

ALIBABA CLOUD

阿里云

云服务器ECS
网络

文档版本：20220711

 阿里云

法律声明

阿里云提醒您在使用或阅读本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
 危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 危险 重置操作将丢失用户配置数据。
 警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	 警告 重启操作将导致业务中断，恢复业务时间约十分钟。
 注意	用于警示信息、补充说明等，是用户必须了解的内容。	 注意 权重设置为0，该服务器不会再接受新请求。
 说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击设置>网络>设置网络类型。
粗体	表示按键、菜单、页面名称等UI元素。	在结果确认页面，单击确定。
Courier字体	命令或代码。	执行 <code>cd /d C:/window</code> 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] 或者 [a b]	表示可选项，至多选择一个。	<code>ipconfig [-all -t]</code>
{ } 或者 {a b}	表示必选项，至多选择一个。	<code>switch {active stand}</code>

目录

1.网络类型	07
2.实例IP地址介绍	08
2.1. 专有网络的IP	08
2.2. 经典网络的IP	09
2.3. 弹性公网IP	09
2.4. IPv6地址	11
2.5. 内网	12
3.管理IPv4地址	14
3.1. 修改私有IP地址	14
3.2. 更换公网IP地址	14
3.3. 绑定和解绑弹性公网IP	15
3.4. 专有网络类型ECS公网IP转为弹性公网IP	16
3.5. 经典网络类型ECS公网IP转为弹性公网IP	17
4.配置IPv6地址	20
4.1. Windows实例配置IPv6地址	20
4.1.1. Windows实例使用IPv6导航	20
4.1.2. 步骤1：搭建IPv6 VPC	20
4.1.3. 步骤2：分配IPv6地址	21
4.1.4. 步骤3：开通IPv6公网带宽	22
4.1.5. 步骤4：配置IPv6地址	22
4.1.6. 步骤5：添加IPv6安全组规则	24
4.1.7. 步骤6：测试网络连通性	25
4.1.8. 步骤7：（可选）删除IPv6地址	25
4.2. Linux实例配置IPv6地址	26
4.2.1. Linux实例使用IPv6导航	26
4.2.2. 步骤1：搭建IPv6 VPC	26

4.2.3. 步骤2：分配IPv6地址	27
4.2.4. 步骤3：开通IPv6公网带宽	28
4.2.5. 步骤4：配置IPv6地址	28
4.2.6. 步骤5：添加IPv6安全组规则	38
4.2.7. 步骤6：测试网络连通性	38
4.2.8. 步骤7：（可选）删除IPv6地址	39
5.查看IP地址	40
6.弹性网卡	42
6.1. 弹性网卡概述	42
6.2. 托管弹性网卡	48
6.3. 创建弹性网卡	48
6.4. 绑定弹性网卡	50
6.5. 配置辅助弹性网卡	53
6.6. 分配辅助私网IP地址	63
6.7. 回收辅助私网IP地址	72
6.8. 修改弹性网卡	73
6.9. 编辑弹性网卡标签	75
6.10. 解绑弹性网卡	75
6.11. 删除弹性网卡	76
6.12. 基于弹性网卡操作完成事件实现业务自动化处理	77
7.弹性RDMA网卡	84
7.1. 使用ERI	84
7.2. 在RDMA增强型实例上部署Redis	86
7.3. 基于RDMA增强型实例部署HPC应用	89
7.4. 基于RDMA增强型实例部署Spark集群	94
8.前缀列表	98
8.1. 前缀列表概述	98
8.2. 创建前缀列表	98

8.3. 克隆前缀列表	100
8.4. 管理前缀列表条目	100
8.5. 删除前缀列表	102
8.6. 为RAM用户授予前缀列表相关权限	102
8.7. 使用前缀列表提高安全组规则管理的效率	104
9.更换ECS实例的VPC	107
10.配置网卡多队列	109
11.设置网卡MTU值	112
12.经典网络迁移到专有网络（新版）	115
12.1. ECS实例从经典网络迁移到专有网络	115
12.2. 经典网络实例全部迁移到VPC最佳实践	124
12.3. 经典网络实例部分迁移到VPC最佳实践	130
13.经典网络和专有网络互通	140
14.网络FAQ	143

1. 网络类型

云服务器ECS支持的网络类型包括专有网络和经典网络。

专有网络

专有网络（Virtual Private Cloud，简称VPC）是您基于阿里云构建的一个隔离的网络环境，专有网络之间逻辑上彻底隔离。您可以自定义这个专有网络的拓扑和IP地址，适用于对网络安全要求较高和有一定网络管理能力的用户。

更多信息，请参见[什么是专有网络](#)。

经典网络

经典网络类型的云产品，统一部署在阿里云公共基础设施内，规划和管理由阿里云负责，更适合对网络易用性要求比较高的用户。

 **说明** 如果您在2017年6月14日17点（UTC+8）以后第一次创建ECS实例，不能选择经典网络。

功能差异

专有网络和经典网络的功能差异如下表所示。

比较点	专有网络	经典网络
二层逻辑隔离	支持	不支持
自定义私网网段	支持	不支持
私网IP规划	专有网络内唯一，专有网络间可重复	经典网络内唯一
私网互通	专有网络内互通，专有网络间隔离	同一账号同一地域内互通
隧道技术	支持	不支持
自定义路由器	支持	不支持
路由表	支持	不支持
交换机	支持	不支持
SDN	支持	不支持
自建NAT网关	支持	不支持
自建VPN	支持	不支持

以下视频将为您形象地描述云服务器ECS两种不同网络类型的特点。

2. 实例IP地址介绍

2.1. 专有网络的IP

IP地址是您访问ECS实例或者您的用户访问部署在ECS实例上的服务的主要方式。专有网络VPC类型的ECS实例有两种IP地址，分为私有IP地址和公网IP地址。

私有IP地址

根据实例所属的专有网络VPC和虚拟交换机网段，专有网络VPC类型ECS实例一经创建即被分配一个私有IP地址。

私有IP地址可以用于以下场景：

- 负载均衡。
- 同一局域网内ECS实例之间内网互访。
- 同一局域网内ECS实例与其他云服务（如OSS、RDS）之间内网互访。

您可以根据业务需要，在ECS管理控制台上修改私有IP地址。具体操作，请参见[修改私有IP地址](#)。关于更多内网通讯的信息，请参见[内网](#)。

公网IP地址

专有网络VPC类型的ECS实例支持两种公网IP地址：

- ECS系统分配的公网IP地址（PublicIP）。
- 弹性公网IP（EIP）地址。更多信息，请参见[弹性公网IP](#)。

专有网络两种公网IP地址的主要区别如下表所示：

维度	ECS系统分配的公网IP地址（PublicIP）	弹性公网IP（EIP）地址
使用场景	如果希望在创建ECS实例时由ECS系统自动分配一个公网IP地址，释放实例时这个公网IP地址随实例一起释放，不保留该公网IP地址，您可以选择PublicIP。	如果希望长期使用某个公网IP地址，根据业务需要将它绑定到指定的ECS实例上，您可以选择弹性公网IP（EIP）。EIP可以反复绑定和解绑。释放实例后，EIP仍然存在。
获取方式	在创建ECS实例时，如果您选择 分配公网IPv4地址 ，实例即被分配一个PublicIP。	单独申请EIP地址，并绑定到未分配PublicIP的ECS实例上。具体操作，请参见 申请EIP 和 绑定EIP 。
分配上限	一台ECS实例只能分配一个PublicIP。	一台ECS实例可以关联多个EIP，通过设置多EIP网卡可见模式实现。更多信息，请参见 设置多EIP网卡可见模式（停止接受使用申请） 。
解绑方式	PublicIP一经分配，只能释放，不能解绑。您可以按需将PublicIP转换为EIP，EIP可以随时与ECS实例解绑或绑定。具体操作，请参见 专有网络类型ECS公网IP转为弹性公网IP 。	EIP支持解绑。具体操作，请参见 解绑EIP 。
释放方式	<ul style="list-style-type: none"> • 释放实例时，PublicIP地址随实例一起释放。 • 在实例的使用期间，将带宽值设置为0 Mbit/s，可以释放PublicIP。包年包月实例请参见包年包月实例修改带宽，按量付费实例请参见按量付费实例修改带宽。 	更多信息，请参见 释放按量计费EIP实例 。
如何查看MAC地址	VPC类型的ECS实例的公网访问通过私有网卡映射完成。所以，无论您的实例是否分配或者绑定了公网IP地址，在实例内部您都无法查询到公网网卡。	

计费

阿里云只对公网出网带宽收取费用，入网带宽免费。更多公网带宽的计费信息，请参见[公网带宽计费](#)。

2.2. 经典网络的IP

IP地址是您访问ECS实例或者您的用户访问部署在ECS实例的服务的主要方式。经典网络IP地址由阿里云统一分配，分为内网IP地址和公网IP地址。

内网IP地址

每台经典网络类型ECS实例一定会被分配一个IP地址用于内网通信，这个IP地址被称为内网IP地址。关于内网通信的详细信息，请参见[内网](#)。

 **说明** 经典网络内网IP地址不支持组播和广播。

内网IP地址可以应用于以下场景：

- 负载均衡。
- 同一局域网内ECS实例之间内网互访。
- 同一局域网内ECS实例与其他云服务（如对象存储OSS或者云数据库RDS）之间内网互访。

经典网络类型ECS实例一经分配了内网IP地址后，不支持修改。禁止在操作系统内部自行变更内网IP地址，否则会导致内网通讯中断。

公网IP地址

如果您购买了公网带宽，即公网带宽不为0 Mbit/s，阿里云会为您的经典网络类型实例分配一个公网IP地址。

公网IP地址可以应用于以下场景：

- ECS实例与公网（Internet）之间互访。
- 不在同一局域网内的ECS实例与其他云服务之间互访。

公网IP地址相关操作如下：

- 在创建ECS实例时，只要您选择**分配公网IP地址**，您的ECS实例就会分配一个公网IP地址。具体操作，请参见[使用向导创建实例](#)。

 **说明** 经典网络类型ECS实例一经分配公网IP地址，该公网IP地址既不能释放，也不能解绑。即使您通过续费降配或者按量实例更改带宽等功能将公网带宽值设为0 Mbit/s，您的实例不能访问公网，但公网IP地址仍会保留。

- 如果在创建ECS实例时未分配公网IP地址，您可以通过修改公网出网带宽分配。包年包月ECS实例请参见[包年包月实例修改带宽](#)，按量付费ECS实例请参见[按量付费实例修改带宽](#)。
- 您可以在成功创建ECS实例的六小时内修改公网IP地址。具体操作，请参见[更换公网IP地址](#)。
- 手动释放经典网络类型ECS实例时，您可以将公网IP转换为弹性公网IP（Elastic IP，简称EIP）。转换后，EIP可绑定到专有网络VPC类型的ECS实例上，适用于网络迁移、弹性绑定、灵活升降带宽等场景。更多信息，请参见[经典网络类型ECS公网IP转为弹性公网IP](#)。

计费

内网通信产生的流量免费，即使用内网IP地址不产生流量费用。

公网出网带宽收取费用，入网带宽免费。更多公网带宽的计费信息，请参见[公网带宽计费](#)。

2.3. 弹性公网IP

阿里云弹性公网IP（Elastic IP Address，简称EIP）是可以独立购买和持有的公网IP地址资源。如果您希望长期使用某个公网IP地址，根据业务需要将它绑定或解绑指定的专有网络VPC类型ECS实例上，您可以选择EIP。

EIP概述

EIP是一种NAT IP，位于阿里云的公网网关上，通过NAT方式映射到被绑定的ECS实例的主网卡上。因此，绑定了EIP的专有网络类型ECS实例可以直接使用这个IP进行公网通信。EIP地址和公网IP地址（PublicIP）一样，无法在ECS实例的操作系统内看到。

EIP与PublicIP的差异

专有网络VPC类型的ECS实例支持公网IP地址（PublicIP）和EIP两种公网IP地址。两者的使用场景和主要区别如下表所示。

维度	ECS系统分配的公网IP地址（PublicIP）	弹性公网IP（EIP）地址
使用场景	如果希望在创建ECS实例时由ECS系统自动分配一个公网IP地址，释放实例时这个公网IP地址随实例一起释放，不保留该公网IP地址，您可以选择PublicIP。	如果希望长期使用某个公网IP地址，根据业务需要将它绑定到指定的ECS实例上，您可以选择弹性公网IP（EIP）。EIP可以反复绑定和解绑。释放实例后，EIP仍然存在。
获取方式	在创建ECS实例时，如果您选择分配公网IPv4地址，实例即被分配一个PublicIP。	单独申请EIP地址，并绑定到未分配PublicIP的ECS实例上。具体操作，请参见 申请EIP 和 绑定EIP 。
分配上限	一台ECS实例只能分配一个PublicIP。	一台ECS实例可以关联多个EIP，通过设置多EIP网卡可见模式实现。更多信息，请参见 设置多EIP网卡可见模式（停止接受使用申请） 。
解绑方式	PublicIP一经分配，只能释放，不能解绑。您可以按需将PublicIP转换为EIP，EIP可以随时与ECS实例解绑或绑定。具体操作，请参见 专有网络类型ECS公网IP转为弹性公网IP 。	EIP支持解绑。具体操作，请参见 解绑EIP 。
释放方式	<ul style="list-style-type: none"> 释放实例时，PublicIP地址随实例一起释放。 在实例的使用期间，将带宽值设置为0 Mbit/s，可以释放PublicIP。包年包月实例请参见包年包月实例修改带宽，按量付费实例请参见按量付费实例修改带宽。 	更多信息，请参见 释放按量计费EIP实例 。
如何查看MAC地址	VPC类型的ECS实例的公网访问通过私有网卡映射完成。所以，无论您的实例是否分配或者绑定了公网IP地址，在实例内部您都无法查询到公网网卡。	

