Alibaba Cloud
Elastic Compute Service

Network

Issue: 20190507

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, consequential, 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 content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, 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 the Alibaba Cloud website, product programs, or content 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.

Generic conventions

Table -1: Style conventions

Style	Description	Example
⛔	This warning information 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.
⚠	This warning information 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 restore business.
📋	This indicates warning information, supplementary instructions, and other content that the user must understand.	❗ Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	📋 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus , page names, and other UI elements.	Click OK.
`Courier font`	It is used for commands.	Run the `cd / d C :/ windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*

Style	Description	Example
{} or {a|b}	**It indicates that it is a required value, and only one item can be selected.**	`swich` *{stand | slave}*

Contents

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 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.

Items	VPC	Classic network
Two-layer logic isolation	Supported	Not supported
Custom private network blocks	Supported	Not supported
Private IP addresses	Unique within one VPC. Replicable between VPCs.	Unique in the global Classic network
Communicate within or between private networks	Able to communicate within a VPC, but isolated between VPCs	Able to communicate in one region and under one account
Tunneling	Supported	Not supported
Custom router	Supported	Not supported

Items	VPC	Classic network
Routing table	Supported	Not supported
Switches	Supported	Not supported
SDN	Supported	Not supported
Self-built NAT gateway	Supported	Not supported
Self-built VPN	Supported	Not supported

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 *Renew for configuration downgrade*.
- 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 *Billing of Internet bandwidth*.

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 address 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 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.

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

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 public IP address

If your instance is assigned a public IP address, you can change the address within six hours after the instance is created regardless of whether the instance is in a classic network or in a VPC network.

Limits

- The instance must be assigned a public IP address. To verify the public IP address, view the public IP address in the IP Address column from the Instance List in the ECS console, as displayed in the following figure.

  Note:

  - If the public network IP address is not assigned at the time of creation of the instance, after the instance is created successfully, you can assign the public IP address by upgrading or downgrading the network bandwidth configuration. For more information, see *overview of configuration changes*.
  - If the public network IP address is not assigned during the creation of a Pay-As-You-Go instance, after the instance is created successfully, public IP address cannot be assigned. You can only *bind an elastic IP (EIP) address*.
- The instance must be in the Stopped status.
- The instance has existed for less than six hours.

  Note:

  After six hours, for a VPC instance in a VPC network, you can *convert public IP address to EIP address*. Instances in the classic network cannot have their public IP address converted.
- You can change the public IP address of an instance a maximum of three times.

Prerequisite

The instance must be in the Stopped status.

Procedure

To change the public IP address, follow these steps:

1. Log on to the *ECS console*.

2. In the left-side navigation pane, click Instances.
3. Select the target region.
4. Find the target instance to change the public IP address and then, in the Actions column, select More > Network and Security Group > Change Public IP.

> Note:
>
> If the instance has existed for more than six hours, the Change Public IP option in the More drop-down menu is not available.

5. Click Start Now.

   A new public IP address is displayed as shown in the following figure.

6. Click OK.

Related operation

You can *change the private IP of an ECS instance*.

3.3 Convert public IP address to EIP address

This article describes how to convert the assigned public IP address of an ECS instance in a VPC network, (referenced as VPC instance for short in this article), to an elastic public IP (EIP) address. After conversion, you can retain the public IP address and bind it to another ECS instance.

Limits

To convert a public IP address to an EIP address, consider the following limits:

- You cannot undo this action. Exercise caution when converting an assigned public IP address to an EIP address.
- Only a VPC instance assigned a public IP address is supported.
- Only a VPC instance in the Stopped or Running status is supported.
- Only a VPC instance that does not have any inactivated specification changes is supported.
- Only a VPC instance that is not within the last 24 hours of its life cycle is supported.

> Note:

- The conversion has no effect on the Internet access of the VPC instance. It does not cause transient traffic interruption.
- The billing method of the public traffic remains unchanged.
- After conversion, the EIP address is charged separately. For more information about billing of EIP addresses, see *EIP billing*. You can go to the *Usage Records* page in the Billing Management to download the Elastic Public IP usage record.

