Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequent
ial, exemplary, incidental, special, or punitive damages, including lost profits arising from the use or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the 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 contact Alibaba Cloud directly if you discover any errors in this document.
# Document conventions

<table>
<thead>
<tr>
<th>Style</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>![danger]</td>
<td>A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.</td>
<td>Danger: Resetting will result in the loss of user configuration data.</td>
</tr>
<tr>
<td>![warning]</td>
<td>A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.</td>
<td>Warning: Restarting will cause business interruption. About 10 minutes are required to restart an instance.</td>
</tr>
<tr>
<td>![caution]</td>
<td>A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.</td>
<td>Notice: If the weight is set to 0, the server no longer receives new requests.</td>
</tr>
<tr>
<td>![note]</td>
<td>A note indicates supplemental instructions, best practices, tips, and other content.</td>
<td>Note: You can use Ctrl + A to select all files.</td>
</tr>
<tr>
<td>![angle_brackets]</td>
<td>Closing angle brackets are used to indicate a multi-level menu cascade.</td>
<td>Click Settings &gt; Network &gt; Set network type.</td>
</tr>
<tr>
<td><strong>Bold</strong></td>
<td>Bold formatting is used for buttons, menus, page names, and other UI elements.</td>
<td>Click OK.</td>
</tr>
<tr>
<td><strong>Courier font</strong></td>
<td>Courier font is used for commands.</td>
<td>Run the <code>cd /d C:/window</code> command to enter the Windows system folder.</td>
</tr>
<tr>
<td><strong>Italic</strong></td>
<td>Italic formatting is used for parameters and variables.</td>
<td><code>bae log list --instanceid Instance_ID</code></td>
</tr>
<tr>
<td><code>[ ]</code> or `[a</td>
<td>b]`</td>
<td>This format is used for an optional value, where only one item can be selected.</td>
</tr>
<tr>
<td>Style</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>{} or {a</td>
<td>b}</td>
<td>This format is used for a required value, where only one item can be selected.</td>
</tr>
</tbody>
</table>
## Contents

Legal disclaimer ................................................................. 1
Document conventions ........................................................... 1
1 Network types ....................................................................... 1
2 Instance IP addresses ............................................................. 3
  2.1 IP addresses of VPC-Connected ECS instances ......................... 3
  2.2 IP addresses of a classic network-connected ECS instance ............... 4
  2.3 Elastic IP Addresses ....................................................................... 6
  2.4 Intranet ......................................................................................... 8
3 Change IPv4 addresses ............................................................. 10
  3.1 Change the private IP of an ECS 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 an Elastic IP address ............................................................................................. 13
  3.4 Convert the public IP address of a classic network-type instance to an Elastic IP address ............................................................................................. 14
4 Elastic Network Interfaces ......................................................... 17
  4.1 ENI overview ............................................................................. 17
  4.2 Create an ENI ............................................................................. 20
  4.3 Attach an ENI ............................................................................. 21
  4.4 Configure an ENI ............................................................................. 24
  4.5 Assign a secondary private IP address ............................................. 28
  4.6 Revoke a secondary private IP address ............................................. 35
  4.7 Modify an ENI ............................................................................. 36
  4.8 Detach an ENI from an instance ..................................................... 38
  4.9 Delete an ENI ............................................................................. 39
5 Multiqueue for NICs ............................................................... 40
6 Connect a classic network to a VPC ........................................ 43
7 Network FAQ ........................................................................... 45
1 Network types

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

Virtual Private Cloud (VPC)

VPCs are logically isolated networks established in Alibaba Cloud. You can customize the topology and IP addresses in a VPC. We recommend that the VPC network type is used if you have high network security requirements.

For more information about VPC, see Virtual Private Cloud documentation.

Classic network

A classic network is deployed in the public infrastructure of Alibaba Cloud, which is responsible for its planning and management. We recommend that the classic network type is used if your business requirements are high in terms of network usability.

Note:

If you purchased an ECS instance after 17:00 (UTC+8) on June 14, 2017, you cannot choose the classic network type.

VPC vs. Classic networks

The following table describes key network functions and indicates whether they are supported within VPCs and classic networks.

<table>
<thead>
<tr>
<th>Items</th>
<th>VPC</th>
<th>Classic network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Two-layer logic isolation</td>
<td>Supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>Custom private network blocks</td>
<td>Supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>Private IP addresses</td>
<td>Unique within one VPC.</td>
<td>Unique in the global</td>
</tr>
<tr>
<td></td>
<td>Replicable between VPCs.</td>
<td>Classic network</td>
</tr>
<tr>
<td>Communicate within or between private networks</td>
<td>Able to communicate within a VPC, but isolated between VPCs</td>
<td>Able to communicate in one region and under one account</td>
</tr>
<tr>
<td>Tunneling</td>
<td>Supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>Custom router</td>
<td>Supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>Items</td>
<td>VPC</td>
<td>Classic network</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Routing table</td>
<td>Supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>Switches</td>
<td>Supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>SDN</td>
<td>Supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>Self-built NAT gateway</td>
<td>Supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>Self-built VPN</td>
<td>Supported</td>
<td>Not supported</td>
</tr>
</tbody>
</table>
2 Instance IP addresses

2.1 IP addresses of VPC-Connected ECS instances

Each VPC-Connected ECS instance can communicate within an intranet by using a private IP address, or communicate over the Internet by using a public IP address.