计费方式

EIP支持包年包月和按量付费计费方式。更多信息，请参见[计费概述](#)。

使用限制

EIP可以绑定ECS实例或弹性网卡。当EIP绑定ECS实例时，ECS实例有以下限制条件：

- 网络类型必须是专有网络VPC。
- 地域必须和EIP的地域相同。
- 必须处于运行中或已停止状态。
- 实例的主网卡上没有绑定公网IP地址。

相关操作

- [申请EIP](#)

您可以在[弹性公网IP管理控制台](#)上单独申请EIP，然后绑定到未分配公网IP地址的专有网络VPC类型ECS实例上。具体操作，请参见[申请EIP](#)。

说明 一台ECS实例可以关联多个EIP，通过设置多EIP网卡可见模式实现。更多信息，请参见[设置多EIP网卡可见模式（停止接受使用申请）](#)。

- ECS实例绑定EIP
 - 您可以在[ECS管理控制台](#)，将EIP绑定到未分配公网IP地址的专有网络VPC类型ECS实例上。具体操作，请参见[绑定EIP](#)。
 - 您也可以[在弹性公网IP管理控制台](#)，将EIP绑定到未分配公网IP地址的专有网络VPC类型ECS实例上。具体操作，请参见[绑定ECS实例](#)。
- EIP绑定辅助弹性网卡

您可以在[弹性公网IP管理控制台](#)将EIP与弹性网卡ENI（Elastic Network Interface）进行绑定。弹性网卡本身提供一个私网IP，在绑定EIP后，弹性网卡相当于同时具备了私网IP和公网IP。更多信息，请参见[绑定辅助弹性网卡](#)。
- ECS实例解绑EIP
 - 如果您的ECS实例不再需要EIP，您可以在[ECS管理控制台](#)上将EIP从ECS实例上解绑。具体操作，请参见[解绑EIP](#)。
 - 您也可以[在弹性公网IP管理控制台](#)上将EIP从ECS实例上解绑。具体操作，请参见[解绑云资源](#)。
- 释放EIP

解绑后的EIP仍会继续收费，如果不再使用，您可以在[弹性公网IP管理控制台](#)上释放EIP。更多信息，请参见[释放按量计费EIP实例](#)。
- 续费EIP

如果您的EIP采用的是包年包月计费方式，包年包月类型的EIP实例到期后会保留7天，您可以在到期后7天内续费，否则EIP实例将被自动释放。更多信息，请参见[续费](#)。

关于EIP的更多信息，请参见[EIP实例概述](#)。

2.4. IPv6地址

IPv4的应用范围虽广，但网络地址资源有限，制约了互联网的发展。IPv6地址不仅可以解决网络地址资源有限的问题，还可以解决多种接入设备连入互联网障碍的问题。云服务器ECS同时支持IPv4和IPv6地址。

IPv6的优势

对比项	IPv4	IPv6
地址长度	32位（4个字节）	128位（16个字节）
地址数量	2 ³² 个	2 ¹²⁸ 个
格式	xxx.xxx.xxx.xxx 其中，0≤xxx≤255，每个x都是十进制数，可省略前导零。 示例：192.168.1.1	xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx 其中，每个x都是十六进制数，可省略前导零。可在地址的文本格式中使用一次双冒号 (::)，用于指定任意数目的0位。 示例： CDCD:0000:0000:0000:8475:1111:3900:2020=CDCD::8475:1111:3900:2020

对比项	IPv4	IPv6
地址解析协议	通过ARP广播请求帧将IP地址解析为链路层地址	通过多播邻居请求消息将IP地址解析为链路层地址
安全性	安全机制建立于应用程序级，无法从IP层来保证网络的安全	支持IP分组的私密和数据完整性，从IP层来保证网络的安全
LAN连接	通过网络接口到达物理网络	可与任何以太网适配器配合使用，并且可以通过虚拟以太网在逻辑分区间使用
地址类型	<ul style="list-style-type: none"> 单点广播地址 多点广播地址 广播地址 	<ul style="list-style-type: none"> 单点广播地址 多点广播地址 任意广播地址

使用限制

- 网络类型：仅专有网络VPC类型的ECS实例支持IPv6地址。
- 实例规格：关于实例是否支持IPv6的更多信息，请参见[实例规格族](#)。
- IPv6地址数量：每台ECS实例可以配置1个或多个IPv6地址，数量由实例规格确定。更多信息，请参见[实例规格族](#)。
- 公网访问：IPv6地址支持VPC内网通信。如果要通过IPv6地址访问公网或被公网访问，您必须开通IPv6公网带宽。具体操作，请参见[步骤3：开通IPv6公网带宽](#)或者[步骤3：开通IPv6公网带宽](#)。

2.5. 内网

如果两台同城域的ECS实例之间需要传输数据，建议使用内网连接。云服务器ECS与云数据库、负载均衡以及对象存储之间也可以使用内网相互连接使用。

云服务器ECS内网间，非I/O优化的实例为千兆共享带宽，I/O优化的实例为万兆或25 GB共享带宽。由于是共享网络，因此无法保证带宽速度是不变的。

对于内网中的ECS实例：

- ECS实例的网络类型、所属账号、地域、安全组等都会影响内网通信。具体信息，如下表所示。

网络类型	所属账号	地域	安全组	如何实现内网互通
VPC（同一VPC）	同一账号或不同账号	同一地域	同一安全组	默认互通，也可以实现安全组内网络隔离。更多信息，请参见 普通安全组内网络隔离 。
			不同安全组	安全组授权实现内网互通。更多信息，请参见 安全组应用案例ECS安全组配置操作指南 。
VPC（不同VPC）	同一账号或不同账号	同一地域	不同安全组	通过高速通道实现网络互通。更多信息，请参见 应用场景 。
		不同地域		
经典网络	同一个账号	同一地域	同一安全组	默认互通。
	不同账号	同一地域	不同安全组	安全组授权实现内网互通。更多信息，请参见 安全组应用案例ECS安全组配置操作指南 。

-
- 专有网络的私有IP地址可以修改。具体操作，请参见[修改私有IP地址](#)。不能修改或更换经典网络类型的ECS实例的私有IP地址。
 - 您可以使用专有网络VPC的ClassicLink功能，使经典网络类型的ECS实例通过私网访问VPC网络内的云资源。更多信息，请参见[ClassicLink](#)。

3. 管理IPv4地址

3.1. 修改私有IP地址

您可以直接修改专有网络中ECS实例的私有IP，也可以通过更改ECS实例所属的交换机来更改ECS实例的私有IP。

前提条件

- 实例的弹性网卡未设置辅助私网IP地址。
- 实例处于已停止状态。

操作步骤

1. 登录[ECS管理控制台](#)。
2. 在左侧导航栏，选择实例与镜像 > 实例。
3. 在顶部菜单栏左上角处，选择地域。
4. 找到目标实例，在操作区域选择更多 > 网络和安全组 > 修改私有IP。
5. 在修改私有IP对话框，完成配置，然后单击修改。
 - 如果您要更换交换机，请确保所选交换机的可用区和实例的可用区相同。
 - 如果您不需要更换交换机，则直接修改私有IP即可。

修改私有IP

实例: i-lbp-1n3d3qg-1j2p3rwm3kx6a

可用区: cn-hangzhou-i

交换机: vsw-lbp-1n3d3qg-1j2p3rwm3kx6a(172.16.0.0/20) 有4084个可用私有IP
交换机与实例必须在相同的可用区。

私有IP: 172.16.1.244
指定的私有IP必须为交换机网段中的未被占用的私有IP，如果不指定将自动为云服务器实例分配一个空闲的私有IP。

修改 取消

6. 在操作区域选择更多 > 实例状态 > 启动。

说明 ECS实例重新启动后，修改的私有IP生效。

相关文档

- [ModifyInstanceVpcAttribute](#)

3.2. 更换公网IP地址

如果您的ECS实例分配了公网IP地址，无论是经典网络还是专有网络VPC，在创建后六小时内，您都可以更换公网IP地址。

前提条件

更换公网IP地址之前，请确保ECS实例已满足以下条件：

- 处于已停止（`Stopped`）状态。

说明 如果实例的计费方式为按量付费、网络类型为专有网络，在停止实例时需要启用普通停机模式。如果启用节省停机模式，在控制台操作界面无法看到更换公网IP选项。

- 已经分配了公网IP地址。
- 成功创建不足六小时。

说明 如果ECS实例不满足以上条件，在控制台操作界面无法看到更换公网IP选项。

背景信息

更换公网IP地址操作有以下限制：

- 一台实例最多只能更换三次公网IP地址。
- 如果在创建实例时未分配公网IP地址，则不适用于本文操作。但您可以通过以下方法重新分配：
 - 申请和绑定弹性公网IP，具体操作，请参见[弹性公网IP文档申请EIP](#)。
 - 变更实例公网带宽，从而分配一个固定公网IP地址。包年包月实例的更多信息，请参见[升降配方式概述](#)，按量付费实例的更多信息，请参见[按量付费实例修改带宽](#)。

操作步骤

1. 登录[ECS管理控制台](#)。
2. 在左侧导航栏，选择实例与镜像 > 实例。
3. 在顶部菜单栏左上角处，选择地域。
4. 找到更换公网IP地址的实例，单击更多 > 网络和安全组 > 更换公网IP。
5. 在更换公网IP对话框中，单击开始更换。
更换成功后，对话框会显示新的公网IP地址。
6. 单击确定。

3.3. 绑定和解绑弹性公网IP

阿里云弹性公网IP（Elastic IP Address，简称EIP）是可以独立购买和持有的公网IP地址资源。您可以单独申请EIP地址，并绑定到未分配公网IP地址的专有网络VPC类型ECS实例上，使ECS实例可以访问公网。

前提条件

如果您需要为ECS实例绑定EIP，请确保ECS实例满足以下条件：

- 网络类型必须是专有网络VPC。
- 地域必须和EIP的地域相同。
- 实例必须处于运行中或已停止状态。
- 实例主网卡没有绑定公网IP地址。

绑定EIP

1. 登录[ECS管理控制台](#)。

2. 在左侧导航栏，选择实例与镜像 > 实例。
3. 在顶部菜单栏左上角处，选择地域。
4. 找到待绑定EIP的ECS实例，单击更多 > 网络和安全组 > 绑定弹性IP。
5. 在绑定弹性IP对话框中，选择已申请的EIP。

如果没有可选择的EIP，您可以在选择框右侧单击创建弹性公网IP先去创建EIP。具体操作，请参见[申请EIP](#)。

6. 单击确定。
绑定成功后，在ECS实例页面的IP地址列会显示已绑定的EIP，例如：192.168.XX.XX（弹性）。

解绑EIP

1. 登录[ECS管理控制台](#)。
2. 在左侧导航栏，选择实例与镜像 > 实例。
3. 在顶部菜单栏左上角处，选择地域。
4. 找到待解绑EIP的ECS实例，单击更多 > 网络和安全组 > 解绑弹性IP。
5. 在解绑弹性IP对话框中，确认提示信息。

6. 单击确定。
解绑成功后，在ECS实例页面的IP地址列不再显示EIP。

② 说明

- 解绑后的EIP仍会继续收费，如果不再使用请自行释放EIP。更多信息，请参见[释放按量计费EIP实例](#)。
- 解绑成功后，ECS实例无法再通过EIP访问公网。

3.4. 专有网络类型ECS公网IP转为弹性公网IP

转换为弹性公网IP（Elastic IP，简称EIP）后，EIP可以随时与ECS实例解绑或绑定。转换过程不会影响ECS实例的公网接入，也不会造成网络闪断。

前提条件

专有网络VPC公网IP转换为EIP前，请确保ECS实例已满足以下要求：

- 分配了公网IP地址。
- 计费方式为按量付费时，您的账号不能处于欠费状态。
- 计费方式为包年包月时，到期前24小时内不支持此操作。
- 计费方式为包年包月时，公网带宽计费方式必须是按使用流量计费。按固定带宽计费的公网带宽可以先通过升降配变更计费方式，详情请参见[升降配方式概述](#)。
- 已操作过实例规格变更时，请等待变更生效后再转换公网IP地址。
- ECS实例处于运行中或者已停止状态。

