported.	Not supported.

Item	VPC	Classic network
Self-built NAT gateway	Supported.	Not supported.
Self-built VPN	Supported.	Not supported.

2.Instance IP addresses

2.1. IP addresses of ECS instances within VPCs

IP addresses are used for access to ECS instances or to the services deployed on the instances. ECS instances within VPCs can be assigned two types of IP addresses: private IP addresses and public IP addresses.

Alibaba Cloud Elastic IP address ECS public bandwidth

Private IP addresses

Each new ECS instance within a VPC is assigned a private IP address based on the VPC and CIDR block of the VSwitch to which the instance is connected. Private IP addresses can be used in the following scenarios:

- Load balancing
- Communication between ECS instances within the internal network
- Communication between an ECS instance and other cloud services such as OSS and ApsaraDB for RDS within the internal network

You can use the ECS console to modify the private IP addresses of ECS instances within VPCs based on your business needs. For more information, see Change the private IP address of an instance. For more information about internal network communication, see 内网.

Public IP addresses

ECS instances within VPCs support the following types of public IP addresses:

- NatPublicIP addresses, which are the public IP addresses assigned by the ECS system
- Elastic IP addresses (EIPs). For more information, see What are Elastic IP Addresses.

The following table lists the major differences between the two types of public IP addresses.

Item	NatPublicIP address	EIP
Scenarios	If you want to assign a public IP address to an ECS instance during instance creation but do not want the public IP address to be retained when the instance is released, use a NatPublicIP address.	If you want to retain a public IP address to be used with other ECS instances located within the same region, use an EIP. Each EIP can be associated or unassociated with different ECS instances. After an instance is released, its associated EIP will be retained.
Method to obtain an address	If you select **Assign Public IP Address** when creating an ECS instance within a VPC, a NatPublicIP address is assigned to the instance.	Create an EIP, and associate it to an ECS instance that is not assigned a NatPublicIP address. For more information, see Create an Elastic IP address.

Item	NatPublicIP address	EIP
Maximum number of public IP addresses that can be assigned or associated to a single ECS instance	An ECS instance can only be assigned a single NatPublicIP address.	Multiple EIPs can be associated to a single ECS instance in multi-EIP to ENI mode. For information about how to configure the multi-EIP to ENI mode, see Associate EIPs with secondary ENIs in multi-EIP-to-ENI mode.
Method to unassociate an address	After a NatPublicIP address is assigned to an ECS instance, the address can be released only and cannot be unassociated from the instance.	See Disassociate an EIP from a cloud resource.
Method to release an address	• When ECS instances are released, their assigned NatPublicIP addresses are also released. • During the lifecycle of an ECS instance, you can release its NatPublicIP address by setting the public bandwidth of the instance to 0 Mbit/s. For information about how to modify the public bandwidth of a pay-as-you-go ECS instances, see Change the bandwidth of a pay-as-you-go instance.	See Release an EIP.
Method to view the MAC address	ECS instances within VPCs access the Internet through the mapping of public IP addresses to internal NICs. Therefore, you cannot find public NICs inside ECS instances within VPCs regardless of whether the instances are assigned NatPublicIP addresses or associated with EIPs.	

Billing

You are only billed for outbound Internet traffic. For more information, see Billing methods of public bandwidth.

2.2. Elastic IP Addresses

An Elastic IP Address (EIP) is an independent public IP address that you can purchase and use. EIPs can be associated to different ECS instances that reside within VPCs over time to allow access to the ECS instances.

Overview

EIPs are NAT IP addresses that are located in the public gateway of Alibaba Cloud. Through NAT, EIPs are mapped to the NICs in internal networks of the ECS instances that are associated with the EIPs. You can associate EIPs to ECS instances that reside within VPCs to enable the instances to communicate with the public network. However, you cannot view the EIPs on the NICs of the ECS instances.

Benefits

Public IP addresses are automatically assigned to ECS instances when you configure public bandwidth for the instances. Compared with these public IP addresses, EIPs provide more flexibility for purchase and management. The following table compares public IP addresses assigned to ECS instances and EIPs.

Item	Public IP address assigned to an ECS instance	EIP
Can the IP address be independently purchased and used?	No	Yes
Can the IP address be associated to or disassociated from an ECS instance as needed?	No	Yes
Can the bandwidth value for the IP address be adjusted in real time?	Yes	Yes

Billing method

EIPs can be billed by traffic or by bandwidth. For more information, see *EIP document* Billing.

Limits

An EIP can be associated only to an ECS instance that meets the following requirements:

- The ECS instance resides within a VPC.
- The ECS instance is in the same region as the EIP.
- The ECS instance is in the **Running** or **Stopped** state.
- The ECS instance is not associated with system-assigned public IP addresses or EIPs.

Create an EIP

You can create an EIP and associate it to an ECS instance that resides within a VPC and is not assigned public IP addresses. For more information, see Apply for new EIPs.

You can follow these steps to allow an ECS instance that resides within a VPC to have one system-assigned public IP address and multiple EIPs: Associate multiple EIPs to an ENI by selecting the Multi-EIP to ENI mode and attach the ENI to the ECS instance. For more information, see Associate EIPs with secondary ENIs in multi-EIP-to-ENI mode.

Release an EIP

If you no longer need an EIP, disassociate it from the ECS instance and then log on to the EIP console to release it. For more information, see Disassociate an EIP from a cloud resource.

3.Change IPv4 addresses

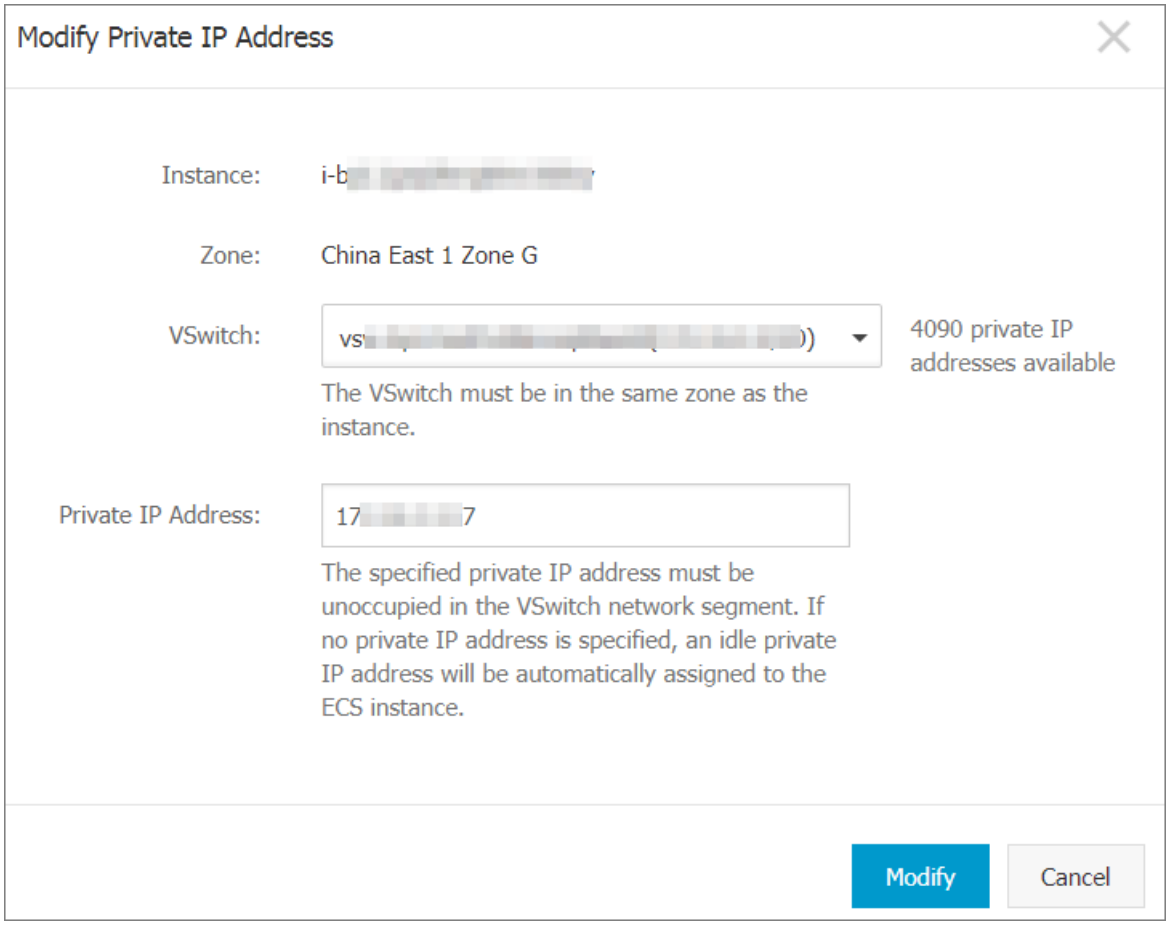
3.1. Change the private IP address of an instance

After creating a VPC-type ECS instance, you can change the private IP address of the instance or the private IP address of the VSwitch for the ECS instance.

private IP address

Procedure

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 a region.
4. Find the target disk and choose **More > Instance Status > Stop** in the **Actions** column.
5. After the instance is stopped, click the instance ID.
6. In the **Configuration Information** section, choose **More > Modify Private IP Address**.
7. In the **Modify Private IP Address** dialog box that appears, modify the parameters and click **Modify**.
   - If you want to change the VSwitch, make sure that the selected VSwitch resides within the same zone as the instance.
   - If you do not want to change the VSwitch, modify the private IP address.



8. Go back to the Instances page. Find the target disk and choose **More > Instance Status > Start** in the **Actions** column. The new private IP address will take effect after the ECS instance has been restarted.

Related information

- ModifyInstanceVpcAttribute

3.2. Change the public IP address of an ECS instance

If your ECS instance of the classic network or VPC type was assigned a public IP address within the last six hours, you can change the public IP address.

change IP address change DNS record new DNS IP address ECS IP address

Prerequisites

Before changing the public IP address of an ECS instance, ensure that the following requirements are met:

- The ECS instance is in the `Stopped` state.

> **Note** If **No Charges After Instance Is Stopped** is enabled for your account, you must select **Retain Instance and Continue Charging After Instance Is Stopped** when stopping the ECS instance. Otherwise, the **Change Public IP Address** item will not be displayed in the ECS console after you stop the ECS instance.

- The ECS instance was assigned a public IP address.
- The public IP address was assigned within the last six hours.