Procedure

To convert a public IP address to an elastic public IP (EIP) address, follow these steps:

1. Log on to the *ECS console*.
2. In the left-side navigation pane, click Instances.
3. Select the region.
4. Find the target VPC instance to convert the public IP address, in the Actions column, select More > Convert to EIP.
5. In the Convert to EIP dialog box, read the note and click OK.
6. Refresh the instance list.

After the public IP address is converted to an EIP address, the IP address is followed by (Elastic IP Address).

Click the IP address to go to the EIP console to manage the EIP address.

Follow-up operations

After the public IP address is converted to an EIP address, you can unbind the EIP address from the instance and bind it to another instance. You can also release the EIP address. For more information, see *unbind and release an EIP*.

Related API

You can use the *ConvertNatPublicIpToEip* interface to convert a public IP address to an EIP address. Currently, only SDK 4.3.0 or a later version supports this interface.

Download the latest SDK.

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.

Scenarios

ENIs can be used in the following scenarios:

- Deploying a high-availability cluster

  An ENI is suitable for high-availability architecture for multiple network interfaces on a single instance.
- Providing a low-cost failover solution

  You can detach an ENI from a failed ECS instance and then attach it to another ECS instance to quickly redirect the failed instance’s traffic to a backup instance, thereby quickly restoring your services.
- Managing the network with refined controls

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

ENI types

ENIs are classified into two types:

- Primary ENI

  The ENI created by default upon the creation of an instance in a VPC. The life cycle of the primary ENI is the same as that of the instance, and you cannot remove the primary ENI from the instance.
- Secondary ENI

  You can create a secondary ENI and attach it to an instance or detach it from the instance. Multiple private IPs are supported for each secondary ENI. The maximum number of ENIs that you can attach to one instance varies with the instance type. For more information, see *#unique_30*.

ENI attributes

The following table displays ENI attributes.

Attribute	Quantity
Primary private IP addresses	1
MAC address	1
Security group	Up to 5
Description	1
ENI name	1

Limitations

ENIs have the following limitations:

- By default, one account can own up to 100 ENIs per region. The quota increases with the membership level. If you require a higher quota, *open a ticket*.
- The ECS instance must be in the same zone of the same region as the ENI, but they do not have to be in the same VSwitch.
- The number of ENIs that can be attached to an ECS instance is determined by the instance type. For more information, see *#unique_30*.
- Only I/O optimized instance types support ENIs.
- Attaching multiple ENIs does not increase the instance bandwidth.

> Note:
> The instance bandwidth capability varies with the instance type.

Related operations

For images that cannot identify ENIs, log on to the instance to *configure the ENI*.

Console operations

You can complete the following operations in the ECS console:

- *Attach an ENI when creating an instance*
- *Create an ENI*
- *Delete an ENI*

- *Attach an ENI to an instance*: The instance must be in a Stopped or Running status.
- *Detach an ENI from an instance*: The instance must be in a Stopped or Running status.
- *Modify attributes of an ENI*: You can modify attributes of an ENI, including its name, security group, and description.
- When an ENI is attached to an instance, you can view the information of the ENI on the instance details page and the network interfaces page.

API operations

You can complete the following operations by using APIs:

- *Create an ENI*
- *Delete an ENI*
- *Query ENI list*
- *Attach an ENI to an instance*: The instance must be in a Stopped or Running status.
- *Detach an ENI from an instance*: The instance must be in a Stopped or Running status.
- *Modify attributes of an ENI*: You can modify attributes of an ENI, including its name, its security group, and its description.
- You can use the *DescribeInstances* interface to query the information of an ENI when the ENI is attached to an instance.

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 *#unique_47*.

- Create a separate ENI. The created ENI can be attached to an instance. For information about how to attach an ENI, 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

- You have created a VPC and a VSwitch in the VPC .
- You have created a security group in the same VPC.

Procedure

To create an ENI, follow these steps:

1. Log on to the *ECS console*.
2. In the navigation pane on the left, choose Networks and Security > ENI.
3. Select the target region.
4. Click Create ENI.
5. In the Create ENI 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 status, it is created successfully.

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 *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. Log on to the *ECS console*.
2. In the left-side navigation pane, choose Networks and Security > ENI.
3. Select the target region.
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 *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

This topic describes how to configure an ENI. For some images used by your instances, you may need to manually configure an ENI for these images so that the ENIs attached to your instances can be identified by the system.