背景信息

专有网络VPC公网IP转换为EIP后：

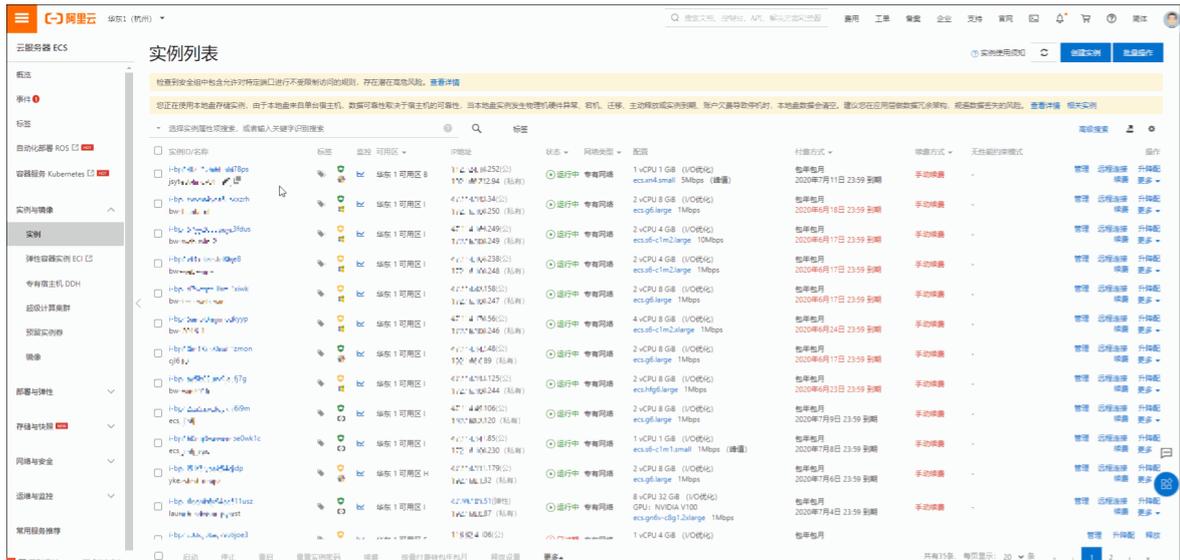
- 公网带宽计费方式不变。
- 转换后EIP将单独计费，单独产生账单。关于EIP计费，请参见[EIP定价](#)。您可以在[用户中心](#)单击费用账单，然后在费用账单页面单击账单明细页签，通过实例名称或实例ID过滤，查看和导出指定弹性公网IP的消费记录。

本文描述如何在ECS管理控制台转换专有网络VPC公网IP为EIP，您也可以调用API ConvertNatPublicIpToEip完成操作。使用API时，请确保您使用的是4.3.0及以上版本的SDK，请下载最新版的SDK。详情请参见[SDK概述](#)。

操作步骤

1. 登录[ECS管理控制台](#)。
2. 在左侧导航栏，选择实例与镜像 > 实例。
3. 在顶部菜单栏左上角处，选择地域。
4. 找到网络类型为专有网络，而且需要转换IP地址的ECS实例，在操作列，单击更多 > 网络和安全组 > 公网IP转换为弹性公网IP。
5. 在弹出的对话框中，确认信息后，单击确定。
6. 刷新实例列表。

以下示例演示了如何将专有网络VPC公网IP转换为EIP。



执行结果

专有网络VPC公网IP转换为EIP后，原公网IP地址会被标注为弹性。

您可以单击这个IP地址前往[IP管理控制台](#)查看并操作弹性公网IP。

后续步骤

专有网络VPC公网IP转换为EIP后，您可以执行以下操作：

- 解绑EIP并绑定其他实例，也可以释放EIP。详情请参见[解绑EIP](#)。
- 在共享带宽包中添加EIP，节省成本。详情请参见[加入共享带宽](#)、[如何选择公网类产品](#)和[如何节约公网成本](#)。

相关文档

- [Convert NatPublicIp To Eip](#)

3.5. 经典网络类型ECS公网IP转为弹性公网IP

手动释放经典网络类型ECS实例时，您可以将公网IP转换为弹性公网IP（Elastic IP，简称EIP）。EIP可绑定到专有网络VPC类型的ECS实例上，适用于网络迁移、弹性绑定、灵活升降带宽等场景。只有在手动释放实例时，才能转换经典网络公网IP为EIP，自动释放实例时，不支持转换。

前提条件

经典网络公网IP转换为EIP前，请确保ECS实例满足以下要求：

- 已分配了公网IP地址。

- 计费方式为按量付费时，实例必须处于已停止状态，且账号不能处于欠费状态。
- 计费方式为包年包月时，实例必须处于已过期或过期回收中状态。

说明 如果您需要在转换公网IP后释放经典网络类型的包年包月ECS实例，已过期或过期回收中的实例可以直接释放。如果您需要提前释放未到期的包年包月ECS实例，可以将实例的计费方式转换为按量计费，然后再手动释放。转换计费方式的具体操作，请参见[包年包月转按量付费](#)。您也可以退订包年包月ECS实例。更多信息，请参见[退款说明](#)。

- 计费方式为包年包月时，公网带宽计费方式必须是按使用流量计费。按固定带宽计费的公网带宽可以先通过升降配变更计费方式，详情请参见[升降配方式概述](#)。
- 实例在实例迁移计划中，不支持转换公网IP。更多信息，请参见[ECS实例从经典网络迁移到专有网络](#)。
- 操作过实例规格变更时，请等待变更生效后再转换公网IP地址。
- 已创建快照以备份数据，防止操作失误导致数据丢失。具体操作，请参见[创建快照](#)。

背景信息

经典网络公网IP转换为EIP后：

- 采用按使用流量计费方式。
- 公网带宽值和原ECS实例保持一致，您可以按需在专有网络管理控制台上升配EIP的公网带宽。但是，如果转换前经典网络类型ECS实例带宽为0 Mbit/s，转换后的EIP带宽自动升级为1 Mbit/s。
- 不能挂载到经典网络类型ECS实例上。
- 不同于专有网络VPC类型ECS实例，经典网络类型ECS实例具有公网网卡。如果您将经典网络公网IP转换为EIP，则无法保留该公网网卡和相应的Mac地址。

说明 华东1（杭州）地域可用区C中的部分ECS实例不支持保留公网IP，详情请[提交工单](#)咨询。

操作步骤

1. 登录[ECS管理控制台](#)。
2. 在左侧导航栏，选择实例与镜像 > 实例。
3. 在顶部菜单栏左上角处，选择地域。
4. 找到目标经典网络类型ECS实例，根据实例计费方式选择释放操作。
 - 释放一台包年包月实例：在操作列中，单击释放。
 - 释放一台按量付费实例：在操作列中，单击更多 > 实例状态 > 释放设置。
5. 选择立即释放，并勾选保留经典网络公网IP并将其转换为弹性公网IP（未绑定实例的弹性公网IP会产生配置费用），然后单击下一步。

释放设置 [实例释放须知](#) ✕

*释放行为： 立即释放 定时释放

[如何在实例释放时保留云盘](#)

相关资源处理： 保留经典网络公网IP并将其转换为弹性公网IP（未绑定实例的弹性公网IP会产生配置费用）

[下一步](#) [取消](#)

6. 单击确定。

执行结果

经典网络公网IP转换为EIP后，ECS实例会被释放，您可以在专有网络管理控制台查看新增的EIP。

实例ID/名称	IP地址	监控	带宽	线路类型	付费类型(全部) ▾	状态(全部) ▾	共享带宽/全球加速
<input type="checkbox"/> eip- v3f1e5	39.151		1 Mbps 按使用流量计费	BGP(多线)	后付费 2019-09-16 14:17:09 创建	● 可用	加入共享带宽 加入全球加速

后续步骤

经典网络公网IP转换为EIP后，您可以绑定EIP到ECS实例。具体操作，请参见[绑定EIP](#)。

4. 配置IPv6地址

4.1. Windows实例配置IPv6地址

4.1.1. Windows实例使用IPv6导航

本文介绍了如何为Windows系统的ECS实例使用和配置IPv6的大致流程，供您参考。

前提条件

ECS实例的网络类型必须是专有网络VPC。在分配IPv6地址前，请先了解IPv6。详情请参见[IPv6地址](#)。

使用导航

使用IPv6的流程图如下所示：



使用IPv6的步骤如下所示：

1. 搭建IPv6 VPC。详情请参见[步骤1：搭建IPv6 VPC](#)。
要在创建ECS实例时分配IPv6地址，您必须先搭建IPv6 VPC。
2. 为ECS实例分配IPv6地址。详情请参见[步骤2：分配IPv6地址](#)。
默认情况下，您在新建ECS实例时只分配私网IPv4地址，不分配IPv6地址。如需使用IPv6地址，您需要在控制台或者调用API为ECS实例分配IPv6地址。
3. 开通公网带宽。详情请参见[步骤3：开通IPv6公网带宽](#)。
创建ECS实例时配置的IPv6地址默认是专有网络VPC内网通信。如果您想通过IPv6地址访问公网或被公网访问，需要开通IPv6公网带宽。
4. 配置IPv6地址。详情请参见[步骤4：配置IPv6地址](#)。
为ECS实例分配IPv6地址后，您需要登录ECS实例并在操作系统内部进行IPv6地址相关的配置，才能正常使用IPv6地址。推荐您使用更高效的自动配置工具配置IPv6地址。
5. 添加安全组规则。详情请参见[步骤5：添加IPv6安全组规则](#)。
您可以通过添加安全组规则，允许或禁止安全组内的ECS实例对公网或私网的访问。常用案例请参见[安全组应用案例ECS安全组配置操作指南](#)。
6. 测试网络连通性。详情请参见[步骤6：测试网络连通性](#)。
您可以登录ECS实例测试网络的连通性，以保证配置的IPv6地址已具备公网访问能力。
7. （可选）删除IPv6地址。详情请参见[步骤7：（可选）删除IPv6地址](#)。
如果您的ECS实例不再需要IPv6地址，您可以删除IPv6地址。删除IPv6地址后，您仍然可以使用IPv4地址。

4.1.2. 步骤1：搭建IPv6 VPC

仅VPC类型的ECS实例支持IPv6地址。要在Windows实例上配置IPv6地址，必须先搭建IPv6 VPC。

背景信息

默认情况下，专有网络使用IPv4寻址协议。您可以根据需要开通IPv6寻址协议。关于IPv6地址的更多信息，请参见[IPv6地址](#)。

操作步骤

- 如果您还未创建VPC，您可以在创建VPC时开通IPv6。具体操作，请参见[新建IPv4和IPv6双栈VPC](#)。
- 如果您已经创建VPC，您可以为已有VPC开通IPv6。具体操作，请参见[为已有VPC开通IPv6网段](#)。

4.1.3. 步骤2：分配IPv6地址

您可以在新建Windows实例时分配IPv6地址，也可以为已有的Windows实例分配IPv6地址。

前提条件

- 为新建实例分配IPv6地址时，需确保实例所在的VPC和交换机已经开通IPv6网段。更多信息，请参见[VPC开启IPv6](#)和[交换机开启IPv6](#)。
- 为已有实例分配IPv6地址时：
 - 实例支持IPv6。关于实例规格是否支持IPv6属性的更多信息，请参见[实例规格族](#)。
 - 实例的网络类型为专有网络，且VPC和交换机已经开通IPv6网段。更多信息，请参见[VPC开启IPv6](#)和[交换机开启IPv6](#)。
 - 实例的状态为运行中或已停止。

为新建实例分配IPv6地址

创建实例的具体步骤，请参见[使用向导创建实例](#)。在选择配置时，您需要注意以下几点：

- 在[基础配置](#)页面，筛选出支持IPv6的实例规格，并选择一个实例规格。
- 在[网络和安全组](#)页面：
 - i. 选择已开通IPv6的专有网络和交换机。
 - ii. 勾选[免费分配IPv6地址](#)。
 - iii. 选择IPv6地址的分配方式。
 - [自动分配](#)：系统自动分配一个新的IPv6地址。
 - [指定地址](#)：需要您手动补全IPv6地址。
- 在[确认订单](#)页面，确认已分配的IPv6地址。

为已有实例分配IPv6地址

完成以下步骤，为已有实例分配IPv6地址。

1. 登录[ECS管理控制台](#)。
2. 在左侧导航栏，选择[实例与镜像](#) > [实例](#)。
3. 在顶部菜单栏左上角处，选择地域。
4. 选择已创建的ECS实例，单击操作列下的[更多](#)。
5. 选择[网络和安全组](#) > [管理辅助私网IP](#)。
6. 在[管理辅助私网IP](#)对话框中，单击IPv6地址右侧的[分配新IP](#)。
7. 选择IPv6地址的分配方式。
 - [自动分配](#)：系统自动分配一个新的IPv6地址。
 - [指定地址](#)：需要您手动补全IPv6地址。
8. 单击确定。

相关文档

- [AssignIpv6Addresses](#)