Private IP addresses

Each VPC-Connected ECS instance is assigned a private IP address when it is created. That address is determined by the VPC and the CIDR block of the VSwitch to which the instance is connected.

Scenarios

A private IP address can be used in the following scenarios:

- Load balancing
- Communication among ECS instances within an intranet
- Communication between an ECS instance and other cloud products (such as OSS and RDS) within an intranet

For more information, see Intranet.

Modify a private IP address

You can modify the private IP address of a VPC-Connected ECS instance in the ECS console. For more information, see Change the private IP of an ECS instance.

Public IP addresses

VPC-Connected ECS instances support two public IP address types:

- NatPublicIp, which is assigned to a VPC-Connected ECS instance, can be released only, and cannot be disassociated from the instance.
- Elastic public IP (EIP). For more information, see What is an EIP address.

When a VPC-Connected ECS instance accesses the Internet, its public IP address is mapped to its private IP address through network address translation (NAT).

You cannot find a network interface for Internet access by running commands within the operating system.
Scenarios

NatPublicIp and EIP are applicable to different scenarios:

- NatPublicIp: If you want to assign a public IP address to a VPC-Connected ECS instance when creating the instance, and do not want to retain the public IP address when the instance is released, you can use a NatPublicIp address.
- EIP: If you want to keep a public IP address and associate it to any of your VPC-Connected ECS instances in the same region, you can use an EIP address.

Obtain a public IP address

- NatPublicIp: When creating a VPC-Connected ECS instance, if you select Assign a public IP, a NatPublicIp is assigned to the instance when it is created.
- EIP: You can apply for an EIP address and bind it to a VPC-Connected ECS instance. In this case, do not assign a NatPublicIp to an instance. For more information, see Apply for an EIP address.

Release a public IP address

- NatPublicIp: When a NatPublicIp address is assigned to an instance, you can only release the IP address, but cannot disassociate it. Only a NatPublicIp address that is assigned to a Subscription instance can be released. For more information, see #unique_11.
- EIP: If you do not need an EIP address, disassociate it from a VPC-Connected ECS instance and release it in the EIP console. For more information, see Unbind and release an EIP address.

Billing

You are billed for outbound Internet traffic usage only. For more information, see #unique_13.

2.2 IP addresses of a classic network-connected ECS instance

Currently, for ECS instances of the classic network type, IP addresses are distributed in a unified way and divided into public and private IP addresses.
Private IP addresses are mainly used for remote access to your instance or to the services deployed on your instance.

Intranet IP addresses

Each classic network-connected ECS instance is assigned a private, that is intranet, IP address.

Scenarios

Intranet IP addresses can be used in the following scenarios:

- Load balancing
- Mutual intranet access between ECS instances
- Mutual intranet access between ECS instances and other cloud services, such as OSS and RDS

Traffic generated through intranet IP addresses within an intranet is free of charge. For more information, see Intranet.

Modify an intranet IP address

Once a classic network-connected ECS instance is created, you cannot change its intranet IP address.

Note:

Do not change an intranet IP address within a guest operating system. Otherwise, communication within an intranet is interrupted.

Public IP addresses

If you purchase bandwidth for Internet access, a public IP address is assigned to your classic network-connected ECS instance. You cannot change the public IP address once it is assigned.

Scenarios

A public IP address is used in the following scenarios:

- Mutual access between an ECS instance and the Internet
- Mutual Internet access between ECS instances and other Alibaba Cloud services

Assign a public IP address
When you create an ECS instance, a public IP address is assigned to it if Assign public IP is selected.

For a Subscription instance with no public IP address, you can use the Upgrade Configuration or the Renew for Configuration Downgrade feature to purchase public network bandwidth.

Note:

- For a Pay-As-You-Go classic network-connected ECS instance with no public IP address, you cannot assign a public IP address after the instance is created.
- For a classic network-connected ECS instance, you cannot disassociate or release its public IP address once the IP address is assigned. If you set the bandwidth to 0 Mbit/s when renewing an instance for configuration downgrade, in the next purchase cycle, the public IP address is retained, but the instance cannot access the Internet.

Billing

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

Multicast and broadcast

Intranet IP addresses cannot be used for multicasting or broadcasting.

2.3 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.

<table>
<thead>
<tr>
<th>Item</th>
<th>Public IP address assigned to an ECS instance</th>
<th>EIP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Can the IP address be independently purchased and used?</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Can the IP address be associated to or disassociated from an ECS instance as needed?</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Can the bandwidth value for the IP address be adjusted in real time?</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Billing method

EIPs can be billed by traffic or by bandwidth. For more information, see EIP document #unique_19.