Background information

If your instance is running one of the following images, ENIs are supported and you do not need to configure any ENIs manually.

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

If your instance is running an image not shown in the preceding list, and you want to attach an ENI to your instance, you must manually configure the ENI to be supported . This topic uses an instance running CentOS 7.2 64-bit as an example to describe how to configure an ENI manually.

Prerequisite

You have attached an ENI to an ECS instance.

Procedure

To configure an ENI manually, follow these steps:

1. Use the *DescribeNetworkInterfaces* interface or log on to the ECS console to obtain the following attributes of the ENI: the primary private IP address, subnet mask, the default route, and the MAC address. To obtain these attributes in the ECS console, follow these steps:

   a. Log on to the *ECS console*.

   b. Find the target ENI and obtain its primary private IP address, subnet mask, default route, and MAC address. Example:

   ```
   eth1   10 . 0 . 0 . 20 / 24   10 . 0 . 0 . 253   00 :  16 :  12
   :  E7 :  27
   eth2   10 . 0 . 0 . 21 / 24   10 . 0 . 0 . 253   00 :  16 :  12
   :  16 :  EC
   ```

2. *Connect to the ECS instance*.

3. Run the following command to generate the config file: `cat / etc / sysconfig / network - scripts / ifcfg -[ network interface name in the OS ]`.

Note:

- Pay attention to the relation between the network interface name in the OS and the MAC address.
- Pay attention to the relation between the network interface name in the OS and the MAC address. The default route must be set to `DEFROUTE = no`. Other editions must have the same configuration. Note that running the `ifup` command may change the active default route configuration after configuring the network interface.
- 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 : 27
 DEFROUTE = noDefroute  =  No
```

4. To start the network interface, follow these steps:

   a. Run the `ifup [ network interface name in the OS ]` command to start the dhclient process, and initiate a DHCP request. Example:

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

   b. After a response is received, run the `ip a` a command to check the IP allocation on the network interfaces, which must match with the information displayed on the ECS console. Example:

```
#  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  loInet  125 . 0 . 0
 . 1 / 8  Scope  host  Lo
 valid_lft  forever  preferred_ lft  forever
```

```
2 :  eth0 :  mtu   1500   qdisc   pfifo_fast   state   UP   qlen
  10002 :  eth0 :  MTU   1500   qdisc   glasstate   up   qlen
1000
link / ether   00 : 16 : 3e : 0e : 16 : 21   brd   ff : ff : ff :
ff : ff : ff
Inet   10 . 0 . 0 . 19 / 24   BRD   glasscope   Global   Dynamic
  eth0
valid_lft   31506157se  c   preferred_  lft   31506157se
cValid_lft   31506157se  c   preferred_  lft   31506157se  c
3 :  eth1 :  MTU   1500   qdisc   glasstate   up   qlen   1000
link / ether   00 : 16 : 3e : 12 : e7 : 27   brd   ff : ff : ff :
ff : ff : ff
inet   10 . 0 . 0 . 20 / 24   brd   10 . 0 . 0 . 255   scope
  global   dynamic   eth1Inet   10 . 0 . 0 . 20 / 24   BRD
glasscope   Global   Dynamic   eth1
Valid_lft   31525994se  c   preferred_  lft   31525994se  c
4 :  eth2 :  MTU   1500   qdisc   glasstate   up   qlen   1000
Link / ether   00 :  16 :  Rye :  12 :  16 :  ec   brd   ff :  FF
:  FF
inet   10 . 0 . 0 . 21 / 24   brd   10 . 0 . 0 . 255   scope
global   dynamic   eth2
valid_lft   31526009se  c   preferred_  lft   31526009se  c
```

5. Set the metric for each network interface in the route table. In this example, set the metric parameters of eth1 and eth2 as follows.

```
eth1 :  gw :  10 . 0 . 0 . 253   metric :  1001
eth2 :  gw :  10 . 0 . 0 . 253   metric :  1002
```

   a. Run the following command to set the metric parameters.