4.1.4. 步骤3：开通IPv6公网带宽

如果您想使用IPv6地址进行公网通信，您需要开通IPv6公网带宽。

背景信息

创建实例时配置的IPv6地址默认是VPC内网通信。

操作步骤

1. 登录[专有网络管理控制台](#)。
2. 在左侧导航栏，选择公网访问 > IPv6网关。
3. 在顶部菜单栏处，选择IPv6网关的地域。
4. 在IPv6网关页面，找到目标IPv6网关，然后在操作列单击管理。
5. 在IPv6网关的详情页面，单击IPv6公网带宽页签，找到目标IPv6地址，然后在操作列单击开通公网带宽。



6. 在IPv6公网带宽（后付费）页面，根据以下信息配置公网带宽，然后单击立即购买并完成支付。

参数	描述
流量	选择公网带宽的计费类型。 公网带宽支持按固定带宽计费和按使用流量计费两种计费类型。更多信息，请参见 计费说明 。
带宽	根据需要调整公网带宽的带宽峰值。
计费周期	公网带宽的计费周期。有Day（按天）和Hour（按小时）两种计费周期。 当公网带宽选择按固定带宽计费时，计费周期为Day（按天），当公网带宽选择按使用流量计费时，计费周期为Hour（按小时）。

4.1.5. 步骤4：配置IPv6地址

本文介绍如何为Windows实例自动配置IPv6地址和手动配置IPv6地址，推荐您使用更高效的自动配置工具配置IPv6地址。

自动配置IPv6地址

ecs-util-ipv6能为已分配IPv6地址的ECS实例一键配置IPv6地址，或者为没有分配IPv6地址的ECS实例一键清理IPv6配置。

使用限制如下：

- ecs-util-ipv6工具仅适用于VPC类型实例，依赖实例元数据服务，使用前请勿将网络禁用或者将相关出口IP端口（100.100.100.200:80）禁用。更多信息，请参见[ECS实例元数据概述](#)。
- ecs-util-ipv6工具运行时会自动重启网卡、网络服务，短时间内网络可能会不可用，请慎重执行。

下载地址：

- [Windows Server 2003/2008/2012/2016 \(32位\)](#)
- [Windows Server 2003/2008/2012/2016 \(64位\)](#)

下载与系统版本相对应的脚本到目标系统，使用管理员权限执行：

```
ecs-utils-ipv6.exe
```

如果当前ECS已绑定IPv6地址，则会自动配置；否则会清除原有IPv6地址配置。

对于需要自动化配置IPv6实例的需求，例如大批量配置，建议您使用云助手或者实例自定义数据配合脚本的方式来调用。更多信息，请参见[云助手概述](#)和[ECS实例自定义数据概述](#)。以下为脚本示例（假设是64位，PowerShell脚本）。

```
#powershell
$install_dir="C:\Windows\system32"
$install_path = "$install_dir\ecs-utils-ipv6.exe"
if(-not (Test-Path -Path $install_path)){
    # download the tool
    $tool_url = 'http://ecs-image-utils.oss-cn-hangzhou.aliyuncs.com/ipv6/win/64/ecs-utils-ipv6.exe'
    Invoke-WebRequest -uri $tool_url -OutFile $install_path
    Unblock-File $install_path
}
# run the tool
Start-Process -FilePath "$install_path" -ArgumentList "--noenterkey" -NoNewWindow
```

手动配置IPv6地址

完成以下操作，手动配置IPv6地址：

1. 检查实例是否已开启IPv6服务。
 - i. 远程连接实例。具体操作，请参见[通过密码认证登录Windows实例](#)。
 - ii. 打开Windows命令处理程序CMD。
 - iii. 运行`ipconfig`。
 - 若返回IPv6地址相关内容，表示实例已成功开启IPv6服务。
 - 若实例还未开启IPv6服务，请根据下面步骤开启IPv6服务。
2. 开启IPv6服务。
 - o Windows Server 2008/2012/2016的操作步骤如下：
 - a. 远程连接实例。
 - b. 选择控制面板 > 网络和共享中心 > 网络连接。
 - c. 单击当前网络连接名，打开状态界面，再单击属性。
 - d. 检查IPv6协议这一行是否被选中。如果没有选中则需要先选中，然后单击确定。
 - o Windows Server 2003的操作步骤如下：
 - a. 远程连接实例。具体步骤，请参见[通过密码认证登录Windows实例](#)。
 - b. 选择控制面板 > 网络和共享中心 > 网络连接。
 - c. 单击当前网络连接名，打开状态界面，再单击属性。

- d. 根据IPv6协议是否存在，执行不同操作。
 - 如果存在IPv6协议，则选中**Internet 协议版本 6 (TCP/IPv6)**，再单击**确定**。
 - 如果不存在IPv6协议，您需要手动安装IPv6协议后选中**Internet 协议版本 6 (TCP/IPv6)**，再单击**确定**。以下为手动安装IPv6协议的操作步骤：
 - a. 在本地连接属性页面，单击**安装**，在网络组件类型页面单击**协议 > 添加**。
 - b. 在**选择网络协议**页面，选择**Microsoft TCP/IP 版本 6 > 确定**完成安装。
3. 查询实例的IPv6地址。

您可以通过控制台和实例元数据查看实例分配的IPv6地址。

 - 控制台：具体操作，请参见[步骤2：分配IPv6地址](#)。
 - 实例元数据：通过以下元数据项获取IPv6地址。更多信息，请参见[ECS实例元数据概述](#)。
 - IPv6地址：network/interfaces/macs/[mac]/ipv6s
 - IPv6网关：network/interfaces/macs/[mac]/ipv6-gateway
 - IPv6虚拟交换机CIDR地址段：network/interfaces/macs/[mac]/vswitch-ipv6-cidr-block
4. 手动配置IPv6地址。
 - Windows Server 2008/2012/2016的操作步骤如下：
 - a. 远程连接实例。具体步骤，请参见[通过密码认证登录Windows实例](#)。
 - b. 选择**控制面板 > 网络**。
 - c. 单击当前网络连接名，打开状态界面，再单击**属性**。
 - d. 选择**IPv6协议 > 属性**。
 - e. 选中**使用以下IPv6地址**，并填入IPv6地址、子网前缀长度和IPv6网关，单击**确定**。
 - f. （可选）绑定多个IPv6地址：在**Internet 协议版本 6 (TCP/IP)** 属性界面，单击**高级**打开高级设置界面，单击**添加**做批量处理。完成后单击**确定**。
 - Windows Server 2003的操作步骤如下：
 - a. 远程连接实例。具体步骤，请参见[通过密码认证登录Windows实例](#)。
 - b. 选择**控制面板 > 网络连接**，查看当前网络连接名，假设为本地连接 2。
 - c. 打开Windows命令处理程序CMD。
 - d. 添加IPv6地址。
 - 单个IPv6地址运行以下命令：

```
netsh interface ipv6 add address "本地连接 2" <IPv6 地址>
```
 - 多个IPv6地址运行以下命令：

```
netsh interface ipv6 add address "本地连接 2" <IPv6 地址 1>
netsh interface ipv6 add address "本地连接 2" <IPv6 地址 2>
```
 - e. 运行以下命令添加默认路由：

```
netsh interface ipv6 add route ::/0 "本地连接 2" <IPv6 网关>
```

4.1.6. 步骤5：添加IPv6安全组规则

IPv4和IPv6通信彼此独立，如果当前的安全组规则不能满足业务需求，您需要为ECS实例单独配置IPv6安全组规则。

操作步骤

1. 登录[ECS管理控制台](#)。

2. 在左侧导航栏，选择网络与安全 > 安全组。
3. 在顶部菜单栏左上角处，选择地域。
4. 找到目标安全组，然后单击配置规则。
5. 单击手动添加。
6. 配置安全组规则。

其中，授权对象中输入授权的IPv6地址段。例如输入::/0则代表授权所有IPv6地址。

关于安全组规则的配置操作和常见案例，请参见[添加安全组规则](#)和[安全组应用案例ECS安全组配置操作指南](#)。

4.1.7. 步骤6：测试网络连通性

您可以登录ECS实例测试网络的连通性，以保证配置的IPv6地址已具备公网访问能力。

背景信息

本示例中，将通过ping -6命令测试ECS实例与 `aliyun.com` 的连通性。

操作步骤

1. 远程连接已配置IPv6地址的ECS实例。
具体操作请参见[通过密码或密钥认证登录Windows实例](#)。
2. 打开命令行工具。
您可以通过以下任一方式打开命令行工具。
 - 在桌面单击开始图标，查找Windows PowerShell并打开。
 - 在桌面使用 *Win+ R*组合键打开运行对话框，并输入 `cmd` 打开命令行工具。
3. 运行以下命令验证网络连通性。

```
ping -6 aliyun.com
```

测试结果如下图所示。



```
PS C:\Users\Administrator> ping -6 aliyun.com
正在 Ping aliyun.com [2401:b180::6] 具有 32 字节的数据:
来自 2401:b180::6 的回复: 时间=29ms
来自 2401:b180::6 的回复: 时间=29ms
来自 2401:b180::6 的回复: 时间=29ms
来自 2401:b180::6 的回复: 时间=29ms

2401:b180:1:60::6 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 29ms, 最长 = 29ms, 平均 = 29ms
```

4.1.8. 步骤7：（可选）删除IPv6地址

如果您的Windows实例不需要IPv6地址，您可以删除实例的IPv6地址。删除IPv6地址后，您仍然可以使用IPv4地址。

前提条件

实例的状态为运行中或已停止。

操作步骤

1. 登录[ECS管理控制台](#)。
2. 在左侧导航栏，选择实例与镜像 > 实例。
3. 在顶部菜单栏左上角处，选择地域。

4. 在实例页面，选择已创建的ECS实例，单击更多 > 管理辅助私网IP。
5. 在管理辅助私网IP对话框中，单击IPv6地址信息右侧的取消分配。
6. 单击确定。

4.2. Linux实例配置IPv6地址

4.2.1. Linux实例使用IPv6导航

本文介绍了如何为Linux系统的ECS实例使用和配置IPv6的大致流程，供您参考。

前提条件

ECS实例的网络类型必须是专有网络VPC。在分配IPv6地址前，请先了解IPv6地址。详情请参见[IPv6地址](#)。

使用导航

使用IPv6的流程图如下所示：



使用IPv6的步骤如下所示：

1. 搭建IPv6 VPC。详情请参见[步骤1：搭建IPv6 VPC](#)。
要在创建ECS实例时分配IPv6地址，您必须先搭建IPv6 VPC。
2. 为ECS实例分配IPv6地址。详情请参见[步骤2：分配IPv6地址](#)。
默认情况下，您在新建ECS实例时只分配私网IPv4地址，不分配IPv6地址。如需使用IPv6地址，您需为ECS实例分配IPv6地址。
3. 开通公网带宽。详情请参见[步骤3：开通IPv6公网带宽](#)。
创建ECS实例时配置的IPv6地址默认是专有网络VPC内网通信。如果您想通过IPv6地址访问公网或被公网访问，需要开通IPv6公网带宽。
4. 配置IPv6地址。详情请参见[步骤4：配置IPv6地址](#)。
您可以为ECS实例自动配置IPv6地址或手动配置IPv6地址，推荐您使用更高效的自动配置工具配置IPv6地址。
5. 添加安全组规则。详情请参见[步骤5：添加IPv6安全组规则](#)。
您可以通过添加安全组规则，允许或禁止安全组内的ECS实例对公网或私网的访问。常用案例请参见[安全组应用案例ECS安全组配置操作指南](#)。
6. 测试网络连通性。详情请参见[步骤6：测试网络连通性](#)。
您可以登录ECS实例测试网络的连通性，以保证配置的IPv6地址已具备公网访问能力。
7. (可选) 删除IPv6地址。详情请参见[步骤7：\(可选\) 删除IPv6地址](#)。
如果您的ECS实例不再需要IPv6地址，您可以删除IPv6地址。删除IPv6地址后，您仍然可以使用IPv4地址。

4.2.2. 步骤1：搭建IPv6 VPC

仅VPC类型的ECS实例支持IPv6地址。要在Linux实例上配置IPv6地址，必须先搭建IPv6 VPC。

背景信息

默认情况下，专有网络使用IPv4寻址协议。您可以根据需要开通IPv6寻址协议。关于IPv6地址的更多信息，请参见[IPv6地址](#)。

操作步骤

- 如果您还未创建VPC，您可以在创建VPC时开通IPv6。具体操作，请参见[新建IPv4和IPv6双栈VPC](#)。
- 如果您已经创建VPC，您可以为已有VPC开通IPv6。具体操作，请参见[为已有VPC开通IPv6网段](#)。

4.2.3. 步骤2：分配IPv6地址

您可以在新建Linux实例时分配IPv6地址，也可以为已有的Linux实例分配IPv6地址。

前提条件

- 为新建实例分配IPv6地址时，需确保实例所在的VPC和交换机已经开通IPv6网段。更多信息，请参见[VPC开启IPv6](#)和[交换机开启IPv6](#)。
- 为已有实例分配IPv6地址时：
 - 实例支持IPv6。关于实例规格是否支持IPv6属性的更多信息，请参见[实例规格族](#)。
 - 实例的网络类型为专有网络，且VPC和交换机已经开通IPv6网段。更多信息，请参见[VPC开启IPv6](#)和[交换机开启IPv6](#)。
 - 实例的状态为运行中或已停止。