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 #unique_10.

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. #unique_20

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 #unique_12.

2.4 Intranet

If you need to transmit data between two ECS instances in the same region, use an intranet connection. Intranet connections can also be used to connect any combination of ECS, RDS, SLB, and OSS if they are deployed in the same region. However, the network speed is limited to one gigabit of shared bandwidth for non I/O optimized instances.

Alibaba Cloud instances can communicate over an intranet. The instances use one gigabit of shared bandwidth for non I/O optimized instances, and 10 gigabits of shared bandwidth for I/O optimized instances, with no special restrictions. However, because the intranet is a shared network, the bandwidth may fluctuate.

The following table describes how to enable intranet communication between ECS instances across different network types, depending on the number of accounts and whether the target regions and security groups are the same or different.

<table>
<thead>
<tr>
<th>Network type</th>
<th>Accounts used</th>
<th>Regions</th>
<th>Security groups</th>
<th>How to enable intranet communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPC, same VPC</td>
<td>One account or multiple accounts</td>
<td>Same</td>
<td>Same</td>
<td>Enabled by default.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Authorize security groups for each other.</td>
</tr>
<tr>
<td>Network type</td>
<td>Accounts used</td>
<td>Regions</td>
<td>Security groups</td>
<td>How to enable intranet communication</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------</td>
<td>---------</td>
<td>-----------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>VPC, different VPCs</td>
<td>One account or multiple accounts</td>
<td>Same</td>
<td>Either the same or different</td>
<td>Use Express Connect. For more information, see Application scenarios from Product Introduction to Express Connect.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Different</td>
<td>Different</td>
<td></td>
</tr>
<tr>
<td>Classic</td>
<td>One account</td>
<td>Same</td>
<td>Same</td>
<td>Enabled by default.</td>
</tr>
<tr>
<td></td>
<td>Multiple accounts</td>
<td></td>
<td>Either the same or different</td>
<td>Authorize security groups for each other. For more information, see Scenarios of security groups.</td>
</tr>
</tbody>
</table>

Private IP addresses are used for intranet communication. You cannot change the private IP address of an instance of the Classic network type, but you can change the private IP address of a VPC-Connected ECS instance. Private and public addresses of ECS instances do not support virtual IP (VIP) configuration.

By default, instances of different network types cannot communicate with one another in one intranet. However, VPC provides the ClassicLink function, which allows you to link an ECS instance in the classic network to cloud resources in a VPC through the intranet.
3 Change IPv4 addresses

3.1 Change the private IP of an ECS instance

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

Procedure

1. Log on to the ECS console.
2. In the left-side navigation pane, click Instances.
3. Select the target region.
4. In the Actions column, click More > Instance Status > Stop.
5. When the instance is stopped, click the instance ID to go to its Instance Details page.
6. In the Configuration Information panel, click More > Modify Private IP Address.
7. In Modify Private IP Address dialog, select a VSwitch, and then click Modify.

Make sure the current VSwitch and the selected VSwitch are in the same zone.

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

8. Go back to the instance page and, in the Actions column, click More > Instance Status > Restart to make the new private IP address take effect.

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.

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: #unique_10.
  - 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 #unique_26. For more information about modifying the public bandwidth of a pay-as-you-go ECS instance, see #unique_27.

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

After the public IP address of a VPC-type instance is converted to an Elastic IP address (EIP), you can unbind the EIP from the instance and bind it to another instance at any time. Address conversion does not affect the access from the public network to your ECS instance or cause transient traffic interruptions.

Prerequisites

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

- The instance has been 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 of expiry.
- 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 #unique_26.
- If the type of the instance has been changed, wait until the change takes effect before proceeding.
- 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 of the Internet bandwidth remains unchanged.
- The EIP is billed separately. For more information about EIP billing, see EIP pricing. You can go to the Billing Management page, select Usage Records, and select Elastic IP 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 #unique_29.

**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 instance with the VPC network type, and then choose *More > Network and Security Group > Convert to EIP* from 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 followed by (EIP).

You can click the EIP to go to the *EIP console* to manage the EIP.

**What's next**

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

- Unbind the EIP from the instance and bind it to another instance, or release it. For more information, see #unique_12.
- Add the EIP to a shared bandwidth package to save costs. For more information, see #unique_30, *Select a product to gain access to the Internet*, and *How to reduce Internet costs*.

**Related topics**

#unique_33

### 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.
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 #unique_26.
- 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 #unique_36.
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.