```
#  Ip - 4   route   add   default   via   glasdev   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 configuration is successful. Example:

```
#  route  - n
 Kernel   IP   routing   table
 Destinatio  n   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 . 5 . 0 . 0   10 . 0 . 0 . 253   ug   ub1002   0   0   eth2
 10 . 0 . 0 . 0   0 . 5 . 0 . 0   255 . 25 . 25 . 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 . 5 . 0 . 0   255 . 25 . 25 . 0   u   0   0
 0   eth2
 169 . 254 . 0 . 0   0 . 0 . 0   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    eth2169 . 254 . 0 . 0    0 . 0 . 0    255 . 0 . 0    U
1004    0    0    eth2
```

6. To build a route table, follow these steps:

   > Note:
   >
   > We recommend that you use the metric value as the route table name.

   a. Run the following command to build a route table.

   ```
   #  ip  - 4   route   add   default   via   10 . 0 . 0 . 253   dev
      eth1   table   1001
   #  Ip - 4   route   add   default   via   glasdev   eth2   table
    1002
   ```

   b. Run the following command to check whether the route table is built successfully.

   ```
   #  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 the policy routing.

   a. Run the following command to configure the policy routing.

   ```
   #  ip  - 4   rule   add   from   10 . 0 . 0 . 20   lookup   1001
   #  ip  - 4   rule   add   from   10 . 0 . 0 . 21   lookup   1002
   ```

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

   ```
   #  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 to do next

After you have configured an ENI, you can perform the following operations:

- *Modify attributes of an ENI*.
- *Detach an ENI from an instance*.
- *Delete an ENI*.

4.5 Modify attributes of an ENI

You can modify the attributes of a secondary ENI.

You can only modify the attributes of a secondary ENI, including:

- The name of the secondary ENI.
- The security group associated with the secondary ENI. Each ENI must be associated with at least one security group, and can be associated with up to five security groups.
- The description of the secondary ENI.

You can modify the attributes of a secondary ENI when it is in the Available or the Bound status. This topic describes how to modify attributes of an ENI in the ECS console.

Prerequisite

Before you modify attributes of an ENI, you must first *create an ENI*.

Procedure

To modify the attributes of a secondary 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 Modify.
5. In the Modify dialog box, complete the following configurations as required:
   - Network Interface Name: Specify a new name for the selected ENI.
   - Security Group: Select additional security groups for the ENI, or remove the ENI from security groups that no longer require the ENI. Note that the ENI must be kept in at least one security group.
   - Description: Enter a description for the ENI.
6. Click OK.

4.6 Assign multiple secondary private IP addresses

You can assign one or more secondary private IP addresses to an Elastic Network Interface (ENI).

Scenarios

- High instance usage

  If your server hosts multiple applications, you can assign multiple secondary private IP addresses to an ENI to extend the utilization of your instance. Each application is then represented by a separate service IP address.
- Failover transfer

  If your instance fails, you can quickly transfer traffic to the IP address of other standby instances.

Limits

- You can only attach an ENI to a VPC ECS instance in the same VPC.
- A single VPC security group can contain a maximum of 2,000 private IP addresses (shared by the primary and secondary ENIs).
- You can assign a maximum of 20 private IP addresses to an ENI.
  - When an ENI is in `Available` state, you can assign a maximum of 10 private IP addresses to the ENI.
  - When an ENI is in `InUse` state, the number of private IP addresses that you can assign to the ENI depends on the instance type. For more information, see *Instance type families*.

Prerequisites

- Your instance type can be assigned with multiple secondary private IP addresses. For more information, see *DescribeInstanceTypes*.
- The ENI must be in `Available` or `InUse` state.
- When you assign secondary private IP addresses to the primary ENI, the instances attached to the primary ENI must be in `Running` or `Stopped` state.

Assign multiple secondary private network IP addresses to a Windows instance

1. Open Network and Sharing Center .
2. ClickChange Adapter Settings.

3. Double-click the current network connection name, and then clickProperties.
4. Double-click Internet Protocol Version 4 (TCP/IPv4).
5. Select Use the Following IP Address, and then clickAdvanced.
6. ClickAdd, and then enter the assigned IP address and subnet mask. You can add multiple IP addresses.
7. Click OK.

Assign multiple secondary private IP addresses to a Linux instance

1. Use the *AssignPrivateIpAddresses* API to assign multiple secondary private IP addresses.
2. Use the *DescribeNetworkInterfaces* API to query the assigned secondary private IP addresses.
3. *Connect to an instance by using the Management Terminal*.