为新建实例分配IPv6地址

创建实例的具体步骤，请参见[使用向导创建实例](#)。在选择配置时，您需要注意以下几点：

- 在[基础配置](#)页面，筛选出支持IPv6的实例规格，并选择一个实例规格。
- 在[网络和安全组](#)页面：
 - i. 选择已开通IPv6的专有网络和交换机。
 - ii. 勾选[免费分配IPv6地址](#)。
 - iii. 选择IPv6地址的分配方式。
 - [自动分配](#)：系统自动分配一个新的IPv6地址。
 - [指定地址](#)：需要您手动补全IPv6地址。
- 在[确认订单](#)页面，确认已分配的IPv6地址。

为已有实例分配IPv6地址

完成以下步骤，为已有实例分配IPv6地址。

1. 登录[ECS管理控制台](#)。
2. 在左侧导航栏，选择[实例与镜像](#) > [实例](#)。
3. 在顶部菜单栏左上角处，选择地域。
4. 选择已创建的ECS实例，单击操作列下的[更多](#)。
5. 选择[网络和安全组](#) > [管理辅助私网IP](#)。
6. 在[管理辅助私网IP](#)对话框中，单击IPv6地址右侧的[分配新IP](#)。
7. 选择IPv6地址的分配方式。
 - [自动分配](#)：系统自动分配一个新的IPv6地址。
 - [指定地址](#)：需要您手动补全IPv6地址。
8. 单击确定。

相关文档

- [AssignIpv6Addresses](#)

4.2.4. 步骤3：开通IPv6公网带宽

如果您想使用IPv6地址进行公网通信，您需要开通IPv6公网带宽。

背景信息

创建实例时配置的IPv6地址默认是VPC内网通信。

操作步骤

1. 登录[专有网络管理控制台](#)。
2. 在左侧导航栏，选择公网访问 > IPv6网关。
3. 在顶部菜单栏处，选择IPv6网关的地域。
4. 在IPv6网关页面，找到目标IPv6网关，然后在操作列单击管理。
5. 在IPv6网关的详情页面，单击IPv6公网带宽页签，找到目标IPv6地址，然后在操作列单击开通公网带宽。

IPv6地址ID/名称	IPv6地址	监控	网络类型(全部)	公网付费类型	状态	关联实例ID/名称	实例类型	操作
ipv6-bp105...	2408:...		私网	-	✓ 可用	i-bp-...	ECS	开通公网带宽 删除公网带宽 分配带宽

6. 在IPv6公网带宽（后付费）页面，根据以下信息配置公网带宽，然后单击立即购买并完成支付。

参数	描述
流量	选择公网带宽的计费类型。 公网带宽支持按固定带宽计费和按使用流量计费两种计费类型。更多信息，请参见 计费说明 。
带宽	根据需要调整公网带宽的带宽峰值。
计费周期	公网带宽的计费周期。有Day（按天）和Hour（按小时）两种计费周期。 当公网带宽选择按固定带宽计时，计费周期为Day（按天），当公网带宽选择按使用流量计费时，计费周期为Hour（按小时）。

4.2.5. 步骤4：配置IPv6地址

本文介绍了如何为Linux实例自动配置IPv6地址和手动配置IPv6地址，推荐您使用更高效的自动配置工具配置IPv6地址。

自动配置IPv6地址

ecs-util-ipv6能为已分配IPv6地址的ECS实例一键配置IPv6地址，或者为没有分配IPv6地址的ECS实例一键清理IPv6配置。

ecs-util-ipv6工具下载地址如下所示：

系列	发行版	下载地址

系列	发行版	下载地址
RHEL	<ul style="list-style-type: none"> CentOS 5/6/7/8 Red Hat 5/6/7 Anolis OS Fedora Alibaba Cloud Linux 2/3 	下载地址
Debian	<ul style="list-style-type: none"> Ubuntu 14/16/18/20 Debian/8/9/10/11 	下载地址
SLES	<ul style="list-style-type: none"> SUSE 11/12/15 OpenSUSE 15/42 	下载地址
FreeBSD	FreeBSD 11	下载地址

使用限制如下：

- ecs-util-ipv6工具仅适用于VPC类型实例，依赖实例元数据服务，使用前请勿将网络禁用或者将相关出口IP端口（100.100.100.200:80）禁用。详情请参见[实例元数据](#)。
- ecs-util-ipv6工具运行时会自动重启网卡、网络服务，短时间内网络可能会不可用，请慎重执行。

下载对应系统版本工具到目标系统，赋予执行权限后使用管理员权限执行：

```
chmod +x ./ecs-utils-ipv6
./ecs-utils-ipv6
```

 **注意** 如果镜像版本是Ubuntu 14版本的公共镜像，执行完该命令后，需重启ECS实例才能生效。具体操作，请参见[重启实例](#)。

如果当前ECS已绑定IPv6地址，则会自动配置；否则会清理原有IPv6地址配置。

命令行参数：

```
ecs-utils-ipv6 --help          # show usage
ecs-utils-ipv6 --version      # show version
ecs-utils-ipv6                # auto config all dev ipv6
ecs-utils-ipv6 --static [dev] [ip6s][prefix_len] [gw6] # config dev static ipv6
e.g. ecs-utils-ipv6 --static eth0
     ecs-utils-ipv6 --static eth0 xxx::x1 64 xxx::x0
     ecs-utils-ipv6 --static eth0 "xxx::x1 xxx:x2 xxx:x3" 64 xxx::x0
ecs-utils-ipv6 --enable       # enable ipv6
ecs-utils-ipv6 --disable     # disable ipv6
```

可以开启、禁用、手动配置、自动配置（默认）IPv6。

```
./ecs-utils-ipv6                #默认可不带参数，自动配置多网卡多IPv6
./ecs-utils-ipv6 --enable       #开启IPv6
./ecs-utils-ipv6 --disable     #禁用IPv6
./ecs-utils-ipv6 --static <dev> #自动配置网卡IPv6
./ecs-utils-ipv6 --static <dev> <ip6s> <prefix_len> <gw6> #手动配置网卡IPv6，支持多IPv6，请用""包含，多个IPv6用空格隔开
```

对于需要自动化配置IPv6实例的需求，例如大批量配置，建议您使用云助手或者实例自定义数据配合脚本的方式来调用。详情请参见[云助手](#)和[实例自定义数据](#)。以下为脚本示例（假设是RHEL系列，Bash Shell脚本）。

```
#!/bin/sh
install_dir=/usr/sbin
install_path="$install_dir"/ecs-utils-ipv6
if [ ! -f "$install_path" ]; then
    tool_url="http://ecs-image-utils.oss-cn-hangzhou.aliyuncs.com/ipv6/rhel/ecs-utils-ipv6"
    # download the tool
    if ! wget "$tool_url" -O "$install_path"; then
        echo "[Error] download tool failed, code $?"
        exit "$?"
    fi
fi
# chmod the tool
if ! chmod +x "$install_path"; then
    echo "[Error] chmod tool failed, code $?"
    exit "$?"
fi
# run the tool
"$install_path"
```

手动配置IPv6地址（Alibaba Cloud Linux 2/3操作系统）

Alibaba Cloud Linux操作系统请完成以下操作，手动配置IPv6地址：

1. 远程连接实例。具体操作，请参见[通过密码认证登录Linux实例](#)。
2. 检查实例是否已开启IPv6服务。

 **说明** Alibaba Cloud Linux 2镜像在 `aliyun_2_1903_64_20G_alibase_20190829.vhd` 及之前的版本未开启IPv6，从 `aliyun_2_1903_x64_20G_alibase_20200221.vhd` 版本开始默认开启IPv6服务。

运行 `ip addr | grep inet6` 或者 `ifconfig | grep inet6` 命令：

- 如果返回 `inet6` 相关内容，表示实例已成功开启IPv6服务。您可以跳过下文开启IPv6服务的步骤，直接配置IPv6地址。
 - 如果未返回 `inet6` 相关内容，表示实例未开启IPv6服务，请根据下文开启IPv6服务。
3. 开启IPv6服务。

开启IPv6支持配置为暂时或持久。暂时配置将在实例停止或重启时失效，持久配置将不受实例的状态影响。您可以根据实际情况选择配置方式。

- 暂时开启IPv6。
 - a. 运行以下命令进入`/etc/systemd/network/`目录。

```
cd /etc/systemd/network/
```

- b. 使用命令 `ls` 查询该目录下的 `.network` 文件。

例如，`50-dhcp.network` 文件。

- c. 修改文件`50-dhcp.network`内容。

```
vi /etc/systemd/network/50-dhcp.network
```

d. 按键进入编辑模式。

将 [Network] 下的信息修改为 DHCP=yes 。

说明 文件内参数 Name=eth* 表示适配所有网络接口，所有网络接口都将通过DHCP配置IP地址与路由。如果只需要配置指定的网络接口，可以修改参数 Name 为指定的网络接口，例如， Name=eth0 表示只适配 eth0 网络接口。更多关于 network 的信息请参见 [systemd.network](#)。

```
[Match]
Name=eth*
[Network]
DHCP=yes
```

修改完成后按 `Esc` 键，并输入 `:wq` 后按下回车键，保存并退出。

e. 运行以下命令开启IPv6。

■ 开启所有网络接口。

```
sudo sysctl -w net.ipv6.conf.all.disable_ipv6=0
sudo sysctl -w net.ipv6.conf.default.disable_ipv6=0
```

■ 开启指定网络接口示例。

```
sudo sysctl -w net.ipv6.conf.eth0.disable_ipv6=0
```

■ 重启systemd-networkd服务使配置生效。

```
sudo systemctl restart systemd-networkd
```

o 持久开启IPv6。

a. 修改 /etc/sysctl.conf 配置文件。

```
vi /etc/sysctl.conf
```

b. 按进入编辑模式。使用以下任一方式修改文件内容。

■ 删除下列配置信息。

```
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
net.ipv6.conf.lo.disable_ipv6 = 1
```

■ 修改对应的配置信息为如下内容。

```
net.ipv6.conf.all.disable_ipv6 = 0
net.ipv6.conf.default.disable_ipv6 = 0
net.ipv6.conf.lo.disable_ipv6 = 0
```

如果需要开启指定网络接口，修改信息示例如下。

```
net.ipv6.conf.eth0.disable_ipv6 = 0
```

修改完成后按 `Esc` 键，并输入 `:wq` 后按下回车键，保存并退出。

- c. 验证 `/etc/sysctl.conf` 配置信息是否与 `initramfs` 中的 `/etc/sysctl.conf` 存在差异。

```
diff -u /etc/sysctl.conf <(lsinitrd -f /etc/sysctl.conf)
```

说明 Alibaba Cloud Linux 2配置了 `initramfs` (init ram file system)。如果 `initramfs` 中的 `/etc/sysctl.conf` 文件与IPv6的配置文件 `/etc/sysctl.conf` 存在差异，系统可能会生效新的配置，与您需求的配置混淆。

- d. 如果两个配置文件存在差异，您可以执行以下命令重新生成 `initramfs`。

```
sudo dracut -v -f
```

- e. 重启实例。

```
reboot
```

- f. 执行 `ifconfig` 命令判断是否已开启IPv6。

如果网络配置信息包含以下信息，表示IPv6已开启。

```
inet6 <以fe80::开头的单播地址>
inet6 <ECS实例的IPv6地址>
```

4. 手动配置IPv6地址。

- i. 运行 `vi /etc/sysconfig/network-scripts/ifcfg-eth0` 打开网卡配置文件，`eth0`为网卡标识符，您需要修改成实际的标识符。在文件中根据实际信息添加以下配置：

```
DHCPV6C=yes
IPV6INIT=yes
```

修改完成后，保存并退出。

- ii. 重启实例。

```
reboot
```

手动配置IPv6地址（其他操作系统）

CentOS、Debian、Ubuntu、Fedora等操作系统请完成以下操作，手动配置IPv6地址：

1. 远程连接实例。具体操作，请参见[通过密码认证登录Linux实例](#)。
2. 检查实例是否已开启IPv6服务。

说明 CentOS 8、Debian 10及以上版本、Ubuntu 18及以上版本等操作系统已默认开启IPv6服务。

运行 `ip addr | grep inet6` 或者 `ifconfig | grep inet6` 命令：

- 如果返回 `inet6` 相关内容，表示实例已成功开启IPv6服务。您可以跳过下文开启IPv6服务的步骤，直接配置IPv6地址。
- 如果未返回 `inet6` 相关内容，表示实例未开启IPv6服务，请根据下文开启IPv6服务。