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.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Quality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary private IP address</td>
<td>1</td>
</tr>
<tr>
<td>Secondary private IP address</td>
<td>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 <em>#unique_40</em>.</td>
</tr>
<tr>
<td>EIP</td>
<td>1 or more. The maximum number of EIPs that can be associated to an ENI depends on the associating mode. For more information, see <em>Overview for associating an EIP with a secondary ENI</em>.</td>
</tr>
<tr>
<td>MAC address</td>
<td>1</td>
</tr>
<tr>
<td>Security group</td>
<td>1 to 5</td>
</tr>
<tr>
<td>Network instance name</td>
<td>1</td>
</tr>
</tbody>
</table>
Limits

- A limited number of ENIs can be created for one account in each region. For more information, see the ENI limits section of #unique_42.
- 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. Click Create ENI.
2. In the displayed dialog box, complete the following configurations:

a. Network Interface Name: Enter a name for the ENI.

b. 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.

c. 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.

d. 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.

e. Security Group: Select a security group in the selected VPC.

f. Description: Optional. Enter a description for the ENI.

g. 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. Locate an available ENI, and then click Bind to Instance.
2. 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](#)
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

This topic describes how to configure an ENI. You may need to manually configure ENIs for some images used by your instances so that the attached ENIs can be identified by the operating systems.

Prerequisites

You have attached an ENI to an ECS instance. For more information on how to attach an ENI to an ECS instance, see Attach an ENI.

Context

If your instance is running one of the following images, you do not need to manually configure their ENIs:

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

If your instance is running an image not included in the preceding list, you must manually configure the ENI for the image.

Automatic configuration

If your instance is running a CentOS image, you can download and install the multi-nic-util tool to automatically configure the ENI. This tool supports only images later than CentOS 6.8 and CentOS 7.3.

1. Remotely connect to an ECS instance. For more information, see #unique_62.
2. Run the following command to download the multi-nic-util tool:

```
```

3. Run the following commands to 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
```

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

```
systemctl restart eni.service
```

Manual configuration

This section takes an instance running CentOS 7.2 64-bit as an example to describe how to manually configure ENIs attached to a Linux instance.

1. Remotely connect to an ECS instance. For more information, see #unique_62.

2. Query the attributes of each ENI, including the primary private IP address, subnet mask, default route, and MAC address.

Examples:

```
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:**
```

- Call the DescribeNetworkInterfaces operation to query the preceding attributes of the ENIs.
- Perform the following steps in the ECS console to query the attributes of the ENIs:
  a. Log on to the ECS console.
  b. In the left-side navigation pane, choose Network & Security > ENI.
  c. On the Network Interfaces page, find the target ENIs and view their primary private IP addresses and MAC addresses in the Primary Private IP Address and Type/MAC Address(All) columns.
- Obtain the attributes of ENIs from instance metadata. For more information, see #unique_63.
3. Run the command to view the configuration file of each ENI.

```
[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
```

Note:

- To facilitate configuration, take note of the correlation between the ENI name in the operating system and the MAC address.
- To prevent the active default route of the ECS instance from being changed when ENIs configured by (ifup) are started, do not set the ENI interface to the default route. DEFROUTE=no means the ENI interface is not the default route.

Example:

```
# cat /etc/sysconfig/network-scripts/ifcfg-eth1
DEVICE=eth1
BOOTPROTO=dhcp
ONBOOT=yes
TYPE=Ethernet
USERCTL=yes
PEERDNS=no
IPV6INIT=no
PERSISTENT_DHCLIENT=yes
HWADDR=00:16:3e:12:e7:**
DEFROUTE=no
```

4. Perform the following steps to start ENIs:

a) Run the command to start the dhclient process, and initiate a DHCP request.

Examples:

```
# ifup eth1
# ifup eth2
```

b) After a response is received, run the command to check the IP addresses of the ENIs, which must be the same as the IP addresses of the ENIs displayed in the ECS console.

Example:

```
# ip a
```
5. Set the default metric parameter for each ENI in the routing table.

In this example, set the metric parameters for eth1 and eth2:

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

a) Run the following commands to set the metric parameters:

```
# 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
```

b) Run the `route -n` command to check whether the metric parameters have been set.

```
# 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 0 eth1
0.0.0.0 10.0.0.253 0.0.0.0 UG 1002 0 0 eth2
10.0.0.0 255.255.255.0 U 0 0 0 eth0
10.0.0.0 255.255.255.0 U 0 0 0 eth1
10.0.0.0 255.255.255.0 U 0 0 0 eth2
169.254.0.0 255.255.255.0 U 0 0 0 eth0
169.254.0.0 255.255.255.0 U 0 0 0 eth1
169.254.0.0 255.255.255.0 U 0 0 0 eth2
```

6. Perform the following steps to create a routing table:

**Note:**

We recommend that you use the metric value as the routing table name.

a) Run the following commands to create a routing table:

```
# ip -4 route add default via 10.0.0.253 dev eth1 table 1001
```
b) Run the following commands to check whether the routing table has been created:

```bash
# ip route list table 1001
default via 10.0.0.253 dev eth1
# ip route list table 1002
default via 10.0.0.253 dev eth2
```

7. Configure a policy-based routing.

a) Run the following commands to create a policy-based routing.

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

b) Run the `ip rule list` command to view the routing rules.