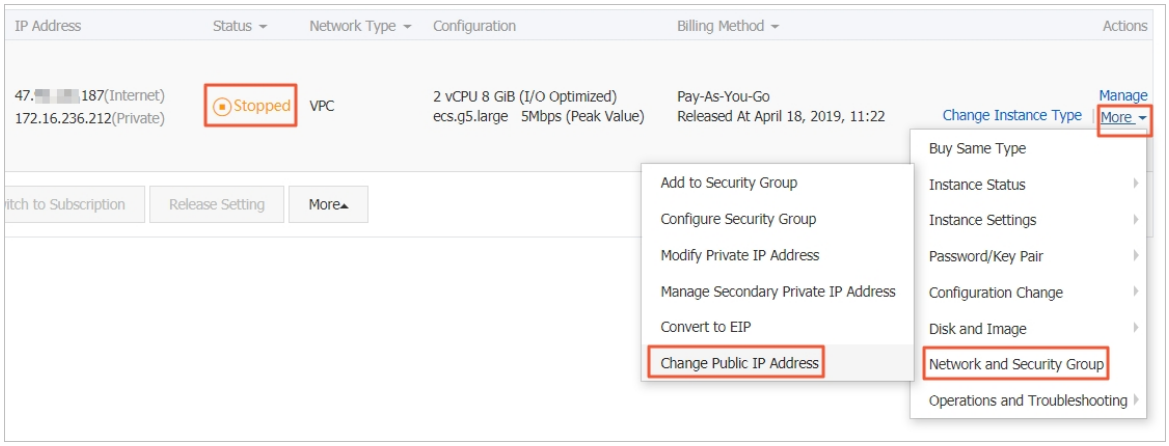
Context

Changing the public IP address of an ECS instance is subject to the following limits:

- You can change the public IP address of an ECS instance a maximum of three times.
- If no public IP address was allocated during ECS instance creation, you cannot use the procedure set out in this topic. In this case, you must use either of the following methods:
  - Apply for and bind an Elastic IP Address (EIP) to the ECS instance. For more information, see the following topic of *EIP documentation:* Apply for new EIPs.
  - Modify the public bandwidth of the ECS instance to allocate a fixed public IP address. For more information about modifying the public bandwidth of a subscription ECS instance, see Overview of instance upgrade and downgrade. For more information about modifying the public bandwidth of a pay-as-you-go ECS instance, see Change the Internet bandwidth of a pay-as-you-go instance.

Procedure

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 a region.
4. Find the ECS instance that you want to change the IP address for. Choose **More > Network and Security Group > Change Public IP Address**.



5. In the **Change Public IP Address** dialog box that appears, click **Start Now**.
   If the operation is successful, a new public IP address is displayed in the dialog box.
6. Click **OK**.

3.3. Convert the public IP address of a VPC-type instance to an Elastic IP address

You can convert the public IP address of a VPC-type instance to an Elastic IP address (EIP), and then unbind the EIP from the instance and bind the EIP to another instance at any time. Address conversion does not affect the access from the Internet to your ECS instance or cause transient network outage.

Prerequisites

Before you convert the public IP address of a VPC-type instance to an EIP, make sure the following requirements are met:

- The instance is assigned a public IP address.
- If the instance is a pay-as-you-go instance, your account has no overdue payments.
- If the instance is a subscription instance, the instance must not be within 24 hours before expiry.
- If the instance is a subscription instance, the instance uses **Pay-By-Traffic** billing method for Internet usage. You can change the billing method for Internet usage from **Pay-By-Bandwidth** to Pay-By-Traffic by upgrading or downgrading instance configurations. For more information, see Overview of instance upgrade and downgrade.
- If the instance type has been changed, wait until the change takes effect before you make the address conversion.
- The instance is in the **Running** or **Stopped** state.

Context

After the public IP address of a VPC-type instance is converted to an EIP:

- The billing method for Internet usage remains unchanged.
- The EIP is billed separately. For more information about EIP billing, see Billing overview. You can go to the **Billing Management** console. In the left-side navigation pane, click Usage Records, and select **Elastic IP** from the Product Name drop-down list to export EIP usage records.

This section describes how to convert the public IP address of a VPC-type ECS instance to an EIP by using the ECS console. You can also convert the IP address by calling the ConvertNatPublicIpToEip operation. To call this operation, use SDK 4.3.0 or later. For more information, see SDK reference.

Procedure

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 a region.
4. Find the target instance whose network type is **VPC**, and then choose **More > Network and Security Group > Convert to EIP** in the **Actions** column.
5. In the dialog box that appears, confirm the information, and click **OK**.
6. Refresh the instance list.

Result

After the public IP address is converted to an EIP, the public IP address is marked by **(EIP)**.

You can click the EIP to go to the Elastic IP Addresses page in the VPC console to manage the EIP.

What's next

After the public IP address is converted to an EIP, you can perform the following operations:

- Unbind the EIP from the instance and bind the EIP to another instance, or release the EIP. For more information, see Disassociate an EIP from a cloud resource.
- Add the EIP to a shared bandwidth plan to save costs. For more information, see Associate an EIP with an EIP bandwidth plan, Select a product to gain access to the Internet, and Reduce Internet costs.

Related information

- ConvertNatPublicIpToEip

3.4. Convert the public IP address of a classic network-type instance to an Elastic IP address

When you manually release a classic network-type ECS instance, you can convert its public IP address to an Elastic IP address (EIP). An EIP can be bound to a VPC-type ECS instance for various scenarios such as network migration, elastic binding, and flexible bandwidth adjustment. You can convert the public IP address of a classic network-type instance to an EIP only when you manually release the instance.

classic network public IP address convert the public IP address network migration EIP

Prerequisites

Before you convert the public IP address of a classic network-type ECS instance to an EIP, make sure the following requirements are met:

- The instance has been assigned a public IP address.
- The zone to which the instance belongs cannot be Hangzhou Zone C.
- If the instance is a pay-as-you-go instance, it is in the **Stopped** state and your account has no overdue payments.
- If the instance is a subscription instance, it is in the **Expired** or **To Be Released** state.
- If the instance is a subscription instance, the billing method of the Internet bandwidth is **Pay-By-Traffic**. You can change the **Pay-By-Bandwidth** billing method of the Internet bandwidth by upgrading or downgrading the instance. For more information, see Overview of instance upgrade and downgrade.
- If the type of the instance has been changed, wait until the change takes effect before proceeding.
- You have created snapshots for the instance to prevent data loss caused by incorrect operations. For more information, see Create a snapshot.

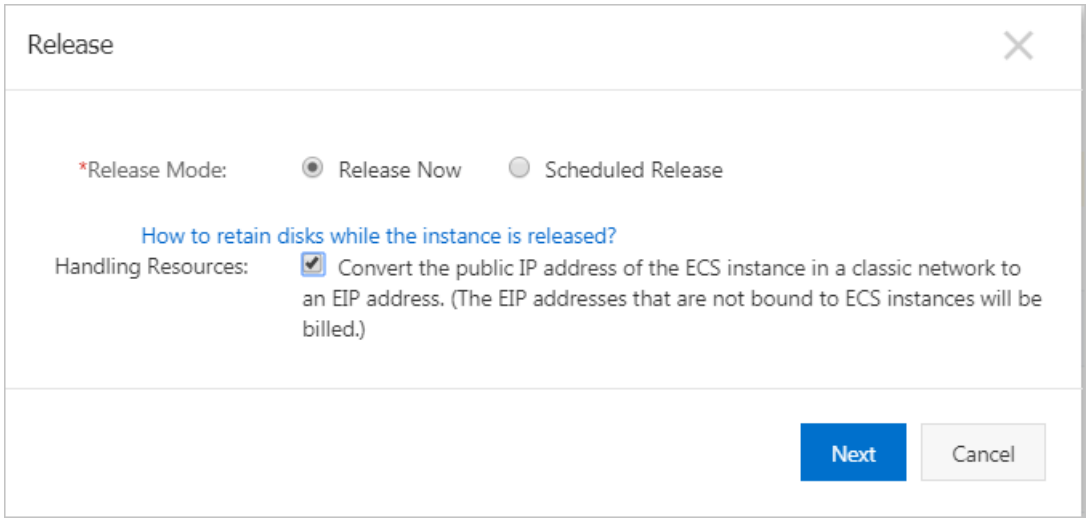
Context

After the public IP address of a classic network-type instance is converted to an EIP,

- The billing method for the Internet bandwidth of the EIP is Pay-By-Traffic.
- The Internet bandwidth of the EIP is the same as that of the original ECS instance. You can change the Internet bandwidth of the EIP as needed in the VPC console. If the Internet bandwidth of the classic network-type instance is 0 Mbit/s before conversion, the Internet bandwidth of the converted EIP is automatically upgraded to 1 Mbit/s.
- The EIP cannot be bound to a classic network-type ECS instance.
- A classic network-type ECS instance has a public network interface controller (NIC). If the public IP address of the ECS instance is converted to an EIP, the public NIC and MAC address of the instance will not be retained.

Procedure

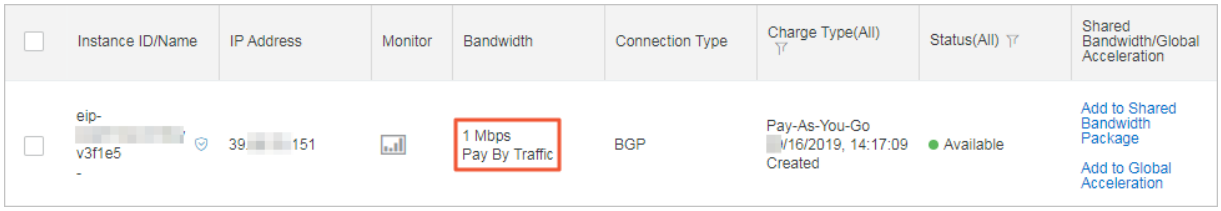
1. Log on to the ECS console.
2. In the left-side navigation pane, choose **Instances & Images > Instances**.
3. In the top navigation bar, select a region.
4. Find the classic network-type instance and select a release method.
   - To release a subscription instance, click **Release** in the **Actions** column corresponding to the instance.
   - To release a pay-as-you-go instance, choose **More > Instance Status > Release** from the **Actions** column.
5. Select **Release Now**, select **Convert the public IP address of the ECS instance in a classic network to an EIP address. (The EIP addresses that are not bound to ECS instances will be billed.)**, and then click **Next**.



6. Click **OK**.

Result

After the public IP address of a classic network-type ECS instance is converted to an EIP, the instance is released. You can view the converted EIP in the VPC console.



What's next

You can bind this EIP to another ECS instance. For more information, see Associate an EIP with an ECS instance.

4.Elastic Network Interfaces

4.1. ENI overview

An Elastic Network Interface (ENI) is a virtual network interface that can be attached to an ECS instance in a VPC. You can use ENIs to deploy high-availability clusters and perform low-cost failovers and fine-grained network management.