3. 开启IPv6服务。

操作系统	操作步骤
------	------

操作系统	操作步骤
CentOS 6	<p>i. 运行 <code>vi /etc/modprobe.d/disable_ipv6.conf</code>，将 <code>options ipv6 disable=1</code> 修改为 <code>options ipv6 disable=0</code> 后保存退出。</p> <p>ii. 运行 <code>vi /etc/sysconfig/network</code>，将 <code>NETWORKING_IPV6=no</code> 修改为 <code>NETWORKING_IPV6=yes</code> 后保存退出。</p> <p>iii. 运行以下命令：</p> <pre>modprobe ipv6 -r modprobe ipv6</pre> <p>iv. 运行 <code>lsmod grep ipv6</code>，当返回以下内容时，表明IPv6模块已经成功加载：</p> <pre>ipv6 xxxxxx 8</pre> <p>说明 第三列参数值不能为 0，否则您需要重新设置IPv6服务。</p> <p>v. 运行 <code>vi /etc/sysctl.conf</code> 做如下修改：</p> <pre>#net.ipv6.conf.all.disable_ipv6 = 1 #net.ipv6.conf.default.disable_ipv6 = 1 #net.ipv6.conf.lo.disable_ipv6 = 1 net.ipv6.conf.all.disable_ipv6 = 0 net.ipv6.conf.default.disable_ipv6 = 0 net.ipv6.conf.lo.disable_ipv6 = 0</pre> <p>修改完成后，保存并退出。</p> <p>vi. 运行 <code>sysctl -p</code> 使配置生效。</p>
CentOS 7	<p>i. 运行 <code>vi /etc/modprobe.d/disable_ipv6.conf</code>，将 <code>options ipv6 disable=1</code> 修改为 <code>options ipv6 disable=0</code> 后保存退出。</p> <p>ii. 运行 <code>vi /etc/sysconfig/network</code>，将 <code>NETWORKING_IPV6=no</code> 修改为 <code>NETWORKING_IPV6=yes</code> 后保存退出。</p> <p>iii. 运行 <code>vi /etc/sysctl.conf</code> 做如下修改：</p> <pre>#net.ipv6.conf.all.disable_ipv6 = 1 #net.ipv6.conf.default.disable_ipv6 = 1 #net.ipv6.conf.lo.disable_ipv6 = 1 net.ipv6.conf.all.disable_ipv6 = 0 net.ipv6.conf.default.disable_ipv6 = 0 net.ipv6.conf.lo.disable_ipv6 = 0</pre> <p>修改完成后，保存并退出。</p> <p>iv. 运行 <code>sysctl -p</code> 使配置生效。</p>

操作系统	操作步骤
Debian 8/9	<p>i. 运行 <code>vi /etc/default/grub</code> , 删除 <code>ipv6.disable=1</code> 后保存退出。</p> <p>ii. 运行 <code>vi /boot/grub/grub.cfg</code> , 删除 <code>ipv6.disable=1</code> 后保存退出。</p> <p>iii. 重启实例。</p> <p>iv. 运行 <code>vi /etc/sysctl.conf</code> 做如下修改:</p> <pre data-bbox="598 481 1385 689"> #net.ipv6.conf.all.disable_ipv6 = 1 #net.ipv6.conf.default.disable_ipv6 = 1 #net.ipv6.conf.lo.disable_ipv6 = 1 net.ipv6.conf.all.disable_ipv6 = 0 net.ipv6.conf.default.disable_ipv6 = 0 net.ipv6.conf.lo.disable_ipv6 = 0 </pre> <p>修改完成后, 保存并退出。</p> <p>v. 运行 <code>sysctl -p</code> 使配置生效。</p>
<ul style="list-style-type: none"> o Ubuntu 14/16 o OpenSUSE 42 <div data-bbox="284 1032 509 1232" style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> 说明 OpenSUSE 42开启服务后, 无需再手动配置, 即可获取IPv6地址。</p> </div>	<p>i. 运行 <code>vi /etc/sysctl.conf</code> 做如下修改:</p> <pre data-bbox="598 965 1385 1173"> #net.ipv6.conf.all.disable_ipv6 = 1 #net.ipv6.conf.default.disable_ipv6 = 1 #net.ipv6.conf.lo.disable_ipv6 = 1 net.ipv6.conf.all.disable_ipv6 = 0 net.ipv6.conf.default.disable_ipv6 = 0 net.ipv6.conf.lo.disable_ipv6 = 0 </pre> <p>修改完成后, 保存并退出。</p> <p>ii. 运行 <code>sysctl -p</code> 使配置生效。</p>
FreeBSD 11	<p>i. 运行 <code>vi /etc/rc.conf</code> , 添加 <code>ipv6_activate_all_interfaces="YES"</code> 后保存退出。</p> <p>ii. 运行 <code>/etc/netstart restart</code> 重启网络。</p>

操作系统	操作步骤
SUSE 11/12 <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>? 说明 SUSE 11/12开启服务后, 无需再手动配置, 即可获取IPv6地址。</p> </div>	<p>i. 运行 <code>vi /etc/modprobe.d/50-ipv6.conf</code>, 删除 <code>install ipv6 /bin/true</code> 后保存退出。</p> <p>ii. 运行 <code>vi /etc/sysctl.conf</code> 做如下修改:</p> <pre style="background-color: #f0f0f0; padding: 10px;">#net.ipv6.conf.all.disable_ipv6 = 1 #net.ipv6.conf.default.disable_ipv6 = 1 #net.ipv6.conf.lo.disable_ipv6 = 1 net.ipv6.conf.all.disable_ipv6 = 0 net.ipv6.conf.default.disable_ipv6 = 0 net.ipv6.conf.lo.disable_ipv6 = 0</pre> <p>修改完成后, 保存并退出。</p> <p>iii. 运行 <code>sysctl -p</code> 使配置生效。</p>

4. 查看实例分配的IPv6地址。

您可以通过控制台和实例元数据两种方式查看实例分配的IPv6地址。

- 控制台: 更多信息, 请参见[分配 IPv6 地址](#)。
- 实例元数据: 通过以下元数据项获取IPv6地址。更多信息, 请参见[实例元数据](#)。
 - IPv6 地址: `network/interfaces/macs/[mac]/ipv6s`
 - IPv6 网关: `network/interfaces/macs/[mac]/ipv6-gateway`
 - IPv6 虚拟交换机 CIDR 地址段: `network/interfaces/macs/[mac]/vswitch-ipv6-cidr-block`

5. 手动配置IPv6地址。

操作系统	操作步骤
<ul style="list-style-type: none"> ○ CentOS 6/7 ○ Red Hat 6/7 ○ Almalinux ○ Rocky Linux 	<p>以<code>centos_6_10_x64_20G_alibase_20201120.vhd</code>、<code>centos_7_9_x64_20G_alibase_20211227.vhd</code>为例:</p> <p>i. 运行 <code>vi /etc/sysconfig/network-scripts/ifcfg-eth0</code> 打开网卡配置文件, <code>eth0</code> 为网卡标识符, 您需要修改成实际的标识符。在文件中根据实际信息添加以下信息:</p> <pre style="background-color: #f0f0f0; padding: 10px;">DHCPV6C=yes IPV6INIT=yes</pre> <p>修改完成后, 保存并退出。</p> <p>ii. 运行 <code>reboot</code> 重启实例。</p>

操作系统	操作步骤
CentOS 8	<p>以centos_8_5_x64_20G_alibase_20211228.vhd为例：</p> <ol style="list-style-type: none"> i. 确认网卡配置文件是否包含 <code>IPV6INIT=yes</code> 和 <code>DHCPV6C=yes</code> 两项内容。如果包含直接进行下一步操作，如果未包含需先手动添加。 <pre>vi /etc/sysconfig/network-scripts/ifcfg-eth0</pre> <p><code>eth0</code> 为网卡标识符，您需要修改成实际的标识符。修改完成后，保存并退出。</p> ii. 禁用cloud-init修改 <code>/etc/sysconfig/network-scripts/</code> 目录下网卡文件的能力。 <div style="border: 1px solid #add8e6; padding: 5px; margin: 10px 0;"> <p>? 说明 分配IPv6地址后无需手动配置，但重启之后可能丢失，因此需要用cloud-init修改网卡文件的能力。</p> </div> <ol style="list-style-type: none"> a. 运行 <code>vi /etc/cloud/cloud.cfg</code> 打开网卡配置文件。 <pre>vi /etc/cloud/cloud.cfg</pre> b. 在 <code>Example datasource config</code> 内容前添加以下信息： <pre>network: config: disabled</pre> <p>修改完成后，保存并退出。</p> iii. 运行 <code>reboot</code> 重启实例。
Ubuntu 14	<p>以ubuntu_14_0405_64_20G_alibase_20170824.vhd为例：</p> <ol style="list-style-type: none"> i. 运行 <code>vi /etc/sysctl.conf</code> 打开网卡配置文件。在文件中修改以下信息： <pre>#net.ipv6.conf.all.disable_ipv6 = 1 #net.ipv6.conf.default.disable_ipv6 = 1 #net.ipv6.conf.lo.disable_ipv6 = 1 net.ipv6.conf.all.disable_ipv6 = 0 net.ipv6.conf.default.disable_ipv6 = 0 net.ipv6.conf.lo.disable_ipv6 = 0</pre> <p>修改完成后，保存并退出。</p> ii. 运行 <code>vi /etc/network/interfaces</code> 打开网卡配置文件，在文件中根据实际信息添加以下信息： <pre>iface eth0 inet6 dhcp</pre> <p><code>eth0</code> 为网卡标识符，您需要修改成实际的标识符。修改完成后，保存并退出。</p> iii. 运行 <code>reboot</code> 重启实例。

操作系统	操作步骤
<ul style="list-style-type: none"> ◦ Ubuntu 16 ◦ Debian 8/9/10/11 	<p>以debian_9_13_x64_20G_alibase_20211227.vhd、debian_10_11_x64_20G_alibase_20211227.vhd、debian_11_2_x64_20G_alibase_20211227.vhd、ubuntu_16_04_x64_20G_alibase_20211028.vhd为例：</p> <p>i. 运行 <code>vi /etc/network/interfaces</code> 打开网卡配置文件，在文件中根据实际信息添加以下信息：</p> <pre>iface eth0 inet6 dhcp</pre> <p><code>eth0</code> 为网卡标识符，您需要修改成实际的标识符。修改完成后，保存并退出。</p> <p>ii. 运行 <code>reboot</code> 重启实例。</p>
Ubuntu 18/20	<p>以ubuntu_18_04_x64_20G_alibase_20211227.vhd、ubuntu_20_04_x64_20G_alibase_20211227.vhd为例：</p> <p>i. 禁用cloud-init修改 <code>/etc/sysconfig/network-scripts/</code> 目录下网卡文件的能力。</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <p>? 说明 分配IPv6地址后无需手动配置，但重启之后可能丢失，因此需要禁用cloud-init修改网卡文件的能力。</p> </div> <p>a. 运行 <code>vi /etc/cloud/cloud.cfg</code> 打开网卡配置文件。</p> <pre>vi /etc/cloud/cloud.cfg</pre> <p>b. 在 <code>Example datasource config</code> 内容前添加以下信息：</p> <pre>network: config: disabled</pre> <p>修改完成后，保存并退出。</p> <p>ii. 运行 <code>reboot</code> 重启实例。</p>
<ul style="list-style-type: none"> ◦ Anolis OS 7.9/8.4 ◦ CentOS Stream ◦ Fedora 	<p>以anolisos_7_9_x64_20G_rhck_alibase_20220110.vhd、anolisos_8_4_x64_20G_rhck_alibase_20211008.vhd、centos_stream_8_x64_20G_alibase_20211227.vhd、fedora_34_1_x64_20G_alibase_20211028.vhd为例：</p> <p>i. 确认网卡配置文件是否包含 <code>IPV6INIT=yes</code> 和 <code>DHCPV6C=yes</code> 两项内容。如果包含无需再做任何操作，如果未包含需先手动添加。</p> <pre>vi /etc/sysconfig/network-scripts/ifcfg-eth0</pre> <p><code>eth0</code> 为网卡标识符，您需要修改成实际的标识符。修改完成后，保存并退出。</p> <p>ii. 运行 <code>reboot</code> 重启实例。</p>

操作系统	操作步骤
FreeBSD 11	<p>以freebsd_11_4_x64_30G_alibase_20210319.vhd为例：</p> <p>i. 运行 <code>vi /etc/rc.conf</code> 打开网卡配置文件，在文件中根据实际信息添加以下信息：</p> <pre> ipv6_enable="YES" ipv6_ifconfig_vtnet0="<IPv6地址> <子网前缀长度>" </pre> <p>ii. 继续在文件中修改以下信息，修改完成后，保存并退出。</p> <pre> ip6addrctl_enable="YES" ipv6_activate_all_interfaces="YES" ipv6_network_interfaces="auto" </pre> <p>修改完成后，配置文件内容示例如下：</p> <pre> hostname="Aliyun" sshd_enable="YES" dumpdev="NO" ipv6_enable="YES" ip6addrctl_enable="YES" ip6addrctl_policy="ipv4_prefer" ipv6_activate_all_interfaces="YES" ipv6_network_interfaces="auto" ifconfig_lo0="inet 127.0.0.1 netmask 255.0.0.0" ifconfig_vtnet0="inet 192.168.XX.XX netmask 255.255.255.0" ipv6_ifconfig_vtnet0="2001:XXXX:4:4:4:4:4:4 prefixlen 64" defaultrouter="192.168.XX.XX" hostname="freebsd" </pre> <p>iii. 运行 <code>reboot</code> 重启实例。</p>