```bash
# 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 you configure the ENI, you can perform the following operations:

- Assign a secondary private IP address
- Detach an ENI from an instance

Related topics

#unique_65

4.5 Assign a secondary private IP address

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 ECS instances in VPCs and divert traffic during a failover.

Prerequisites

- Your instance type must support assigning multiple secondary private IP addresses. For more information, see the Private IP address of a single ENI column corresponding to your instance type in Instance families.
- If you assign a secondary private IP address to a primary ENI, the instance to which the primary ENI is attached must be in 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 ENI. 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 detach ENIs from the instance and attach the ENIs to another instance to divert traffic to that instance, enabling 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.
  
  - If the target ENI is in the Available state, you can assign up to 10 private IP addresses to the ENI.
  
  - If the target 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.

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 a secondary private IP address.

2. Optional: If the ENI is a secondary ENI that is not attached to an ECS instance, attach the ENI to an instance and go to step 3. For more information, see Attach an ENI.

3. In the instance, configure the assigned secondary private IP addresses.

   - **Windows Server:** For more information, see Assign a secondary private IP address for a Windows instance.

   - **Linux:** For more information, see Assign a secondary private IP address to a Linux instance.
Assign a secondary private IP address

1. Log on to the *ECS console*.
2. In the left-side navigation pane, choose Network & Security > ENI.
3. In the top navigation bar, select a region.
4. On the Network Interfaces page, find the target ENI, and then click Manage Secondary Private IP Address in the Actions column.
5. In the Manage Secondary Private IP Address dialog box:
   
   - Method 1: Click Assign New IP. The system randomly assigns IPv4 addresses from the value of IPv4 Private CIDR Block. You can click Assign New IP multiple times if multiple secondary private IP addresses are needed.
   - Method 2: Manually enter secondary private IP addresses within the value of IPv4 Private CIDR Block.

6. Click Modify.

7. Optional: If you configured 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. Then, you can configure the IP addresses for an ECS instance.

8. Optional: If the ENI is a secondary ENI that is not attached to an ECS instance, attach the ENI to an instance and then configure secondary private IP addresses in the instance. For more information, see Attach an ENI.

Assign a secondary private IP address for a Windows instance

1. Remotely connect to an ECS instance. For more information, see #unique_62.
2. Open the Network and Sharing Center.
3. Click Change adapter settings.
4. Double-click the current network connection name, and then click Properties.
6. Select Use the following IP address and then click Advanced.
7. Click Add in the IP addresses section, set IP addresses to the assigned IP address, and configure Subnet Mask.

You can add multiple IP addresses to the same adapter.

8. Click OK.

Assign a secondary private IP address to a Linux instance

In the following example, the primary ENI `eth0` is used. If you are using a secondary ENI, modify the ID of the ENI as needed.

1. Remotely connect to an ECS instance. For more information, see #unique_62.
2. Configure a secondary private IP address based on your operating system of the instance.

- **RHEL series: CentOS 6, CentOS 7, Red Hat 6, Red Hat 7, or Aliyun Linux 2**
  
  a. Open the network configuration file.
  
  - 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 assign 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 topics

#unique_66

4.6 Revoke a secondary private IP address

This topic describes how to revoke a secondary private IP address from an Elastic Network Interface (ENI).

Limits

The primary private IP address cannot be revoked.

Prerequisites

- At least one secondary private IP addresses is assigned to the target ENI.
- The target ENI is in the Available or InUse state.
- If the secondary private IP addresses to be revoked is assigned to the primary ENI, the instance to which the primary ENI is attached must be in the Running or Stopped state.

Procedure

1. On the Network Interfaces page, locate the target ENI, and then click Manage Secondary Private IP Address in the Actions column.

2. In the Manage Secondary Private IP Address dialog box, click Unassign once or multiple times if additional IP addresses need to be revoked.
3. Click Modify.

Related API: UnassignPrivateIpAddresses

What to do next

If your application requirements change, you can assign multiple secondary private IP address to an ENI. For more information, see Assign a secondary private IP address.

4.7 Modify an ENI

This topic describes how to modify primary and secondary Elastic Network Interfaces (ENIs). You can only modify the primary ENI by configuring its associated instance with a different security group as needed, and you can modify a secondary ENI by changing its attributes (such as the name, associated security group, and description).

Limits

Before you can modify the security group to which an ENI belongs, the ENI and its associated ECS instance must meet the following limits:

- An ECS instance cannot be added to a basic security group and an advanced security group at the same time.
- An ENI cannot be added to a basic security group and an advanced security group at the same time.
- An ENI can be attached to an ECS instance only if they belong to the same type of security group.

For more information, see #unique_69.

Modify a primary ENI

To modify a primary ENI, follow these steps:

Note:
The primary ENI and the secondary ENIs of an ECS instance can belong to different security groups. This means that if you associate the ECS instance with another security group, the primary ENI will also be associated with this security group, but the secondary ENIs will remain in the previous security group.