NIC ENI ECS Alibaba Cloud IP

Scenarios

ENIs are suitable for:

- Deploying high-availability clusters

  Multiple ENIs can be attached to an ECS instance, implementing a high-availability architecture.

- Providing low-cost failover solutions

  You can detach an ENI from a failed ECS instance and attach the ENI to another instance to redirect traffic destined for the failed instance to the backup instance. This allows quick recovery of services.

- Managing networks with refined controls

  You can configure multiple ENIs for an instance. For example, you can use some ENIs for internal management and other ENIs for Internet business access to isolate confidential data from business data. You can also configure specific security group rules for each ENI based on the source IP addresses, protocols, ports, and more to achieve traffic control.

- Configuring multiple private IP addresses for one instance

  You can assign multiple private IP addresses to the ENIs that are attached to ECS instances. The maximum number of private IP addresses that can be assigned varies with the instance type. Up to 20 private IP addresses can be assigned to an ENI that is attached to an instance.

- Configuring multiple public IP addresses for one instance

  An ECS instance with no ENI attached can be assigned only one public IP address. You can assign multiple public IP addresses to an instance by associating Elastic IP addresses (EIPs) to one or more ENIs of the instance. EIPs can be bound with the private IP addresses of an ENI in NAT mode.

ENI types

ENIs are classified into two types:

- Primary ENIs

  A primary ENI is the ENI that is automatically created when an instance in a VPC is created. The life cycle of the primary ENI is the same as that of the instance, and you cannot detach the primary ENI from the instance.

- Secondary ENIs

  You can create a separate secondary ENI that can be freely attached and detached.

> **Note** For the instances whose images cannot identify secondary ENIs, log on to the instance to configure the ENIs. For more information, see Configure an ENI.

ENI attributes

The following table describes the attributes of an ENI.

Attribute	Quality
Primary private IP address	1
Secondary private IP address	1 or more. The maximum number of secondary private IP addresses that can be associated to an ENI depends on the instance type. For more information, see Instance families.
EIP	1 or more. The maximum number of EIPs that can be associated to an ENI depends on the associating mode. For more information, see Overview for associating an EIP with a secondary ENI.
MAC address	1
Security group	1 to 5
Network instance name	1

Limits

- A limited number of ENIs can be created for one account in each region. For more information, see the ENI limits section of Limits.
- The ECS instance and the secondary ENI you want to attach must be in the same zone and region, but can belong to different VSwitches and security groups.
- The number of secondary ENIs that can be attached to an ECS instance depends on the instance type.
- Only I/O-optimized instance types support ENIs.
- ECS instances in a classic network do not support ENIs.
- The instance bandwidth varies with the instance type. You cannot increase the bandwidth of an ECS instance by attaching multiple ENIs to the instance.

Console operations

You can perform the following operations in the ECS console:

- Attach an ENI.
- Create an ENI.
- Delete an ENI.
- Attach an ENI to an instance: The instance must be in the **Stopped** or **Running** state.
- Detach an ENI from an instance: The instance must be in the **Stopped** or **Running** state.
- Modify a secondary ENI: You can modify the name, security group, and description of a

secondary ENI.

- You can also view the information about the ENI that is attached to an instance by using the ECS console.

API operations

You can perform the following operations through the API:

- CreateNetworkInterface: Creates an ENI.
- DeleteNetworkInterface: Deletes an ENI.
- DescribeNetworkInterfaces: Queries ENIs.
- AttachNetworkInterface: Attaches a secondary ENI to an instance. The instance must be in the **Stopped** or **Running** state.
- DetachNetworkInterface: Detaches a secondary ENI from an instance. The instance must be in the **Stopped** or **Running** state.
- ModifyNetworkInterfaceAttribute: Modifies the name, security group, and description of an ENI.
- DescribeInstances: Queries the ENIs that are attached to ECS instances.

4.2. Create an ENI

This topic describes how to create an elastic network interface (ENI) in the ECS console. You can use an ENI to deploy a high-availability cluster, and perform low-cost failover and fine-grained network management.

Background information

You can create an ENI by using either of the following two methods:

- Attach an ENI when you create an instance. For more information, see Attach an ENI. You can attach a maximum of two ENIs. One is the primary ENI and the other is the secondary ENI. A secondary ENI created in this way will be released with the instance if it is not detached from the instance. For information about how to detach an ENI, see Detach an ENI from an instance.
- Create a separate ENI. The created ENI can be attached to an instance. For more information, see Attach an ENI. An ENI created in this way can only be used as a secondary ENI.

Limits

Before you create an ENI, note the following limits:

- Each ENI must be in a VSwitch of a VPC.
- Each ENI must belong to at least one security group.

Prerequisites

- A VPC and a VSwitch are created in the VPC.
- A security group is created in the same VPC.

Procedure

To create an ENI, follow these steps:

1.

2.
3.
4. Click **Create ENI**.
5. In the displayed dialog box, complete the following configurations:
   i. **Network Interface Name**: Enter a name for the ENI.
   ii. **VPC**: Select a VPC. When you attach an ENI to an instance, they must be in the same VPC.

   > Note After an ENI is created, you cannot change the VPC.

   iii. **VSwitch**: Select a VSwitch. When you attach an ENI to an instance, they must be in the same zone, but they do not have to be in the same VSwitch.

   > Note After an ENI is created, you cannot change the VSwitch.

   iv. **Primary Private IP**: Specify an IPv4 address as the private IP address of the ENI. The IPv4 address must be available in the CIDR block of the specified VSwitch. If you do not specify one, a private IP address is automatically assigned to your ENI after the ENI is created.
   v. **Security Group**: Select a security group in the selected VPC.
   vi. **Description**: Optional. Enter a description for the ENI.
   vii. Click **OK**.

On the **Network Interfaces** page, refresh the table. When the new ENI is in the **Available** state, it is created.

What to do next

After you create an ENI, you can:

- Attach an ENI to an instance.
- Modify attributes of the ENI.
- Delete the ENI.

4.3. Attach an ENI

This topic describes how to attach an Elastic Network Interface (ENI). Specifically, you either attach an ENI when you create an ECS instance, or you can alternatively create an ENI separately and then attach it to an ECS instance. Attaching an ENI allows you to build clusters with higher availability, perform failovers with lower costs, and manage your network with finer granularity.

Attach an ENI when you create an ECS instance

Limits

If you attach a secondary ENI, as opposed to a primary ENI, to an ECS instance and do not detach it from the ECS instance, the secondary ENI will be released when you release the ECS instance. For more information, see Detach an ENI from an instance.

Procedure

Before you begin, make sure that you have created an ECS instance. For the specific procedure, see Step 2: Create an instance.

When you attach an ENI to an ECS instance during the process of creating an ECS instance, configure the following parameters:

1. Basic configurations
   - Region: ENIs are supported in all regions.
   - Instance type: Select an I/O-optimized instance type that supports ENIs. For more information, see Instance type families.
   - Image: The following image types support ENIs without any manual configuration required:
     - CentOS 7.3 64-bit
     - CentOS 6.8 64-bit
     - Windows Server 2016 Datacenter Edition 64-bit
     - Windows Server 2012 R2 Datacenter Edition 64-bit

     > **Note**
     >
     > For other image types, after you create an ECS instance, you must configure the ENI to enable the instance to support ENIs.

2. Networking
   - Network: Select **VPC**, and then select a VPC and VSwitch that you created.
   - ENI: Click **Add ENI** to attach the target ENI. The ENI and the instance must belong to the same VSwitch.

     > **Note** When you create an instance in the ECS console, you can attach up to two ENIs to the instance. One is the primary ENI, and the other is the secondary ENI. You can attach more secondary ENIs to the instance by using one of the following two methods:
     >
     > - Create an ENI in the ECS console, and then attach the ENI to the instance.
     > - Call the API action AttachNetworkInterface to attach more ENIs to the instance.

Attach an ENI to an existing ECS instance

Limits

- The ENI can only be attached to the existing ECS instance as a secondary ENI, rather than a primary ENI.
- The ENI must be in the **Available** state.
- The ECS instance must be in the **Stopped** or **Running** state.
- The ENI can only be attached to a VPC ECS instance. The ENI and the instance must be in the same VPC.
- The VSwitch to which the ENI belongs must be in the same zone as the ECS instance to which

the ENI is attached.

- The ENI can only be attached to an I/O-optimized instance.
- One ENI can be attached to only one VPC ECS instance, but one instance can be attached with multiple ENIs. For more information, see Instance type families.

Prerequisites

- An ENI is created. For more information, see Create an ENI.
- The ENI is in the **Available** state.
- The instance can be attached with secondary ENIs and is in the **Stopped** or **Running** state. For more information, see Instance type families.

Procedure

1.
2.
3.
4. Locate an available ENI, and then click **Bind to Instance**.
5. In the displayed dialog box, select the target instance, and then click **OK**.

Refresh the list. When the ENI is in the **Bound** state, the ENI is attached to the instance.

> **Notice** If the last time your instance was started or restarted is earlier than April 1, 2018, then you must use the ECS console or call the API action RebootInstance to Restart the instance, as opposed to logging on to the instance to restart it. Otherwise, the ENI cannot be attached to the instance.

What to do next

After you attach an ENI to an ECS instance, you can perform the following operations:

- Detach the ENI from the instance or Delete the ENI.
- Configure the ENI if the image cannot identify the ENI.

4.4. Configure an ENI

You may need to manually configure elastic network interfaces (ENIs) for some images used by your instances so that the bound ENIs can be identified by the operating systems. This topic describes how to configure ENIs.

Prerequisites

The ENIs are bound to ECS instances. For more information about how to bind an ENI to an ECS instance, see Attach an ENI.

Context

You do not need to configure ENIs for the following versions of images used by your instances:

- CentOS 7.3 64-bit
- CentOS 6.8 64-bit
- Windows Server 2008 R2 and later

If your instances are running images that are not included in the preceding list, you must manually configure ENIs for the images.

Procedure

1. View and record information of the ENIs. For more information, see Preparations.
2. Choose one of the following methods to configure the ENIs based on your instance operating systems:
   - Alibaba Cloud Linux 2: Configure ENIs for instances that run Alibaba Cloud Linux 2
   - CentOS or Red Hat: Configure ENIs for instances that run CentOS or Red Hat
   - Ubuntu or Debian: Configure ENIs for instances that run Ubuntu or Debian
   - SUSE or openSUSE: Configure ENIs for instances that run SUSE or openSUSE
3. Configure routes for ENIs. For more information, see Configure routes for ENIs.

Preparations

You must query the attributes of each ENI, including the primary private IP address, subnet mask, default route, and MAC address. You must also pay attention to the mapping between the ENI name and the MAC address in subsequent configurations.