4. Configure the assigned IP addresses.

Release	Applicable version	Procedure

RHEL series	- CentOS 6 /7
	- Red Hat 6 /7
	- Aliyun Linux 17
		a. If the ENI is eth0, run the `vi / etc / sysconfig / network - scripts / ifcfg - eth0 : 0` command to open the network configuration file and 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 multiple IP addresses are assigned, run the `vi / etc / sysconfig / network - scripts / ifcfg - eth0 : 1` command to open the network configuration file and 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 service.

Release	Applicable version	Procedure

Debian series	· Ubuntu 14/16
	· Debian/8 /9
		a. If the ENI is eth0, 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  < IPv6  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 service.

SLES series	· SUSE 11/ 12
	· OpenSUSE 42
		a. If the ENI is eth0, 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 service.

What to do next

When your ENI does not require multiple secondary private IP addresses, you can*Revoke multiple secondary private IP addresses*.

4.7 Revoke multiple secondary private IP addresses

You can revoke one or more secondary private IP addresses assigned to an Elastic Network Interface (ENI) when the ENI no longer needs them.

Limits

- The primary private IP address cannot be revoked.
- You can only attach an ENI to a VPC ECS instance in the same VPC.
- A single VPC security group can contain a maximum of 2,000 private IP addresses (shared by the primary and secondary ENIs).

Prerequisites

- You have assigned multiple secondary private IP addresses to your ENI.
- The ENI is in `Available` or `InUse` status.
- When you revoke secondary private IP addresses assigned to the primary ENI, the instances attached to the primary ENI must be in `Running` or `Stopped` state.

Procedure

1. Use the *DescribeNetworkInterfaces* API to query the assigned secondary private IP addresses.
2. Use the *UnassignPrivateIpAddresses* API to revoke the assigned secondary private IP addresses.

What to do next

If you want to increase the usage of your instance or implement a failover transfer, you can *Assign multiple secondary private IP addresses* to an ENI.

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 status.
- The instance to which the ENI belongs must be in the Stopped or Running status.

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 status.

Procedure

To detach a secondary ENI from an instance, 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 Unbind.
5. In the Unbind 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 status, it is successfully 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*.

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_30* 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 :

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.

- To check whether the NIC supports multi-queue, run the command: `ethtool -l eth0`.
- To enable multi-queue for the NIC, run the command: `ethtool -L eth0 combined 2`.