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 then click Manage Instances in the Actions column.
5. On the Instances in Security Group page, modify the security group with which the primary ENI is associated.
   • To add the primary ENI to a new security group, follow these steps:
     a. In the upper-right corner of the Instances in Security Group page, click Add Instance.
     b. In the displayed dialog box, select an instance ID to which the primary ENI is attached, and then click OK.
        The primary ENI is added to the new security group along with the corresponding ECS instance.
   • To remove the primary ENI from the current security group, follow these steps:
     a. On the Instances in Security Group page, select one or more instances, and then click Remove from Security Group.
     b. In the displayed dialog box, 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 Security Groups page and find the target primary ENI to verify that the settings have taken effect.

Related APIs:
   • JoinSecurityGroup
   • LeaveSecurityGroup

Modify a secondary ENI

To modify a secondary ENI, follow these steps:

1. Log on to the ECS console.
2. In the left-side navigation pane, choose Network & Security > ENI.
3. In the top navigation bar, select a region.
4. Find the target secondary ENI, and then click Modify in the Actions column.
5. In the displayed dialog box, modify the ENI attributes as follows:
   - Network Interface Name: Set a new ENI name according to the rules 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 according to the rules displayed under this field.
6. Click OK.

Related API: `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. Find the target ENI, and in the Actions column, click Unbind.
2. 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:
4.9 Delete an ENI

You can only delete a secondary ENI. You cannot delete the primary ENI of an instance.

After a secondary ENI is deleted:

- The primary private IP address of the secondary ENI is released automatically.
- The deleted secondary ENI is automatically removed from all associated security groups.

If you release an instance, any attached ENIs will be deleted along with its release. You can choose to detach the ENI first and then release the corresponding instance separately.

Limits

You can only delete an ENI in the Available status.

Prerequisite

If an ENI is attached to an instance, you must first detach it from the instance to delete it separately.

Procedure

To delete an ENI, follow these steps:

1. Log on to the ECS console.
2. In the left-side navigation pane, select Networks and Security > ENI.
3. Select the target region.
4. Find the target ENI, and in the Actions column, click Delete.
5. Click OK.

In the Network Interfaces page, refresh the table. If the ENI is no longer displayed, it is deleted successfully.
5 Multiqueue for NICs

Multiqueued NICs route NIC interruptions in ECS instances to different CPUs. Results of network PPS and bandwidth tests show that a solution that uses two queues instead of one queue can enhance network performance by between 50% to 100%.

ECS instance types supporting multiqueue

See #unique_40 to find instance types that support multiqueue and the number of queues that are supported.

Images supporting multi-queue

The following public images officially provided by Alibaba Cloud support multiqueue:

<table>
<thead>
<tr>
<th>Image</th>
</tr>
</thead>
<tbody>
<tr>
<td>CentOS 6.8/6.9/7.2/7.3/7.4</td>
</tr>
<tr>
<td>Ubuntu 14.04/16.04</td>
</tr>
<tr>
<td>Debian 8.9</td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server 12 SP1</td>
</tr>
</tbody>
</table>

Note:
Whether an image supports multiqueue is not related to the memory address width of the operating system.

- CentOS 6.8/6.9/7.2/7.3/7.4
- Ubuntu 14.04/16.04
- Debian 8.9
- SUSE Linux Enterprise Server 12 SP1

Support for SUSE Linux Enterprise Server 12 SP2 edition is in development. Support for Windows 2012 R2 and Windows 2016 is by invitation.

Configure multi-queue support for NICs on a Linux ECS instance

We recommend that you use one of the latest Linux distributions, such as CentOS 7.2, to configure multi-queue for the NICs.

Here we take CentOS 7.2 as an example to illustrate how to configure multi-queue for the NIC. In this example, two queues are configured, and the NIC name is eth0.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>To check whether the NIC supports multi-queue, run the command:</td>
<td><code>ethtool -l eth0</code></td>
</tr>
<tr>
<td>To enable multi-queue for the NIC, run the command:</td>
<td><code>ethtool -L eth0 combined 2</code></td>
</tr>
</tbody>
</table>

Issue: 20200226
If you are using more than one NIC, configure each NIC.

```
[root@localhost ~]# ethtool -l eth0
Channel parameters for eth0:
Pre-set maximums:
  RX: 0
  TX: 0
  Other: 0
  Combined: 2  # This line indicates that a maximum of two queues can be configured
Current hardware settings:
  RX: 0
  TX: 0
  Other: 0
  Combined: 1  # It indicates that one queue is currently taking effect
[root@localhost ~]# ethtool -L eth0 combined 2  # It sets eth0 to use two queues currently
```

We recommend that you enable the irqbalance service so that the system can automatically adjust the allocation of the NIC interrupts on multiple CPU cores. Run the command: ```systemctl start irqbalance``` (this feature is enabled by default in CentOS 7.2).