1. Remotely connect to an ECS instance. For more information, see Overview.
2. Query the attributes of each ENI, including the primary private IP address, subnet mask, default route, and MAC address.
   - Method 1: Query the attributes in the ECS console.
     a. Log on to the ECS console.
     b. In the left-side navigation pane, choose **Network & Security > ENIs**.
     c. On the **Network Interfaces** page, find the ENIs whose attributes you want to query and view their primary private IP addresses and MAC addresses in the **Primary Private IP Address** and **Type/MAC Address(All)** columns.
   - Method 2: Run the **curl** command to query the attributes from the instance metadata. For more information, see Metadata.

```
[root@LocalHost ~]# curl http://100.100.100.200/latest/meta-data/network/interfaces/macs/
00:16:3e:12:e7:**/
00:16:3e:12:16:**/
[root@LocalHost ~]# curl http://100.100.100.200/latest/meta-data/network/interfaces/macs/00
:16:3e:12:e7:**/netmask
255.255.255.0
[root@LocalHost ~]# curl http://100.100.100.200/latest/meta-data/network/interfaces/macs/00
:16:3e:12:e7:**/primary-ip-address
10.0.0.20
[root@LocalHost ~]# curl http://100.100.100.200/latest/meta-data/network/interfaces/macs/00
:16:3e:12:e7:**/gateway
10.0.0.253
```

   - Method 3: Call the DescribeNetworkInterfaces operation to query the attributes.

In this example, the following ENI information is returned:

```
eth1 10.0.0.20/24 10.0.0.253 00:16:3e:12:e7:**
eth2 10.0.0.21/24 10.0.0.253 00:16:3e:12:16:**
```

Configure ENIs for instances that run Alibaba Cloud Linux 2

eth1 is used in the following example. If you want to configure another ENI, modify the ENI ID.

1. Open the configuration file of the ENI.

   ```
   vi /etc/systemd/network/60-eth1.network
   ```

2. Press the /key to enter the edit mode and add the configuration information to the ENI configuration file.Choose one of the following configuration information sets based on your actual needs.
   - Scenario 1: Allocate a dynamic IP address for the ENI over DHCP.

     Example:

     ```
     [Match]
     Name=eth1 # Specify the ENI to be configured.

     [Network]
     DHCP=yes

     [DHCP]
     UseDNS=yes
     ```

   - Scenario 2: Allocate a static IP address for the ENI.

     Example:

     ```
     [Match]
     Name=eth1 # Specify the ENI to be configured.

     [Network]
     Address=192.168. **. **/24 # Specify the static IP address and subnet mask to be allocated.
     ```

   Press the *Esc* key, enter `:wq` , and then press the Enter key to save the file and exit the edit mode.

3. Check the ENI configuration file and confirm the modification.

   ```
   cat /etc/systemd/network/60-eth1.network
   ```

4. Restart the network service.

   ```
   systemctl restart systemd-networkd
   ```

Configure ENIs for instances that run CentOS or Red Hat

eth1 is used in the following example. If you want to configure another ENI, modify the ENI ID.

Method 1: Use the multi-nic-util tool.

> Note You can download and install the multi-nic-util tool on some CentOS instances to automatically configure ENIs. multi-nic-util supports only images later than CentOS 6.8 or CentOS 7.3.

1. Download the multi-nic-util tool.

```
wget https://image-offline.oss-cn-hangzhou.aliyuncs.com/multi-nic-util/multi-nic-util-0.6.tgz
```

2. Decompress the package and install the multi-nic-util tool.

```
tar -zxvf multi-nic-util-0.6.tgz
cd multi-nic-util-0.6
bash install.sh
```

3. Restart ENI.

```
systemctl restart eni.service
```

Method 2: Manually configure the ENI.

1. Open the configuration file of the ENI.

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

2. Press the /key to enter the edit mode and add the configuration information to the ENI configuration file.Example:

```
DEVICE=eth1  #Specify the ENI to be configured.
BOOTPROTO=dhcp
ONBOOT=yes
TYPE=Ethernet
USERCTL=yes
PEERDNS=no
IPV6INIT=no
PERSISTENT_DHCLIENT=yes
HWADDR=00:16:3e:12:e7:** #Specify this address as the queried MAC address of the ENI.
DEFROUTE=no  #This indicates that the ENI is not the default route. To prevent the active default route of the ECS instance from being changed when you start the ENI by running the ifup comman d, do not set eth1 to the default route.
```

Press the *Esc* key, enter `:wq` , and then press the Enter key to save the file and exit the edit mode.

3. Check the ENI configuration file and confirm the modification.

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

4. Run the `service network restart` or `systemctl restart network` command to restart the network service.

> **Note** If you want to create custom images after ENIs are configured in your instance, you must first run the **/etc/eni_utils/eni-cleanup** command to remove network configurations under */etc/udev/rules.d/70-persistent-net.rules* and */etc/sysconfig/network-scripts/*.

Configure ENIs for instances that run Ubuntu or Debian

You can perform the following operations on instances that run Ubuntu 14.04, Ubuntu 16.04, or Debian:

1. Open the configuration file of an ENI.

```
vi /etc/network/interfaces
```

2. Press the **/**key to enter the edit mode and add the configuration information to the ENI configuration file.eth1 is used in this example:

```
auto eth0
iface eth0 inet dhcp

auto eth1 #Specify the ENI to be configured.
iface eth1 inet dhcp
```

Press the *Esc* key, enter `:wq` , and then press the Enter key to save the file and exit the edit mode.

3. Check the ENI configuration file and confirm the modification.

```
cat /etc/network/interfaces
```

4. Run the `service networking restart` or `systemctl restart networking` command to restart the network service.

You can perform the following operations on instances that run Ubuntu 18.04:

1. Create and edit the configuration file of an ENI.eth1 is used in this example:

```
vi /etc/netplan/eth1-netcfg.yaml
```

2. Press the **/**key to enter the edit mode and add the configuration information to the ENI configuration file.eth1 is used in this example:

```
network:
 version: 2
 renderer: networkd
 ethernets:
  eth1:
   dhcp4: yes
   dhcp6: no
```

Press the *Esc* key, enter `:wq`, and then press the Enter key to save the file and exit the edit mode.

> **Note** Take note of the following items when you edit the configuration file:
>
> - The configuration file is in the `YAML` format. Therefore, you must follow the `YAML` syntax rules when you configure the file.
> - You cannot use tabs for indentation in `YAML` files. Use the space instead.
> - We recommend that you copy content in the default */etc/netplan/99-netcfg.yaml* configuration file to avoid format issues.

3. Check the ENI configuration file and confirm the modification.

```
cat /etc/netplan/eth1-netcfg.yaml
```

4. Run the `netplan apply` command to validate the configuration.

Configure ENIs for instances that run SUSE or openSUSE

eth1 is used in the following example. If you want to configure another ENI, modify the ENI ID.

1. Open the configuration file of the ENI.

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

2. Press the /key to enter the edit mode and add the configuration information to the ENI configuration file.

```
BOOTPROTO='dhcp4'
STARTMODE='auto'
USERCONTROL='no'
```

Press the *Esc* key, enter `:wq`, and then press the Enter key to save the file and exit the edit mode.

3. Check the ENI configuration file and confirm the modification.

```
cat /etc/sysconfig/network/ifcfg-eth1
```

4. Run the `service network restart` or `systemctl restart network` command to restart the network service.

Configure routes for ENIs

1. Start ENIs.
   i. Run the `ifup [ENI name]` command to start the dhclient process, and initiate a DHCP request.

   ```
   ifup eth1
   ifup eth2
   ```

   ii. Check the allocation of IP addresses. The result must be the same as the ENI information that you queried in the "Preparations" section.

   ```
   [root@ecshost~ ]# ip a
   1: lo:  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:  mtu 1500 qdisc pfifo_fast state UP qlen 1000
   link/ether 00:16:3e:0e:16:** brd ff:ff:ff:ff:ff:ff
   inet 10.0.0.19/24 brd 10.0.0.255 scope global dynamic eth0
   valid_lft 31506157sec preferred_lft 31506157sec
   3: eth1:  mtu 1500 qdisc pfifo_fast state UP qlen 1000
   link/ether 00:16:3e:12:e7:** brd ff:ff:ff:ff:ff:ff
   inet 10.0.0.20/24 brd 10.0.0.255 scope global dynamic eth1
   valid_lft 31525994sec preferred_lft 31525994sec
   4: eth2:  mtu 1500 qdisc pfifo_fast state UP qlen 1000
   link/ether 00:16:3e:12:16:** brd ff:ff:ff:ff:ff:ff
   inet 10.0.0.21/24 brd 10.0.0.255 scope global dynamic eth2
   valid_lft 31526009sec preferred_lft 31526009sec
   ```

2. Set the metric parameter of the default route for each ENI in the route table.
   i. Set the metric parameter.

   ```
   ip -4 route add default via 10.0.0.253 dev eth1 metric 1001
   ip -4 route add default via 10.0.0.253 dev eth2 metric 1002
   ```

   The preceding commands set the metric parameter of eth1 and eth2 to the following values:

   ```
   eth1: gw: 10.0.0.253 metric: 1001
   eth2: gw: 10.0.0.253 metric: 1002
   ```

ii. Check whether the configuration succeeds. Pay attention to whether information of the Gateway and Metric columns is the same as the configured information.

```
[root@ecshost~ ]# route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 10.0.0.253 0.0.0.0 UG 0 0 0 eth0
0.0.0.0 10.0.0.253 0.0.0.0 UG 1001 0 0 eth1
0.0.0.0 10.0.0.253 0.0.0.0 UG 1002 0 0 eth2
10.0.0.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
10.0.0.0 0.0.0.0 255.255.255.0 U 0 0 0 eth1
10.0.0.0 0.0.0.0 255.255.255.0 U 0 0 0 eth2
169.254.0.0 0.0.0.0 255.255.0.0 U 1002 0 0 eth0
169.254.0.0 0.0.0.0 255.255.0.0 U 1003 0 0 eth1
169.254.0.0 0.0.0.0 255.255.0.0 U 1004 0 0 eth2
```

3. Create route tables.

i. Create route tables.

```
ip -4 route add default via 10.0.0.253 dev eth1 table 1001
ip -4 route add default via 10.0.0.253 dev eth2 table 1002
```

> **Note** We recommend that you keep the names of the route tables the same as the metric values of the default routes. *1001* and *1002* are used in this example.

ii. Check whether the route tables are created.

```
[root@ecshost~ ]# ip route list table 1001
default via 10.0.0.253 dev eth1
[root@ecshost~ ]# ip route list table 1002
default via 10.0.0.253 dev eth2
```

4. Configure policy-based routes.

i. Create policy-based routes.

```
ip -4 rule add from 10.0.0.20 lookup 1001
ip -4 rule add from 10.0.0.21 lookup 1002
```

ii. View routing rules.

```
[root@ecshost~ ]# ip rule list
0: from all lookup local
32764: from 10.0.0.21 lookup 1002
32765: from 10.0.0.20 lookup 1001
32766: from all lookup main
32767: from all lookup default
```

What's next

After the ENIs are configured, you can perform the following operations:

- Assign secondary private IP addresses
- Modify an ENI
- Detach an ENI from an instance
- 删除弹性网卡

Related information

- DescribeNetworkInterfaces

4.5. Assign secondary private IP addresses

You can assign one or more secondary private IP addresses to a primary or secondary elastic network interface (ENI). This allows you to optimize the usage of VPC-type instances and divert traffic during a failover.

multiple private IP addresses ENI bind an ENI ECS Alibaba Cloud

Prerequisites

- The instance type of your instance supports multiple secondary private IP addresses. The number of private IP addresses that can be assigned to a single ENI depends on the instance type of the instance to which the ENI is bound. For more information, see Instance families.
- When you assign a secondary private IP address to a primary ENI, the instance to which the primary ENI is bound is in the **Running** or **Stopped** state.