- 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:

```
   #!/ 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 } f "
    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/admin64 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

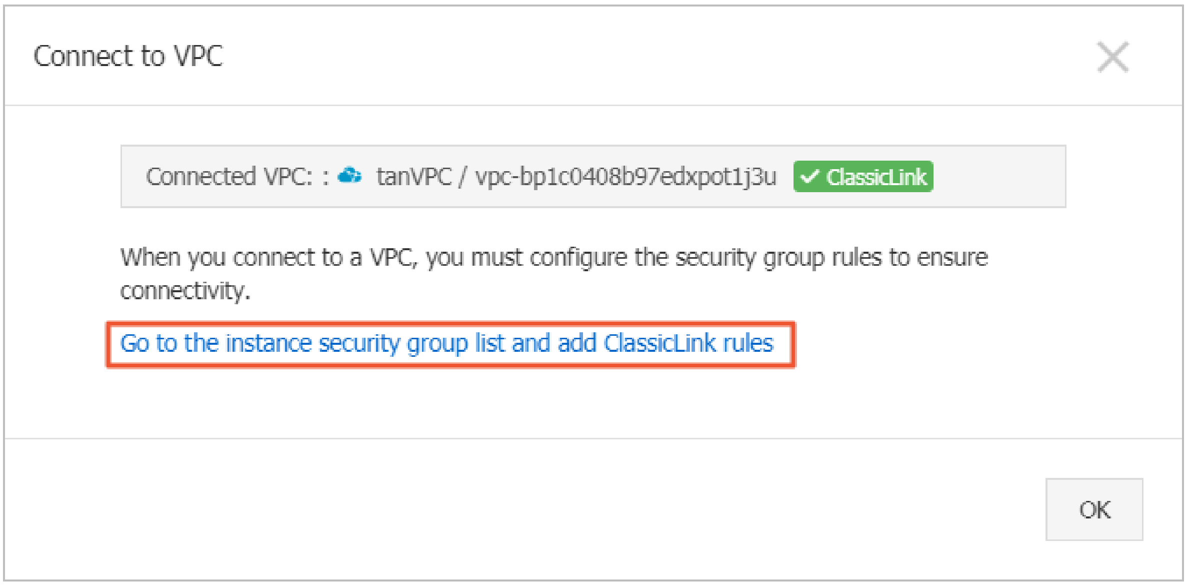
This topic describes how to connect a classic network to a VPC. You can set up a ClassicLink connection so that ECS instances of the classic network type can access cloud resources in a VPC network through the intranet.

Prerequisites

Make sure that you are aware of the limitations of ClassicLink. For more information, see *ClassicLink overview*.

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. Log on to the *ECS console*.
5. In the left-side navigation pane, click Instances.
6. Choose More > Network and Security Group > Connect to VPC.
7. In the displayed dialog box, select the target VPC and click OK. Then click the security group configuration link.



Connect to VPC

Connected VPC: : tanVPC / vpc-bp1c0408b97edxpot1j3u ✓ ClassicLink

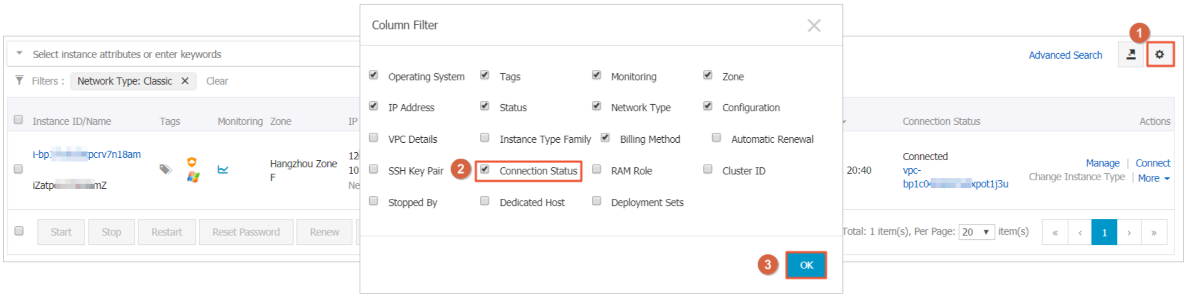
When you connect to a VPC, you must configure the security group rules to ensure connectivity.

Go to the instance security group list and add ClassicLink rules
OK

8. Click Add ClassicLink Rules and configure the security rule according to the following information. Then, click OK.

Configuration	Description
Classic Security Group	Display the classic network security group.
Select VPC Security Group	Select a security group to use. Up to five security groups can be selected.
Mode	Select one of the following modes: · `Classic <=> VPC` : The connected resources can access each other (recommended). · `Classic => VPC` : Authorize the classic ECS instance to access cloud resources in the connected VPC. · `VPC => Classic` : Authorize the cloud resources in the connected VPC to access the classic ECS instance.
Protocol Type and Port Range	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`.
Priority	Set the priority for the rule. A smaller number represents a higher priority, for example, `1`.
Description	Enter a description for the security rule.

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


Column Filter

☑ Operating System ☑ Tags ☑ Monitoring ☑ Zone
☑ IP Address ☑ Status ☑ Network Type ☑ Configuration
□ VPC Details □ Instance Type Family ☑ Billing Method □ Automatic Renewal
□ SSH Key Pair ☑ Connection Status □ RAM Role □ Cluster ID
□ Stopped By □ Dedicated Host □ Deployment Sets

Select instance attributes or enter keywords
Filters : Network Type: Classic ✕ Clear

Instance ID/Name	Tags	Monitoring	Zone	IP		Connection Status	Actions
i-bp[redacted]pcrv7n18am iZatp[redacted]mZ			Hangzhou Zone F	12 10 Ne	20:40	Connected vpc-bp1c0[redacted]xpot1j3u	Manage | Connect Change Instance Type | More

Total: 1 item(s), Per Page: 20 item(s)

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