If the network performance is not improved as expected after the multi-queue feature is enabled, you can enable the RPS feature. To do so, see the following Shell script:

```bash
#!/bin/bash
cpu_num=$(grep -c processor /proc/cpuinfo)
quotient=$((cpu_num/8))
if [ $quotient -gt 2 ]; then
  quotient=2
elif [ $quotient -lt 1 ]; then
  quotient=1
fi
for i in $(seq $quotient)
do
cpuset="${cpuset}${i}"
done
for rps_file in $(ls /sys/class/net/eth*/queues/rx*/rps_cpus)
do
echo $cpuset > $rps_file
done
```

Configure multi-queue support for NICs on a Windows ECS instance

Note:
We are inviting Windows users to sign up and test multiqueue support for performance improvement. Note that the overall performance increase is not as great when compared with performance increase of Linux systems.

If you are using a Windows instance, you must install the driver to use the multiqueue feature for NICs.

To install the driver for Windows systems, follow these steps:

1. **Open a ticket** to request and download the driver installation package.
2. Unzip the driver installation package. For Windows 2012/2016 systems, use the driver in the Win8/amd64 folder.
3. Upgrade the NIC driver:
   a. Select Device Manager > Network adapters.
   b. Right click Red Hat VirtIO Ethernet Adapter and select Update Driver.
   c. Select the Win8/amd64 directory of the driver directory that you have unzipped, and update the driver.
4. Restart the Windows system after the driver is upgraded for the multiqueue feature to take effect.
6 Connect a classic network to a VPC

This topic describes how to connect a classic network to a VPC. You can set up a ClassicLink connection so that ECS instances of the classic network type can access cloud resources in a VPC through the intranet.

Prerequisites

Make sure that you are aware of the limits of ClassicLink. For more information, see #unique_75.

Procedure

1. Log on to the VPC console.
2. Select the region of the target VPC, and click the ID of the target VPC.
3. On the VPC Details page, click Enable ClassicLink. In the displayed dialog box, click OK.
4. Find the target ECS instance of the classic network type, and then choose More > Network and Security Group > Connect to VPC.
5. In the displayed dialog box, select the target VPC and click OK, and then click the security group configuration link.

![Connect to VPC dialog box]

When you connect to a VPC, you must configure the security group rules to ensure connectivity.

Go to the instance security group list and add ClassicLink rules
6. Click Add ClassicLink Rules and configure the security rule according to the following information. Then, click OK.

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classic Security Group</td>
<td>Display the classic network security group.</td>
</tr>
<tr>
<td>Select VPC Security Group</td>
<td>Select a security group to use. Up to five security groups can be selected.</td>
</tr>
<tr>
<td>Mode</td>
<td>Select one of the following modes:</td>
</tr>
<tr>
<td></td>
<td>• Classic &lt;=&gt; VPC: The connected resources can access each other (recommended).</td>
</tr>
<tr>
<td></td>
<td>• Classic =&gt; VPC: Authorize the classic ECS instance to access cloud resources in the connected VPC.</td>
</tr>
<tr>
<td></td>
<td>• VPC =&gt; Classic: Authorize the cloud resources in the connected VPC to access the classic ECS instance.</td>
</tr>
<tr>
<td>Protocol Type and Port Range</td>
<td>Select the protocol and port used for the communication. The port must be in the form of xx/xx. For example, if port 80 is used, enter 80/80.</td>
</tr>
<tr>
<td>Priority</td>
<td>Set the priority for the rule. A smaller number represents a higher priority, for example, 1.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the security rule.</td>
</tr>
</tbody>
</table>

7. Return to the ECS console. On the Instance List page, click the Column Filter icon in the upper-right corner, and then select the Connection Status check box. Then, click OK.

If Connection Status is Connected, ECS instances of the classic network are connected to the VPC network.
7 Network FAQ

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

- **Public bandwidth**
  - What are the inbound and outbound bandwidths of ECS instances?
  - I bought 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 public 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 public 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**
  - How do I query the IP addresses of an ECS instance?
  - How do I disable the public NIC of an ECS instance?

- **Network access and traffic direction**
  - Why can’t I access a website hosted on an ECS instance?
  - An unusual logon to one of my ECS instances has been detected. What can 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?
• Public IP addresses

- Can I change the public IP (IPv4) address of an ECS instance within six hours after the instance is created? How?
- Why can’t I find the option to change the public IP address of an ECS instance in the ECS console?
- Apart from the public IP address, can I change the private IP address of an ECS instance?
- If no public IP (IPv4) address was assigned to an ECS instance during instance creation, how do I assign a public IP address to the instance?

• Network basics

- What is a BGP data center?
- What are WAN and LAN?
- How do I express a subnet mask?
- How do I plan subnets?

• Quotas

- How can I view the resource quota?

What are the inbound and outbound bandwidths of ECS instances?