Context

Secondary private IP addresses are suitable for the following scenarios:

- Optimization of application usage

  If your ECS instance hosts multiple applications, you can assign multiple secondary private IP addresses to the corresponding ENIs. This way, each application uses a separate IP address for services, which optimizes the usage of the ECS instance.

- Optimization of failover

  If an instance fails, you can unbind ENIs from the instance and bind the ENIs to another instance to divert traffic to that instance. This can ensure service continuity.

Take note of the following limits when you assign secondary private IP addresses:

- Each security group of the VPC type can contain a maximum of 2,000 private IP addresses. This quota is shared among all primary and secondary ENIs in the security group.
- You can assign a maximum of 20 private IP addresses to an ENI. The actual number depends on the instance type of the instance to which the ENI is bound.
  - If the ENI is in the **Available** state, you can assign a maximum of 10 private IP addresses to the ENI.
  - If the ENI is in the **Bound** state, the number of private IP addresses that can be assigned to the ENI is subject to the instance type of the instance.

Description

This section applies to both primary and secondary ENIs.

1. In the ECS console, assign a secondary private IP address to an ENI. For more information, see Assign secondary private IP addresses.
2. In the instance to which the ENI is bound, configure the assigned secondary private IP address.

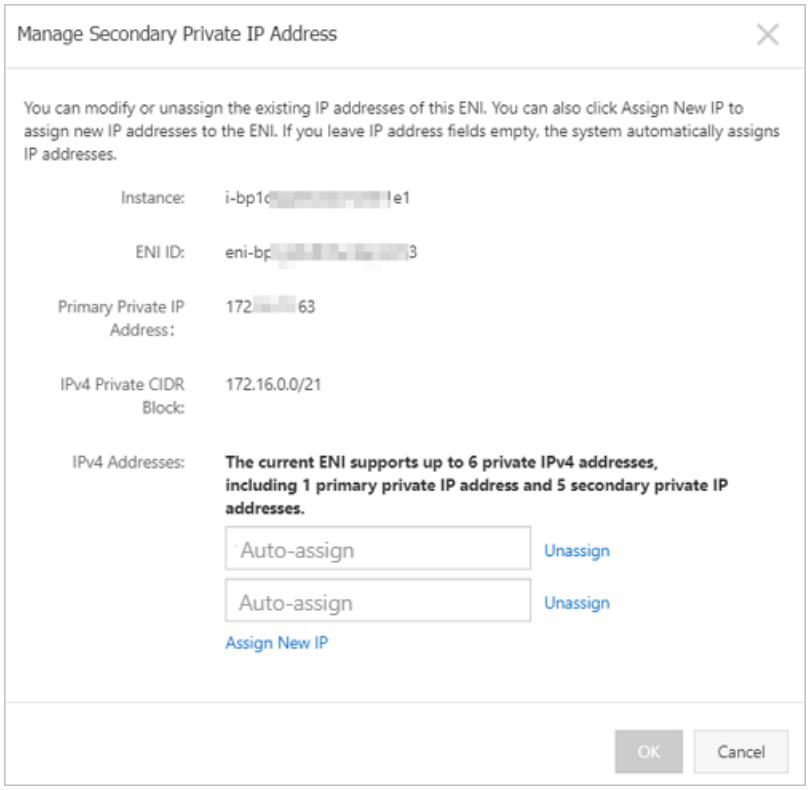
   > **Note** If the ENI is a secondary ENI and is not bound to an instance, bind the ENI to an instance and configure the assigned secondary private IP address in the instance. For more information, see Attach an ENI.

   - For Windows instances, see Configure a secondary private IP address in a Windows instance.
   - For Linux instances, see Configure a secondary private IP address in a Linux instance.

Assign secondary private IP addresses

1. Log on to the ECS console.
2. In the left-side navigation pane, choose **Network & Security** > **ENIs**.
3. In the top navigation bar, select a region.
4. On the **Network Interfaces** page, find the ENI to which you want to assign a secondary private IP address, and then click **Manage Secondary Private IP Address** in the **Actions** column.
5. In the **Manage Secondary Private IP Address** dialog box, click **Assign New IP**.
   - Auto-assign: Keep the default setting. The system randomly assigns IPv4 addresses from the range of **IPv4 Private CIDR Block**.
   - Manual-assign: Manually enter secondary private IP addresses within the range of **IPv4 Private CIDR Block**.

   > **Note** After an IP address is assigned, you can click **Assign New IP** again to assign another private IP address.



6. Click **OK**.

> **Note** After you complete automatic assignment of secondary private IP addresses, click **Manage Secondary Private IP Address** in the **Actions** column corresponding to the ENI to view the assigned secondary private IP addresses.

Configure a secondary private IP address in a Windows instance

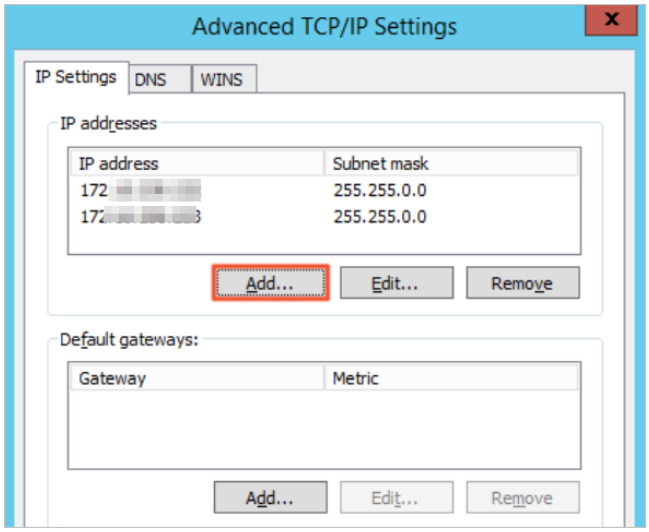
1. Remotely connect to an ECS instance. For more information, see Overview.
2. Query the subnet mask and default gateway of the instance.
   i. Open **Command Prompt** or **Windows PowerShell**.
   ii. Enter the `ipconfig` command to query the subnet mask and default gateway of the instance.

```
PS C:\Users\Administrator> ipconfig
Windows IP Configuration
Ethernet adapter Ethernet:
  Connection-specific DNS Suffix . . . . . :
  Link-local IPv6 Address. . . . . : fe80::6c64:1601:****:****
  IPv4 Address . . . . . : 172. **. **.133
  Subnet Mask ..... : 255.255. **. **
  Default Gateway. . . . . : 172. **. **.253
```

3. Open **Network and Sharing Center**.
4. Click **Change adapter settings**.

5. Double-click the current network connection name and click **Properties**.
6. Double-click **Internet Protocol Version 4 (TCP/IPv4)**.
7. Select **Use the following IP address** and click **Advanced**.
8. In the **Advanced TCP/IP Settings** dialog box, set IP addresses.
   i. In the **IP addresses** section, click **Add...** and enter the assigned IP address in the **IP address** field and the queried subnet mask in the **Subnet mask** field.

      You can add multiple IP addresses to the same adapter.



   ii. In the **Default gateways** section, click **Add...** and enter the queried subnet mask in the **Subnet mask** field.
9. Click **OK**.

Configure a secondary private IP address in a Linux instance

In the following example, the *eth0* primary ENI is used. If you are using a secondary ENI, modify the ENI ID.

1. Remotely connect to an ECS instance. For more information, see Overview.
2. Run the `ipconfig` command to query the subnet mask and default gateway of the instance.

```
[root@ecs ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 172.16. **.**  netmask 255.255. **.**  broadcast 172.16. **.**
      inet6 fe80::216:3eff:****:****  prefixlen 64  scopeid 0x20<link>
      ether 00:16:3e:0e:**:**  txqueuelen 1000  (Ethernet)
      RX packets 27146  bytes 39146111 (37.3 MiB)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 6038  bytes 509398 (497.4 KiB)
      TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

> **Note** If some Linux distributions do not support the `ifconfig` command, you can run the `ip addr show` command.

3. Configure a secondary private IP address based on the operating system of your instance.
   - RHEL series: CentOS 6, CentOS 7, Red Hat 6, Red Hat 7, or Alibaba Cloud Linux 2
     a. Open the network configuration file.
        - If you configure a single IP address, run the `vi /etc/sysconfig/network-scripts/ifcfg-eth0:0` command to add the following configuration items:

          ```
          DEVICE=eth0:0
          TYPE=Ethernet
          BOOTPROTO=static
          ONBOOT=yes
          IPADDR=<IPv4 address 1>
          NETMASK=<IPv4 mask>
          GATEWAY = <IPv4 gateway>
          ```

        - If you configure multiple IP addresses, run the `vi /etc/sysconfig/network-scripts/ifcfg-eth0:1` command to add the following configuration items:

          ```
          DEVICE=eth0:1
          TYPE=Ethernet
          BOOTPROTO=static
          ONBOOT=yes
          IPADDR = <IPv4 address 2>
          NETMASK=<IPv4 mask>
          GATEWAY = <IPv4 gateway>
          ```

     b. Run the `service network restart` or `systemctl restart network` command to restart the network service.
   - Debian series: Ubuntu 14, Ubuntu 16, Debian 8, or Debian 9

a. Run the `vi /etc/network/interfaces` command to open the network configuration file and add the following configuration items:

```
auto eth0:0
iface eth0:0 inet static
address <IPv4 address 1>
netmask <IPv4 mask>
gateway <IPv4 gateway>

auto eth0:1
iface eth0:1 inet static
address <IPv4 address 2>
netmask <IPv4 mask>
gateway <IPv4 gateway>
```

b. Run the `service networking restart` or `systemctl restart networking` command to restart the network service.

- SLES series: SUSE 11, SUSE 12, or openSUSE 42

a. Run the `vi /etc/sysconfig/network/ifcfg-eth0` command to open the network configuration file and add the following configuration items:

```
IPADDR_0 = <IPv4 address 1>
NETMASK_0 = <Subnet prefix length>
LABEL_0='0'

IPADDR_1 = <IPv4 address 2>
NETMASK_1 = <Subnet prefix length>
LABEL_1='1'
```

b. Run the `service network restart` or `systemctl restart network` command to restart the network service.

Related information

- AssignPrivateIpAddresses

4.6. Revoke secondary private IP addresses

You can revoke one or more secondary private IP addresses from an Elastic Network Interface (ENI) when the ENI no longer needs them. You cannot revoke the primary private IP address.

Prerequisites

Before you revoke secondary private IP addresses from an ENI, make sure that the following requirements have been met.

- At least one secondary private IP address has been assigned to the ENI. For more information about how to assign secondary private IP addresses to an ENI, see Assign secondary private IP addresses.
- The ENI must be in the **Available** (`Available`) or **Bound** (`InUse`) state.
- If you want to revoke multiple secondary private IP addresses from a primary ENI, the ECS instance to which the primary ENI is bound must be in the **Running** (`Running`) or **Stopped** (`Stopped`) state.

Context

Limits: The primary private IP address assigned to an ENI cannot be revoked.

Procedure

1. Log on to the ECS console.
2. In the left-side navigation pane, choose **Network & Security** > **ENIs**.
3. In the top navigation bar, select a region.
4. On the **Network Interfaces** page, find the target ENI. Click **Manage Secondary Private IP Address** in the **Actions** column.
5. In the **Manage Secondary Private IP Address** dialog box that appears, click **Unassign** next to the secondary private IP address that you want to revoke. You can revoke multiple secondary private IP addresses by clicking Unassign next to them.
6. Click **OK**.

Related information

- UnassignPrivateIpAddresses

4.7. Modify an ENI

This topic describes how to modify primary and secondary Elastic Network Interfaces (ENIs). You can change the security group of a primary ENI by moving its bound ECS instance to a different security group. You can modify the attributes of a secondary ENI such as the name, associated security group, and description.

Context

Before you can modify the security group to which an ENI belongs, the ENI and its bound ECS instance must meet the following requirements. For more information, see Overview.

- An ECS instance cannot belong to both basic and advanced security groups at the same time.
- An ENI cannot belong to both basic and advanced security groups at the same time.
- An ENI can only be bound to an ECS instance when they belong to the same type of security groups.

Modify a primary ENI

The primary ENI and the secondary ENIs of an ECS instance can belong to different security groups. If you move the ECS instance to a different security group, the primary ENI will also be associated with this security group, but the secondary ENIs will remain in the previous security group. Follow these steps to modify a primary ENI:

1. Log on to the ECS console.
2. In the left-side navigation pane, choose **Network & Security > Security Groups**.
3. In the top navigation bar, select a region.
4. Find the target security group and click **Manage Instances** in the **Actions** column.
5. On the **Instances in Security Group** page, change the security group that the primary ENI is associated with:
   - Follow these steps to add the primary ENI to a new security group:
     a. In the upper-right corner of the **Instances in Security Group** page, click **Add Instance**.
     b. In the **Add Instance** dialog box that appears, select the ID of the instance to which the primary ENI is bound. Click **OK**.

        The primary ENI is added to the new security group along with the corresponding ECS instance.
   - Follow these steps to remove the primary ENI from its current security group:
     a. On the **Instances in Security Group** page, select one or more instances and click **Remove from Security Group**.
     b. In the **Remove ECS Instance from Security Group** message that appears, click **OK**.

        The primary ENI is removed from the current security group along with the corresponding ECS instance. Note that the primary ENI and the ECS instance must belong to at least one security group.
6. Go back to the homepage of the ECS console. In the left-side navigation pane, choose **Network & Security > ENIs**.
7. Find the target primary ENI and verify whether the settings have taken effect.

Modify a secondary ENI

Follow these steps to modify the name, security group, or description of a secondary ENI: Make sure that you have created a secondary ENI before you proceed. For more information, see Create an ENI.

1. Log on to the ECS console.
2. In the left-side navigation pane, choose **Network & Security > ENIs**.
3. In the top navigation bar, select a region.
4. Find the target secondary ENI and click **Modify** in the Actions column.
5. In the **Modify** dialog box that appears, modify the ENI attributes as follows:
   - **ENI Name**: Specify a new ENI name based on the naming conventions displayed under this field.
   - **Security Group**: Select a new security group for the ENI, or remove the ENI from a security group. Note that the ENI must be associated with at least one security group.
   - **Description**: Modify the description based on the instructions displayed under this field.
6. Click **OK**.

Related information

References

- ModifyNetworkInterfaceAttribute

4.8. Detach an ENI from an instance

You can only detach a secondary ENI from an instance. You cannot detach the primary ENI.

Limits

Before you detach a secondary ENI from an instance, note the following limits:

- The secondary ENI must be in the **Bound** state.
- The instance to which the ENI belongs must be in the **Stopped** or **Running** state.

Prerequisites

The secondary ENI is attached to an instance. Before you detach a secondary ENI from an instance, the instance must be in the **Stopped** or **Running** state.

Procedure

To detach a secondary ENI from an instance, follow these steps:

1.
2.
3.
4. Find the target ENI, and in the **Actions** column, click **Unbind**.
5. In the displayed dialog box, confirm the information, and then click **OK**.

After, in the **Network Interfaces** page, refresh the table. When the selected ENI is in the **Available** state, it is detached from the instance.

What to do next

After an ENI is detached from an instance, you can:

- Attach the ENI to another instance.
- Delete the ENI.
- Modify attributes of the ENI.

5.Change the VPC of an ECS instance

This topic describes how to migrate a VPC-type ECS instance from one virtual private cloud (VPC) to another VPC. If you select an inappropriate VPC when you create an ECS instance or if you want to replan the network, you can use this feature to change the VPC of the instance.

Prerequisites

- The instance is in the Stopped state. For more information, see Stop an instance.
- The instance is not added as a backend server of an SLB instance. For more information, see Remove a backend server.
- The secondary elastic network interfaces (ENIs) bound to the instance are unbound. Multiple secondary private IP addresses assigned to the ENIs are revoked. For more information, see Detach an ENI from an instance and Revoke secondary private IP addresses.
- The destination VPC, VSwitch, and security groups are created and available.

Scenarios

- You want to replan the VPCs of your ECS instances because the original VPCs are unable to keep up with the growing needs of your business.
- In the early business stage, only one VPC was planned. Different projects and usage environments share this VPC, which leads to risks in data operations. You want to use different VPCs for different projects and environments.
- Your ECS instances are deployed in the default VPCs in different accounts. Therefore, connectivity between instances across Alibaba Cloud accounts cannot be implemented due to IP address conflicts. In this case, you must change the VPCs of the ECS instances and resolve the address conflict before you interconnect the instances across Alibaba Cloud accounts.

Limits

- The instance cannot be used in other cloud services. For example, the instance cannot be in the process of being migrated or having its VPC changed, or the databases deployed on the instance cannot be managed by Data Transmission (DTS).
- After the VPC is changed, the new VSwitch of the instance must be in the same zone as the original VSwitch.
- You can select up to five security groups in each destination VPC for an instance. However, the destination security groups must be of the same type, basic security group or advanced security group.
- If advanced VPC features are enabled for the destination VPC, you cannot migrate instances of some instance families to the destination VPC. For more information, see Instance families that do not support advanced VPC features.
- You can change the VPCs of up to 20 instances at a time.
- After you change the VPC of an instance, the instance cannot communicate with other instances in the original VPC. For information about how to communicate with other instances, see What is Express Connect?.
- The cut-through mode or multi-EIP to ENI mode cannot be enabled for the instance.
- The instance cannot be associated with a high-availability virtual IP address (HaVip).
- The VSwitch of the instance cannot be associated with a custom route table.

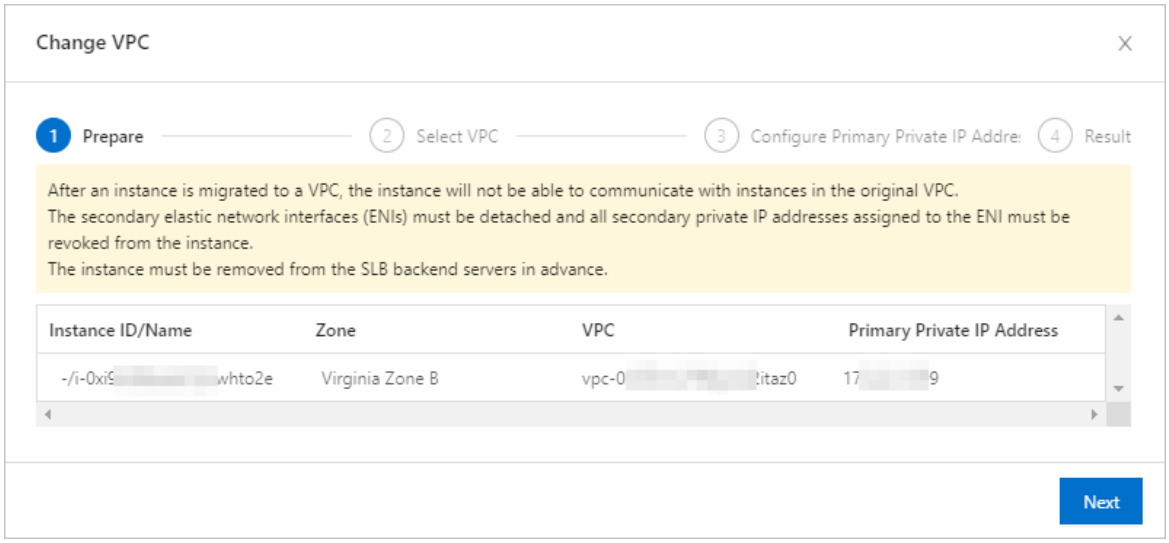
- Global Accelerator (GA) cannot be activated for the instance.

Procedure

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 a region.
4. Change the VPC of one or more ECS instances at a time.
   - Change the VPC of a single instance

     Find the target ECS instance and choose **More > Network and Security Group > Change VPC** in the **Actions** column.
   - Change the VPCs of multiple ECS instances at a time

     Select the instances whose VPCs you want to change, and choose **More > Network and Security Group > Change VPC** in the lower part of the page.
5. In the **Change VPC** wizard, follow the instructions to change the VPCs of the ECS instances.



   i. In the **Prepare** step, check the network information and precautions and click **Next**.

   ii. In the **Select VPC** step, configure the **Destination VPC**, **Destination VSwitch**, and **Destination Security Group** parameters and click **Next**.

   iii. (Optional)In the **Configure Primary Private IP Address** step, specify a primary private IP address for each of the selected instances to use in the destination VPC.
      - The primary private IP address must be within the CIDR block of the destination VSwitch.
      - If you do not manually set the primary private IP address, it is automatically assigned by the system.

   iv. Click **OK**.

After the change is complete, you can click the instance ID to view the new VPC and VSwitch in the **Configuration Information** section of the **Instance Details** page.

Related information

- ModifyInstanceVpcAttribute

6.Configure NIC multi-queue

NIC multi-queue enables an ECS instance to use more than one NIC queues to increase the packet forwarding rate. If performance bottlenecks occur when vCPUs of a single instance are used to process network interrupts, you can use NIC multi-queue to distribute the network interrupts to different vCPUs to enhance network performance.

Prerequisites

- The instance type of your instance supports the NIC multi-queue feature. For more information about instance types that support NIC multi-queue, see Instance families. If the number of NIC queues is greater than 1, the NIC multi-queue feature is supported.
- Your instance uses one of the following images. The following public images provided by Alibaba Cloud support the NIC multi-queue feature. Whether images support this feature is irrelevant to the bit sizes of the operating systems.

> **Note** Even if your operating system is included in the list, public images of earlier versions may not support the NIC multi-queue feature. We recommend that you use the latest public images. If your image has the NIC multi-queue feature enabled by default, skip this topic.

Public image	NIC multi-queue supported	NIC multi-queue enabled
CentOS 6.8/6.9/7.2/7.3/7.4	Yes	Yes
Ubuntu 14.04/16.04/18.04	Yes	Yes
Debian 8.9/9.2	Yes	Yes
SUSE Linux Enterprise Server 12 SP1	Yes	Yes
SUSE Linux Enterprise Server 12 SP2	Yes	Yes
Red Hat Enterprise Linux 6.9/7.4/7.5	Yes	No
OpenSUSE 42.3	Yes	No
Alibaba Cloud Linux 2.1903	Yes	Yes
Aliyun Linux 17.1	Yes	No
Windows 2012 R2	Yes	Yes
Windows 2016	Yes	Yes

Context

NIC multi-queue is a technology that can fix the Quality of Service (QoS) issue of I/O bandwidth. The NIC multi-queue driver binds NIC queues to different cores through interrupts. This solves processing bottlenecks of single-core CPUs when network I/O bandwidth increases, and improves the packet forwarding rate and bandwidth performance. Under identical packet forwarding rate and network bandwidth conditions, the performance of two queues can be 50% to 100% higher than that of a single queue, and the performance of four queues can be even higher.

The following procedure applies only to Linux instances.

Automatic configuration

1. Remotely connect to an ECS instance. For more information, see Overview.
2. Download the script package for automatic configuration.

   ```
   wget https://image-offline.oss-cn-hangzhou.aliyuncs.com/doc/ecs_mq_20200428-1352.tgz
   ```

3. Extract the script.

   ```
   tar -xzf ecs_mq_20200428-1352.tgz
   ```

4. Change the working path.

   ```
   cd ecs_mq/
   ```

5. Start the service.

   ```
   systemctl start ecs_mq
   ```

6. Run the script.The script format varies with the image versions. For example, `bash install.sh centos 7` is suitable for CentOS 7.6 images.

   ```
   bash install.sh <System name> <Major version number of the system>
   ```

Manual configuration

CentOS 7.6 images are used in this section. The name of the primary NIC is eth0, and the name of the secondary ENI is eth1. This section describes how to manually configure NIC multi-queue.

1. Run the `ethtool -l eth0` command to check whether the primary NIC supports NIC multi-queue.