4.2.6. 步骤5：添加IPv6安全组规则

IPv4和IPv6通信彼此独立，如果当前的安全组规则不能满足业务需求，您需要为ECS实例单独配置IPv6安全组规则。

操作步骤

1. 登录[ECS管理控制台](#)。
2. 在左侧导航栏，选择[网络与安全](#) > [安全组](#)。
3. 在顶部菜单栏左上角处，选择地域。
4. 找到目标安全组，然后单击配置规则。
5. 单击手动添加。
6. 配置安全组规则。

其中，授权对象中输入授权的IPv6地址段。例如输入::/0则代表授权所有IPv6地址。

关于安全组规则的配置操作和常见案例，请参见[添加安全组规则](#)和[安全组应用案例ECS安全组配置操作指南](#)。

4.2.7. 步骤6：测试网络连通性

您可以登录ECS实例测试网络的连通性，以保证配置的IPv6地址已具备公网访问能力。

背景信息

本示例中，将通过ping -6（或者ping6）命令测试ECS实例与 `aliyun.com` 的连通性。

操作步骤

1. 远程连接已配置IPv6地址的ECS实例。
具体操作请参见[通过密码或密钥认证登录Linux实例](#)。
2. 运行以下命令验证网络连通性。

```
ping -6 aliyun.com
```

测试结果如下图所示。

```
[root@test ~]# ping -6 aliyun.com
PING aliyun.com(2401:b180:1:50::f (2401:b180:1:50::f)) 56 data bytes
64 bytes from 2401:b180:1:50::f (2401:b180:1:50::f): icmp_seq=1 ttl=251 time=2.32 ms
64 bytes from 2401:b180:1:50::f (2401:b180:1:50::f): icmp_seq=2 ttl=251 time=2.28 ms
64 bytes from 2401:b180:1:50::f (2401:b180:1:50::f): icmp_seq=3 ttl=251 time=2.28 ms
64 bytes from 2401:b180:1:50::f (2401:b180:1:50::f): icmp_seq=4 ttl=251 time=2.34 ms
64 bytes from 2401:b180:1:50::f (2401:b180:1:50::f): icmp_seq=5 ttl=251 time=2.33 ms
64 bytes from 2401:b180:1:50::f (2401:b180:1:50::f): icmp_seq=6 ttl=251 time=2.31 ms
^C
--- aliyun.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5006ms
rtt min/avg/max/mdev = 2.284/2.315/2.344/0.035 ms
```

4.2.8. 步骤7：（可选）删除IPv6地址

如果您的Linux实例不需要IPv6地址，您可以删除实例的IPv6地址。删除IPv6地址后，您仍然可以使用IPv4地址。

前提条件

实例的状态为运行中或已停止。

操作步骤

1. 登录[ECS管理控制台](#)。
2. 在左侧导航栏，选择实例与镜像 > 实例。
3. 在顶部菜单栏左上角处，选择地域。
4. 在实例页面，选择已创建的ECS实例，单击更多 > 管理辅助私网IP。
5. 在管理辅助私网IP对话框中，单击IPv6地址信息右侧的取消分配。
6. 单击确定。

5. 查看IP地址

本文介绍如何查看实例相关的IP地址，包括固定公网IP地址、弹性公网IP地址、主私网IP地址、辅助私网IP地址和IPv6地址。

在实例页面查看IP地址

在实例页面可以查看实例的固定公网IP地址、弹性公网IP地址和主私网IP地址。

1. 登录[ECS管理控制台](#)。
2. 在左侧导航栏，选择实例与镜像 > 实例。
3. 在顶部菜单栏左上角处，选择地域。
4. 在实例页面，找到目标实例，在IP地址列查看IP地址。

显示示例如下：

- 固定公网IP地址：47.98.XX.XX（公）。
- 弹性公网IP地址：121.41.XX.XX（弹性）。
- 主私网IP地址：172.16.XX.XX（私有）。

在实例详情页面查看IP地址

在实例详情页面可以查看实例的固定公网IP地址、弹性公网IP地址、主私网IP地址、辅助私网IP地址和IPv6地址。

1. 登录[ECS管理控制台](#)。
2. 在左侧导航栏，选择实例与镜像 > 实例。
3. 在顶部菜单栏左上角处，选择地域。
4. 在实例页面，找到目标实例，在实例ID/名称列单击实例名称。
5. 在实例详情页面，查看IP地址。

显示示例如下：

- 基本信息区域：
 - 固定公网IP地址：公网IP 47.98.XX.XX。
 - 弹性公网IP地址：弹性公网IP 121.41.XX.XX。
- 网络信息区域：
 - 主私网IP地址：主私网IP 192.168.XX.XX。
 - IPv6地址：IPv6地址 2408:XXXX:325:a216:95f1:3dd9:6640:8b9e。
 - 辅助私网IP地址：辅助私网IP 192.168.XX.XX,192.168.XX.XX。

在弹性网卡页面查看IP地址

在弹性网卡页面可以查看实例的弹性公网IP地址、主私网IP地址、辅助私网IP地址。

1. 登录[ECS管理控制台](#)。
2. 在左侧导航栏，选择网络与安全 > 弹性网卡。
3. 在顶部菜单栏左上角处，选择地域。
4. 在弹性网卡页面，找到目标弹性网卡，查看IP地址。

显示示例如下：

- 公网IP地址列：显示弹性公网IP地址，如果没有弹性公网IP地址，则显示为空。
- 私网IP地址列：

- 主私网IP地址：192.168.XX.XX（主私网）。
- 辅助私网IP地址：192.168.XX.XX（辅助私网）。

 说明 多个辅助私网IP地址会分行显示。

6.弹性网卡

6.1.弹性网卡概述

弹性网卡ENI（Elastic Network Interface）是一种可以绑定到专有网络VPC类型ECS实例上的虚拟网卡。通过弹性网卡，您可以实现高可用集群搭建、低成本故障转移和精细化的网络管理。

网卡属性

弹性网卡是一种虚拟的网络接口，需绑定到专有网络VPC实例上使用。一块弹性网卡包含以下几部分属性：

属性	说明
网卡类型	分为主网卡和辅助网卡。 <ul style="list-style-type: none"> 主网卡：随实例一起创建，生命周期与实例保持一致，不支持从实例上解绑。 辅助网卡：可以单独创建，支持自由绑定到实例上或从实例上解绑。
专有网络VPC	仅专有网络VPC实例支持弹性网卡。弹性网卡与待绑定的实例必须属于同一专有网络VPC。
可用区	弹性网卡所属的交换机与绑定的实例必须属于同一可用区。
安全组	至少加入到一个安全组中，由安全组控制进出弹性网卡的流量。
弹性公网IP地址	可以绑定1个或多个弹性公网IP。
主私网IP地址	创建时系统分配或自定义的IPv4地址，为所属交换机的CIDR网段中的空闲IPv4地址。
辅助私网IPv4地址	所属交换机的CIDR网段中的空闲IPv4地址，支持分配和回收。
辅助私网IPv6地址	所属交换机的CIDR网段中的空闲IPv6地址，支持分配和回收。
MAC地址	全局唯一，是弹性网卡的唯一标识。

功能特点

弹性网卡是独立的虚拟网卡，可以在多个云服务器之间迁移，实现业务的灵活扩展和迁移。您可以随ECS实例创建并绑定弹性网卡，也可以单独创建辅助弹性网卡再绑定到ECS实例上。

弹性网卡具备以下功能特点：

- 除了随ECS实例一起创建的主网卡外，一台ECS实例支持绑定多个辅助网卡。这些辅助网卡和ECS实例必须属于同一专有网络VPC和同一可用区，可以分属于不同虚拟交换机和不同安全组。
- 每个弹性网卡根据绑定的实例规格不同，可以分配相应的多个辅助私网IP地址。
- 将一个辅助弹性网卡从一个实例解绑，再重新绑定到另一个实例时，网卡的属性不会发生变化，网络流量将直接切换到新的实例。
- 弹性网卡支持热插拔，可以在ECS实例之间自由迁移，切换弹性网卡绑定的实例时无需重启实例，不影响实例上运行的业务。

使用限制

限制项		
	主私网IP地址	1个

限制项		
每个弹性网卡各类属性数量	辅助私网IPv4地址	1个或多个，由实例规格确定。更多信息，请参见 实例规格族 。
	辅助私网IPv6地址	1个或多个，由实例规格决定。更多信息，请参见 实例规格族 。
	弹性公网IP地址	1个或多个，由绑定模式决定。更多信息，请参见 EIP绑定弹性网卡概述 。
	MAC地址	1个
	安全组	至少1个，最多5个。
一个账号在一个地域内可以创建的弹性网卡数量		

限制项
每台ECS实例允许绑定的辅助弹性网卡数量

限制项

VPC、可用区、交换机、安全组

限制项
网络类型
实例规格

典型应用场景

弹性网卡可以应用于以下几种场景：

- 搭建高可用集群

满足高可用架构对于单实例多网卡的需求。

- 低成本故障迁移

通过将弹性网卡从ECS实例解绑后再绑定到另外一台ECS实例，将故障实例上的业务流量快速转移到备用实例，实现服务快速恢复。

- 精细化网络管理

可以为实例配置多个弹性网卡，例如，用于内部管理的弹性网卡及用于公网业务访问的弹性网卡等，完成管理数据和业务数据间的隔离。也可以根据源IP地址、应用层协议、端口等对每张弹性网卡配置精准的安全组规则，从而对每张弹性网卡的流量进行安全访问控制。

- 单实例多私网IP地址

支持为ECS实例绑定的弹性网卡分配多个辅助私网IP地址。如果您的ECS实例托管多个应用，每个应用可以对外呈现一个独立的IP地址，提升实例的利用率

- 单实例多公网IP地址

在不使用弹性网卡的情况下，一台ECS实例只能分配一个公网IP地址。通过为弹性网卡绑定弹性公网IP地址，您可以实现单实例分配多公网IP地址。在普通绑定模式下，每个私网IP地址都可以绑定独立的弹性公网IP地址。

控制台操作

在ECS控制台上使用弹性网卡的相关操作如下表所示。

操作任务	说明	相关文档
创建弹性网卡	您可以在创建实例时附加弹性网卡，也可以单独创建弹性网卡。	创建弹性网卡
绑定弹性网卡	您可以在创建实例时绑定弹性网卡，也可以单独创建弹性网卡再绑定到实例上。一块弹性网卡一次只能绑定到一台ECS实例上，但一台ECS实例可以同时绑定多个弹性网卡。	绑定弹性网卡
配置弹性网卡	<p>针对部分不能自动识别辅助弹性网卡的镜像，您需要登录实例配置弹性网卡。</p> <div style="border: 1px solid #ccc; padding: 5px; background-color: #e6f2ff;"> <p> 说明 如果实例的镜像为CentOS 7.3 64位、CentOS 6.8 64位或Window Server 2008 R2及更高版本，无需配置弹性网卡。</p> </div>	配置辅助弹性网卡
分配或回收辅助私网IP地址	弹性网卡支持多个辅助私网IP，您可以自由分配或回收。	<ul style="list-style-type: none"> 分配辅助私网IP地址 回收辅助私网IP地址
修改弹性网卡	您可以修改主网卡所属安全组，还可以修改辅助弹性网卡名称、所属安全组和描述。	修改弹性网卡
解绑弹性网卡	如果某实例不再使用某一辅助弹性网卡，您可以进行解绑。	解绑弹性网卡
删除弹性网卡	如果您不再需要某一辅助弹性网卡，可以在解绑后进行删除。	删除弹性网卡

API操作

您可以调用以下API使用弹性网卡。

API	说明
CreateNetworkInterface	创建一个辅助弹性网卡。
DeleteNetworkInterface	删除一个辅助弹性网卡。
DescribeNetworkInterfaces	查询弹性网卡列表。
AttachNetworkInterface	将辅助弹性网卡绑定到实例上。
AssignPrivateIpAddresses	为一块弹性网卡分配一个或多个辅助私有IP地址。
UnassignPrivateIpAddresses	从一块弹性网卡删除一个或多个辅助私有IP地址。
DetachNetworkInterface	从实例上解绑辅助弹性网卡。
ModifyNetworkInterfaceAttribute	修改辅助弹性网卡名称、所属安全组和描述。
DescribeInstances	查询实例上附加的弹性网卡信息。

6.2. 托管弹性网卡

当您需要为部分云产品（例如容器服务ACK、NAT网关等）创建弹性网卡时，您可以将弹性网卡托管给云产品系统管理，该模式的弹性网卡称为托管弹性网卡。该模式可以防止您误操作资源并保障云产品的服务可用。本文主要介绍托管弹性网卡及其相关权限。