<table>
<thead>
<tr>
<th>Bandwidth type</th>
<th>Description</th>
</tr>
</thead>
</table>
| Inbound bandwidth  | The bandwidth for inbound traffic of 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 for outbound traffic of 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 bought 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 is the outbound bandwidth. The inbound bandwidth of the instance capped at 100 Mbit/s.
- The outbound bandwidth is consumed when data is sent from the ECS instance. The outbound bandwidth of an ECS instance is capped at 200 Mbit/s, regardless of whether the instance resides within a VPC or a classic network.

- The 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 100 Mbit/s, the maximum inbound bandwidth is 100 Mbit/s.
  - If the outbound bandwidth is greater than 100 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 public network usage of ECS instances billed?

For details, see #unique_13.

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. In the network segment to which the newly created ECS instance is assigned, when the gateway receives an ARP request packet that requests the IP address of an ECS instance, the gateway broadcasts this packet to all ECS instances. The new ECS instance will receive the packet and generate inbound traffic. If no request for the IP address of the new ECS instance is sent, the instance will not send an ARP response packet.

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

To view the public 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 Billing > 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 and click OK.

6. Open the exported CSV file to view the public 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 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 own outbound bandwidth to return responses. The bandwidth consumed by these responses is not displayed in the ECS console. However, traffic generated by the responses is counted towards the outbound traffic of the SLB instances and displayed in the CloudMonitor console. Because of this, the bandwidth usage of your ECS instance displayed in the CloudMonitor console 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 the IP addresses of an ECS instance?

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

- Windows instance
  
  In the CLI, run the `ipconfig /all` command to view NIC information. You can view the IP addresses, subnet masks, gateways, DNS servers, and MAC address in the command output.
How do I disable the public NIC of an ECS instance?

- **Linux instance**
  1. Run the `ifconfig` command to view the public NIC name of the instance.
  2. Run the `ifdown` command to disable the public NIC. For example, if the public NIC is named `eth1`, use the `ifdown eth1` command.

  **Note:**
  You can also run the `ifup` command to re-enable the NIC. For example, if the public NIC is named `eth1`, use the `ifup eth1` command.

- **Windows instance**
  1. In the CLI, run the `ipconfig` command to view information about the public NIC.
  2. Open Control Panel > Network and Sharing Center > Change adapter settings to disable the public NIC.

Why can't I access a website 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 public IP address, Elastic IP address, or NAT IP address of the ECS instance to the WAF whitelist. For more information, see *Avoid Anti-DDoS Basic false positives by using a whitelist*.

An unusual logon to one of my ECS instances has been detected. What can 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:
   
a. **Reset the password.**

b. Check whether the ECS instance has been infected by malware.

   c. **Configure security groups to allow access only from specific IP addresses.**

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 that provides traffic scrubbing is enabled on ECS instances. When ECS instances are under attack, the traffic scrubbing service will automatically detect the attack and scrubs the malicious traffic to the ECS instances without affecting their services. When unusual traffic is detected, suspicious traffic is redirected from the destination network to a scrubbing device. The scrubbing device identifies and removes malicious traffic and returns legitimate traffic to the network to ensure that only legitimate traffic is 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.**

![Image of Alibaba Cloud Security Anti-DDoS Basic console]

How do I request reverse lookup for an ECS instance?

Reverse lookup is used in mail services to reject all mail sent from the IP addresses that are mapped to unregistered domain names. Most spammers use dynamic IP addresses or IP addresses mapped to unregistered domain names to send unwanted
emails and escape tracking. When reverse lookup is enabled on a mail server, the server rejects mail sent from dynamic IP addresses or unregistered domains 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 use the dig command to check whether reverse lookup has taken effect for your instance. For 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 for your instance.

```
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 IP (IPv4) address of an ECS instance within six hours after the instance is created? How?

Yes, you can change the public IP (IPv4) address of an ECS instance within six hours after the instance is created. For more information, see Change the public IP address of an ECS instance.

Why can’t I find the option to change the public IP address of an ECS instance in the ECS console?

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 a pay-as-you-go instance. Otherwise, the option to Change Public IP Address option will not be displayed for the instance in the ECS console after the instance is stopped.

Apart from the public IP address, can I change the private IP address of an ECS instance?

Yes, you can change the private IP address of an ECS instance. For more information, see Change the private IP of an ECS instance.
If no public IP (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: #unique_10.
- 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 #unique_26. For more information about modifying the public bandwidth of a pay-as-you-go ECS instance, see #unique_27.

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. A BGP data center is a data center that uses BGP to implement dual-line or multi-line interconnection.

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

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 consist of two computers in an office or thousands of computers in a company. In Alibaba Cloud public cloud, ECS instances within the same region can be created in the same type of networks and communicate with each other through internal networks. ECS instances in different regions are isolated from each other.

How do I express a subnet mask?

You can express a subnet mask in one of the following method:

- **Dotted decimal notation. For example:**

  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. For example:**

  192.168.0.3/24.

How do I plan subnets?

For the best practices for planning subnets, see #unique_80.

How can I view the resource quota?

For more information about how to view the limits and quotas of resources, see #unique_42.