```
[root@localhost ~]# ethtool -l eth0
Channel parameters for eth0:
Pre-set maximums:
RX: 0
TX: 0
Other: 0
Combined: 2 # This value indicates that a maximum of two queues can be configured.
Current hardware settings:
RX: 0
TX: 0
Other: 0
Combined: 1 # This value indicates that one queue is in effect.
```

Note If the returned values of the two Combined fields are the same, the NIC multi-queue feature is enabled.

2. Run the `ethtool -L eth0 combined 2` command to enable the NIC multi-queue feature. This command configures the eth0 primary NIC to use two queues.

```
[root@localhost ~]# ethtool -L eth0 combined 2
```

3. Configure NIC multi-queue for the secondary ENI.

```
# Check whether the eth1 secondary ENI supports NIC multi-queue.
[root@localhost ~]# ethtool -l eth1
Channel parameters for eth1:
Pre-set maximums:
RX: 0
TX: 0
Other: 0
Combined: 4 # This value indicates that a maximum of four queues can be configured.
Current hardware settings:
RX: 0
TX: 0
Other: 0
Combined: 1 # This value indicates that one queue is in effect.
# Configure the eth1 secondary ENI to use four queues.
[root@localhost ~]# ethtool -L eth1 combined 4
```

7.Network FAQ

This topic provides answers to commonly asked questions about networks used by ECS instances.

outbound bandwidth website access failure IP address query traffic monitoring

- Network performance FAQ
  - What is the packet loss rate when instances in different regions communicate over the Internet?
  - How is the network latency while instances in the same region communicate over the internal network?
- Public bandwidth FAQ
  - What are the inbound and outbound bandwidths of ECS instances?
  - I purchased a public bandwidth of 5 Mbit/s for an ECS instance. What is the difference between the inbound and outbound bandwidths of the instance?
  - Is public bandwidth specific to each ECS instance, or is public bandwidth shared across multiple instances?
  - How is the network usage of ECS instances billed?
  - Why has 200 Kbit/s of inbound traffic already been consumed on a newly created ECS instance?
  - How do I view the Internet traffic statistics of an ECS instance?
  - Why is the bandwidth usage of my ECS instance displayed in the CloudMonitor console different from that displayed in the ECS console?
  - My ECS instance has been stopped. Why am I still being charged for its outbound traffic on a pay-as-you-go basis?
- IP addresses FAQ
  - How do I query IP addresses of ECS instances?
  - How do I disable the public NIC of an ECS instance?
- FAQ about network access and traffic direction
  - Why am I unable to access a website that is hosted on an ECS instance? A message similar to "Sorry, your access has been blocked because the requested URL may pose a security threat to the website" is displayed.
  - An unusual logon has been detected on one of my ECS instances. What do I do?
  - What is traffic scrubbing?
  - How do I cancel traffic scrubbing for an ECS instance?
  - How do I request reverse lookup for an ECS instance?
  - Can an IP address point to multiple reverse lookup domain names?
- FAQ about public IP addresses
  - Can I change the public IPv4 address of an instance after the instance has been created?
  - Why am I unable to find the option to change the public IP address of an ECS instance in the ECS console?
  - Can I change the private IP address of an instance?

  - If no public IPv4 address was assigned to an ECS instance during instance creation, how do I assign a public IP address to the instance?
- Network basic FAQ
  - What is a BGP data center?
  - What are WAN and LAN?
  - How do I express a subnet mask?
  - How do I plan subnets?
- Quota FAQ
  - How do I view the resource quota?

What is the packet loss rate when instances in different regions communicate over the Internet?

When instances in different regions communicate through Cloud Enterprise Network (CEN), they use Alibaba Cloud backbone networks to transmit data. Alibaba Cloud aims to provide network services with a P99 packet loss rate of less than 0.0001% per hour.

How is the network latency while instances in the same region communicate over the internal network?

You can achieve the minimum latency when you use instances in the same region and same zone to communicate with each other through the internal network. The P99 round-trip time (RTT) for this communication method is less than 180 us.

What are the inbound and outbound bandwidths of ECS instances?

Bandwidth type	Description
Inbound bandwidth	The bandwidth of inbound traffic for an ECS instance, such as: • Traffic that occurs when you download external resources to the ECS instance • Traffic that occurs when you upload resources to the ECS instance through an FTP client
Outbound bandwidth	The bandwidth of outbound traffic for an ECS instance, such as: • Traffic that occurs when the ECS instance provides external access • Traffic that occurs when you download resources from the ECS instance through an FTP client

I purchased a public bandwidth of 5 Mbit/s for an ECS instance. What is the difference between the inbound and outbound bandwidths of the instance?

The 5 Mbit/s that you purchased applies to the outbound bandwidth. The inbound bandwidth of the instance is capped at 10 Mbit/s.

- Outbound bandwidth is consumed when data is sent from the ECS instance. The maximum outbound bandwidth of an ECS instance is capped at 100 Mbit/s or 200 Mbit/s regardless of

whether the instance resides in a VPC or in the classic network. The maximum available outbound bandwidth value depends on the billing method of the instance.

- Inbound bandwidth is consumed when data is transferred to the ECS instance. The maximum inbound bandwidth is determined by the outbound bandwidth:
  - If the outbound bandwidth is less than 10 Mbit/s, the maximum inbound bandwidth is 10 Mbit/s.
  - If the outbound bandwidth is greater than 10 Mbit/s, the maximum inbound bandwidth is the same as the purchased outbound bandwidth.

Is public bandwidth specific to each ECS instance, or is public bandwidth shared across multiple instances?

The public bandwidth of each instance is exclusive to the instance.

How is the network usage of ECS instances billed?

For more information, see Billing methods of public bandwidth.

Why has 200 Kbit/s of inbound traffic already been consumed on a newly created ECS instance?

This traffic was generated by Address Resolution Protocol (ARP) broadcast packets. New ECS instances are assigned to large network segments. When the gateway receives an ARP request packet for the newly created ECS instance, the gateway broadcasts this packet to all ECS instances within the same network segment. If no requests for the IP address of your new ECS instance are sent, the instance will not send an ARP response packet.

How do I view the Internet traffic statistics of an ECS instance?

To view the Internet traffic statistics of an ECS instance, perform the following steps:

1. Log on to the ECS console.
2. In the top navigation bar of the ECS console, choose **Bill > User Center**.
3. In the left-side navigation pane, choose **Bill > Bill**.
4. On the Bills page, click the **Bills** tab. Specify a billing cycle, and set **Product Detail** to **Elastic Compute Service (ECS) - Pay by quantity** and **Subscription Type** to **Pay-As-You-Go**.
5. Click **Export Billing Overview (CSV)**. In the Export Billing Overview (CSV) dialog box, enter the CAPTCHA verification characters and click **OK**.
6. Open the exported CSV file to view the Internet traffic statistics of the ECS instance.

Why is the bandwidth usage of my ECS instance displayed in the CloudMonitor console different from that displayed in the ECS console?

ECS instances function as backend servers for Server Load Balancer (SLB) instances and use the Layer-7 HTTP forwarding model. In this forwarding model, SLB instances forward client requests to ECS instances, and the ECS instances use their outbound bandwidth to return responses to the corresponding users. The bandwidth consumed by these responses is not displayed in the ECS console, but the traffic generated by the responses is counted towards the outbound traffic of the SLB instances and displayed in the CloudMonitor console. Therefore, the bandwidth usage of your ECS instance displayed in CloudMonitor is different from that displayed in the ECS console.

My ECS instance has been stopped. Why am I still being charged for its outbound traffic on a pay-as-you-go basis?

- Problem description: Your ECS instance is in the **Stopped** state when viewed from the ECS console, but is in the **Cleaning** state when viewed from the Anti-DDoS Basic console. You are charged for outbound traffic from the instance on a pay-as-you-go basis every hour.
- Cause: HTTP flood protection is enabled for the ECS instance. When HTTP flood protection is enabled, the security mechanism sends probe packets to potential attack sources, generating a large volume of outbound traffic.
- Solution: Disable HTTP flood protection for the ECS instance.

How do I query IP addresses of ECS instances?

- Linux instance

  Run the `ifconfig` command to view NIC information. You can view the IP addresses, subnet masks, gateways, DNS servers, and MAC addresses in the command output.

- Windows instance

  In Command Prompt, run the `ipconfig /all` command to view NIC information. You can view the IP addresses, subnet masks, gateways, DNS servers, and MAC addresses in the command output.

How do I disable the public NIC of an ECS instance?

- Linux instance
  i. Run the `ifconfig` command to view the public NIC name of the instance.
  ii. Run the `ifdown` command to disable the public NIC. For example, if the name of the public NIC is `eth1`, enter `ifdown eth1`.

  > **Note** You can also run the **ifup** command to re-enable the NIC. For example, if the name of the public NIC is `eth1`, enter `ifup eth1`.

- Windows instance
  i. In Command Prompt, run the `ipconfig` command to view information about the public NIC.
  ii. Open the **Control Panel** and click View network status and tasks under Network and Internet. In the **Network and Sharing Center** window that appears, click **Change adapter settings** in the left-side navigation pane to disable the public NIC.

Why am I unable to access a website that is hosted on an ECS instance? A message similar to "Sorry, your access has been blocked because the requested URL may pose a security threat to the website" is displayed.

- Problem description: When you access a website built on an ECS instance, you are prompted with a message similar to "Sorry, your access has been blocked because the requested URL may pose a security threat to the website."
- Cause: Web Application Firewall (WAF) has identified your access to the requested URL as an attack and has blocked your access.

- Solution: Add the source public IP address that you use to access the website to the WAF whitelist. For more information, see Avoid Anti-DDoS Basic false positives by using a whitelist.

An unusual logon has been detected on one of my ECS instances. What do I do?

Perform the following operations to solve the problem:

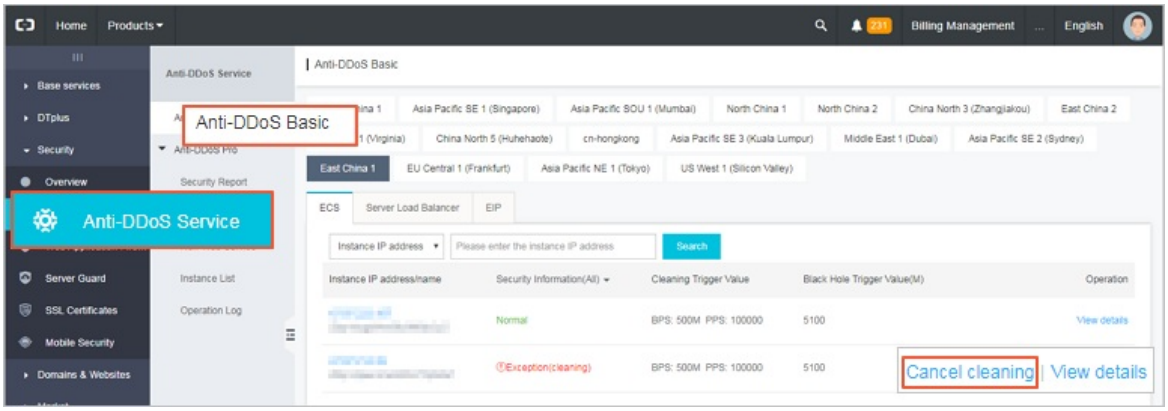
1. Check the logon time to see whether the logon was performed by you or another administrator.
2. If the logon was not performed by you or another administrator, it is an unauthorized logon. Perform the following steps:
   i. Reset the password. For more information, see Reset the logon password of an instance.
   ii. Check whether the ECS instance has been infected.
   iii. Configure security groups to allow access only from specific IP addresses. For more information, see Scenarios for security groups.

What is traffic scrubbing?

The traffic scrubbing service monitors inbound traffic to ECS instances in real time and identifies unusual traffic such as DDoS attacks. By default, Anti-DDoS Basic is enabled on ECS instances to provide traffic scrubbing. When ECS instances are under attack, the traffic scrubbing service will automatically detect the attack and scrub the malicious traffic without affecting the ECS instance services. When unusual traffic is detected, suspicious traffic is redirected from the destination network to a scrubbing device. The device identifies and removes malicious traffic and then returns legitimate traffic to the network to be forwarded to the ECS instances.

How do I cancel traffic scrubbing for an ECS instance?

1. Log on to the Alibaba Cloud Security Anti-DDoS Basic console.
2. Click the ECS tab. In the ECS instance list, find the IP address of an ECS instance that is in the cleaning state. Click **View details**.
3. Click **Cancel cleaning**.



How do I request reverse lookup for an ECS instance?

Reverse lookup is used in mail services to reject all mails from IP addresses mapped to unregistered domain names. Most spammers use dynamic IP addresses or IP addresses mapped to unregistered domain names to send unwanted emails and avoid being tracked. When reverse lookup is enabled on a mail server, the server rejects mails sent from dynamic IP addresses or unregistered domain names to reduce the amount of spam received.

You can submit a ticket to request reverse lookup for your ECS instance. We recommend that you specify the region, public IP address, and registered domain name of your ECS instance in the ticket for more efficient ticket processing.

After your request is approved, you can run the dig command to check whether reverse lookup has taken effect for your instance. Example:

```
dig -x 121.196.255.** +trace +nodnssec
```

If information similar to the following content is displayed in the command output, reverse lookup has taken effect.

```
1.255.196.121.in-addr.arpa. 3600 IN PTR ops.alidns.com.
```

Can an IP address point to multiple reverse lookup domain names?

No, each IP address can only point to a single reverse lookup domain name. For example, you cannot configure the IP address 121.196.255.** to resolve to multiple domain names such as mail.abc.com, mail.ospf.com, and mail.zebra.com.

Can I change the public IPv4 address of an instance after the instance has been created?

You can change the public IPv4 address of an instance within six hours of instance creation. For more information, see Change the public IP address of an ECS instance.

After six hours, whether the public IP address of the instance can be changed depends on the instance network type.

- For instances in VPCs, you can change public IP addresses of instances by converting their IP addresses into EIPs. Then, disassociate the EIPs from the instances and associate new EIPs to the instances or upgrade public bandwidths of the instances to assign new public IP addresses. For more information, see Convert the public IP address of a VPC-type instance to an Elastic IP address.
- For instances in the classic network, you cannot change their public IP addresses. However, you can convert public IP addresses to EIPs when you release the instance. For more information, see Convert the public IP address of a classic network-type instance to an Elastic IP address.

Why am I unable to find the option to change the public IP address of an ECS instance in the ECS console?

- Within six hours after a pay-as-you-go instance is created: If No Fees for Stopped Instances (VPC-Connected) is enabled for your account, you must select Retain Instance and Continue Charging After Instance Is Stopped when you stop the pay-as-you-go instance. Otherwise, the option to change the public IP address will not be displayed in the ECS console after the instance is stopped.

- If more than six hours have passed after the instance was created: You cannot change the public IP address and the option is not displayed.

Can I change the private IP address of an instance?

- For instances in VPCs: You can change the private IP address of an instance. For more information, see Change the private IP address of an instance.
- For instances in the classic network: You cannot change the private IP address of an instance.

If no public IPv4 address was assigned to an ECS instance during instance creation, how do I assign a public IP address to the instance?

- Apply for and bind an Elastic IP Address (EIP) to the ECS instance. For more information, see the following topic of *EIP documentation:* Apply for new EIPs.
- Modify the public bandwidth of the ECS instance to allocate a fixed public IP address. For more information about modifying the public bandwidth of a subscription ECS instance, see Overview of instance upgrade and downgrade. For more information about modifying the public bandwidth of a pay-as-you-go ECS instance, see Change the Internet bandwidth of a pay-as-you-go instance.

What is a BGP data center?

Border Gateway Protocol (BGP) is primarily used for interconnection between Internet autonomous systems (AS). The main function of BGP is to control route propagation and select the best routes.

China Netcom, China Telecom, China Railcom, and some large privately owned IDC service providers all have autonomous system numbers (ASNs). Most major network carriers in China use BGP to achieve multi-line interconnection with their own ASNs.

BGP is currently the world-leading dual-line technology. To achieve multi-line interconnection in this manner, an IDC must obtain a CIDR block and an ASN from the China Internet Network Information Center (CNNIC) or Asia-Pacific Network Information Center (APNIC), and then broadcast this CIDR block to the networks of other carriers through BGP. After networks are interconnected through BGP, the backbone routers of the network carriers will determine the optimal routes to the CIDR block of the IDC to ensure high-speed access for users of different network carriers.

What are WAN and LAN?

- A wide area network (WAN) is also known as an external or public network. It is a telecommunications network that connects smaller networks, including local area networks (LANs) and metro area networks (MANs). Each WAN extends over a large geographical area such as a city or a country and may cover continents to provide telecommunications services and form an international telecommunications network. WAN is not equal to Internet.
- A LAN is also known as an internal network. A LAN is a network that interconnects computers within a small area. Users can manage files, share application software and printers, schedule work for work groups, and communicate with each other such as by sending emails or faxes within a LAN. A LAN is a closed network that can be as small as two computers in an office to as large as thousands of computers in a company. In Alibaba Cloud, ECS instances within the same region can be created in the same type of networks and communicate with each other through the internal network. ECS instances in different regions are isolated from each other.

How do I express a subnet mask?

You can use one of the following methods to express a subnet mask:

- Dotted decimal notation.

  The default subnet mask of a Class A network is 255.0.0.0.

- Append a forward slash (/) and a number ranging from 1 to 32 to the end of an IP address to define a subnet mask. The number indicates the length of the network identification bit in the subnet mask.

  Example: 192.168.0.3/24.

How do I plan subnets?

For more information about the best practices for planning subnets, see Set up network connections.

How can I view the resource quota?

For more information about how to view the limits and quotas of resources, see Limits.