功能介绍

将弹性网卡托管给云产品系统管理，可以解决云产品对弹性网卡操作权限控制问题。托管后，通过云产品或者ECS控制台访问托管弹性网卡时，您只能查看托管弹性网卡的相关信息，不能操作托管弹性网卡。

 **说明** 创建托管弹性网卡过程如下：

您通过阿里云临时安全令牌STS（Security Token Service）为云产品授权后，云产品通过调用ECS的CreateNetworkInterface接口创建弹性网卡。关于STS的更多信息，请参见[什么是STS](#)。

您可以通过调用查询接口DescribeNetworkInterfaces，查看返回值参数ServiceManaged和Description，确认相关的弹性网卡是否为托管弹性网卡。

 **说明** 如果为托管弹性网卡，则ServiceManaged为true，Description显示云产品名称。

托管弹性网卡的OpenAPI权限说明

通过OpenAPI访问托管弹性网卡时，您仅能调用查询接口。如果您调用相关操作接口，将提示您该弹性网卡为云产品系统管理的弹性网卡，您无法操作，即返回InvalidOperation.EniServiceManaged的错误信息。关于各OpenAPI的具体权限如下表所示。

API	操作	您的阿里云账号	创建托管安全的云产品系统
DescribeNetworkInterfaces	查询弹性网卡	可以操作	可以操作
DeleteNetworkInterface	删除弹性网卡	不可操作	可以操作
ModifyNetworkInterfaceAttribute	修改弹性网卡的名称、描述及所属安全组等信息	不可操作	可以操作
AttachNetworkInterface	绑定弹性网卡	不可操作	可以操作
DetachNetworkInterface	解绑弹性网卡	不可操作	可以操作
AssignPrivateIpAddresses	为弹性网卡分配辅助私网IP地址	不可操作	可以操作
UnassignPrivateIpAddresses	回收弹性网卡的辅助私网IP地址	不可操作	可以操作
AssignIpv6Addresses	为弹性网卡分配IPv6地址	不可操作	可以操作
UnassignIpv6Addresses	回收弹性网卡的IPv6地址	不可操作	可以操作

6.3. 创建弹性网卡

弹性网卡可以为您实现高可用集群搭建、低成本故障转移和精细化的网络管理。本文为您介绍如何在控制台上单独创建弹性网卡。

前提条件

- 已在相应地域下创建专有网络VPC，并创建虚拟交换机。具体操作，请参见[创建和管理专有网络](#)和[创建和管理交换机](#)。
- 已在指定的专有网络下创建安全组。具体操作，请参见[创建安全组](#)。

背景信息

您可以通过以下两种方式创建弹性网卡，本文主要介绍如何单独创建弹性网卡。

- 随实例创建弹性网卡

在创建实例时，只能附加2块弹性网卡，一块为主网卡，一块为辅助网卡。通过该方式创建的辅助网卡，如果没有从实例上解绑，会随实例一起释放。具体操作，请参见[创建ECS实例时绑定弹性网卡](#)。

- 单独创建弹性网卡

单独创建的弹性网卡为辅助弹性网卡，可以绑定到实例上。

弹性网卡支持创建、绑定、解绑、删除弹性网卡的操作完成事件，您可以通过在云监控中设置弹性网卡事件通知以获取创建弹性网卡的操作结果。更多信息，请参见[弹性网卡事件通知](#)。

操作步骤

- 登录[ECS管理控制台](#)。
- 在左侧导航栏，选择[网络与安全 > 弹性网卡](#)。
- 在顶部菜单栏左上角处，选择地域。
- 单击[创建弹性网卡](#)。
- 在[创建弹性网卡](#)页面，完成相关设置。

参数	描述
弹性网卡名称	自定义，请按提示要求输入弹性网卡名称。
专有网络	<p>选择要绑定实例所对应的专有网络。弹性网卡创建后无法更改专有网络。</p> <p> 说明 弹性网卡只能绑定到同一个专有网络的实例上。</p>
交换机	<p>选择要绑定实例所在可用区下的交换机。弹性网卡创建后无法更改交换机。</p> <p> 说明</p> <ul style="list-style-type: none"> 弹性网卡和绑定的实例需要属于同一可用区，可以分属不同的交换机。 如果需要为网卡设置IPv6地址，需要选择支持配置IPv6地址的交换机。如果选择的交换机没有打开分配IPv6地址的功能，您可以单击开通交换机IPv6去开通。
安全组	<p>选择当前专有网络的安全组。至少选择1个，最多选择5个。</p> <p> 说明 不能同时选择普通安全组和企业安全组。</p>
主私网IP	<p>(可选) 输入弹性网卡的主私网地址。此IPv4地址必须属于交换机的CIDR网段中的空闲地址。如果您没有指定，创建弹性网卡时将自动为您分配一个空闲的私有地址。</p>

参数	描述
辅助私网IPv4	<p>(可选) 设置辅助私网IPv4地址。</p> <ul style="list-style-type: none"> ○ 暂不分配: 表示弹性网卡暂时不需要辅助私网IPv4地址。 ○ 自动分配: 手动输入辅助私网IPv4地址数量, 取值为1~9的整数。系统将自动为您分配所选交换机下相应数量的空闲IPv4地址。 ○ 指定地址: 手动添加辅助私网IPv4地址, 最多可添加9个辅助私网IPv4地址。
辅助私网IPv6	<p>(可选) 设置辅助私网IPv6地址。</p> <ul style="list-style-type: none"> ○ 暂不分配: 表示弹性网卡暂时不需要辅助私网IPv6地址。 ○ 自动分配: 手动输入辅助私网IPv6地址数量, 取值为1~10的整数。系统将自动为您分配所选交换机下相应数量的空闲IPv6地址。 ○ 指定地址: 手动补全辅助私网IPv6地址的后四位, 最多可添加10个辅助私网IPv6地址。
描述	(可选) 输入对弹性网卡的描述, 方便后期管理。
资源组	(可选) 选择一个资源组。更多有关资源组的详情, 请参见 资源组 。
标签	(可选) 选择一个或多个标签。更多有关标签的详情, 请参见 标签概述 。

6. 单击**创建网卡**, 完成创建。

执行结果

当网卡列表中新建弹性网卡的状态显示为**可用**时, 表示成功创建了弹性网卡。

后续步骤

单独创建弹性网卡后, 您可以将其绑定到实例上, 具体操作请参见[绑定弹性网卡](#)。

相关文档

- [CreateNetworkInterface](#)

6.4. 绑定弹性网卡

弹性网卡可以实现高可用集群搭建、低成本故障转移和精细化的网络管理。您可以在创建ECS实例时绑定弹性网卡, 也可以单独创建弹性网卡再绑定到ECS实例上。

前提条件

- 创建ECS实例时绑定弹性网卡, 需要先完成创建实例前的准备工作。更多信息, 请参见[使用向导创建实例](#)。
- 为已有ECS实例绑定弹性网卡时, 请确认以下注意事项:
 - 待绑定的ECS实例必须是I/O优化型实例规格, 且处于**已停止**或者**运行中**状态。

 **说明** 部分实例规格只在已停止状态下, 才支持绑定辅助弹性网卡。实例规格信息, 请参见[需要停止实例的ECS实例规格](#)。

- 确认实例仍能绑定弹性网卡。

 **说明** 一块弹性网卡一次只能绑定到一台ECS实例上, 但是一台ECS实例可以同时绑定多个弹性网卡。每种实例规格能绑定的弹性网卡数量, 请参见[实例规格族](#)。

- 如果ECS实例最后一次启动时间在2018年4月1日之前（包括但不限于启动新购的实例、重启、重开机），您必须重启一直保持运行中状态的实例，否则不支持绑定弹性网卡。

 **注意** 必须在控制台或者通过API RebootInstance重启ECS实例，在操作系统内重启无效。

- 您已单独创建弹性网卡，该弹性网卡处于可用状态。具体操作，请参见[创建弹性网卡](#)。
- 弹性网卡必须与待绑定的ECS实例属于同一个专有网络VPC。
- 弹性网卡必须与待绑定的ECS实例处于同一可用区。

背景信息

您可以通过以下两种方式绑定弹性网卡。

- 随实例创建绑定弹性网卡。

在控制台上创建ECS实例时，最多只能绑定两块弹性网卡，一块为主网卡，另一块是辅助网卡。具体操作，请参见[创建ECS实例时绑定弹性网卡](#)。

 **说明** 部分ECS实例规格不支持在创建实例时绑定辅助弹性网卡，可以在创建实例后单独绑定。更多信息，请参见[实例规格族](#)。

- 为实例绑定已单独创建的弹性网卡。

您可以在控制台的实例页面、弹性网卡页面或者安全组页面为实例绑定弹性网卡。具体操作，请参见[在实例页面为已有ECS实例绑定弹性网卡](#)、[在弹性网卡页面为已有ECS实例绑定弹性网卡](#)和[在安全组页面为已有ECS实例绑定弹性网卡](#)。

弹性网卡支持创建、绑定、解绑、删除弹性网卡的操作完成事件，您可以通过在云监控中设置弹性网卡事件通知以获取创建弹性网卡的操作结果。更多信息，请参见[弹性网卡事件通知](#)。

创建ECS实例时绑定弹性网卡

创建ECS实例的具体操作与说明，请参见[使用向导创建实例](#)。在创建ECS实例时绑定弹性网卡，您需要注意以下几项配置：

- 基础配置：

- 地域：所有地域均支持弹性网卡。
- 实例：选择一种支持绑定辅助弹性网卡的实例规格，而且必须是I/O优化型实例。更多信息，请参见[实例规格族](#)。
- 镜像：以下几种镜像无需配置即能自动识别弹性网卡：
 - Alibaba Cloud Linux 3.2104 64位
 - CentOS 8.0/8.1/8.2 64位
 - CentOS 7.3/7.4/7.5 64位
 - CentOS 6.8/6.9 64位
 - Debian 10.5/10.6 64位
 - Window Server 2008 R2及更高版本

如果是其他镜像，在创建好ECS实例后，您需要配置弹性网卡使其能被识别。具体操作，请参见[配置辅助弹性网卡](#)。

- 网络和安全组：

- 网络类型：必须为**专有网络**，为ECS实例选择已创建的专有网络VPC和虚拟交换机。
- 弹性网卡：单击**增加弹性网卡**新建一块弹性网卡，弹性网卡和ECS实例须属于同一可用区，可以分属于不同虚拟交换机。

ECS实例创建完成后，您可以前往实例详情的弹性网卡页签查看弹性网卡的状态，显示为已绑定时，表示绑定成功。

在实例页面为已有ECS实例绑定弹性网卡

1. 登录[ECS管理控制台](#)。
2. 在左侧导航栏，选择实例与镜像 > 实例。
3. 在顶部菜单栏左上角处，选择地域。
4. 找到需要绑定弹性网卡的实例，在操作列中，单击更多 > 网络和安全组 > 绑定辅助弹性网卡。
5. 在绑定辅助弹性网卡对话框中，选择弹性网卡后，单击确定。
绑定完成后，您可以前往实例详情的弹性网卡页签查看弹性网卡的状态，显示为已绑定时，表示绑定成功。

在弹性网卡页面为已有ECS实例绑定弹性网卡

1. 登录[ECS管理控制台](#)。
2. 在左侧导航栏，选择网络与安全 > 弹性网卡。
3. 在顶部菜单栏左上角处，选择地域。
4. 找到可用的辅助弹性网卡，在操作列中，单击绑定实例。
5. 在绑定实例对话框中，选择实例后，单击确定。
刷新列表，当弹性网卡的状态显示为已绑定时，表示绑定成功。

在安全组页面为已有ECS实例绑定弹性网卡

1. 登录[ECS管理控制台](#)。
2. 在左侧导航栏，选择网络与安全 > 安全组。
3. 在顶部菜单栏左上角处，选择地域。
4. 找到弹性网卡所在的安全组，在操作列中，单击管理弹性网卡。
5. 在安全组内弹性网卡页面，找到待绑定实例的弹性网卡，在操作列中，单击绑定实例。
6. 在绑定实例对话框中，选择实例后，单击确定。
绑定完成后，您可以前往网络与安全 > 弹性网卡页面查看弹性网卡的状态，显示为已绑定时，表示绑定成功。

后续步骤

根据ECS实例使用的镜像不同，部分镜像需要您手动配置弹性网卡后，绑定在实例上的弹性网卡才能被ECS实例识别。具体操作，请参见[配置辅助弹性网卡](#)。

需要停止实例的ECS实例规格

部分ECS实例规格只能在已停止状态下，才支持绑定或者解绑弹性网卡。具体操作，请参见[停止实例](#)。

具体ECS实例规格如下表所示。更多信息，请参见[实例规格族](#)。

实例规格族	实例规格
共享标准型实例规格族s6	ecs.s6-c1m1.small、ecs.s6-c1m2.large、ecs.s6-c1m2.small、ecs.s6-c1m4.large、ecs.s6-c1m4.small
突发性能实例规格族t6	ecs.t6-c1m1.large、ecs.t6-c1m2.large、ecs.t6-c1m4.large、ecs.t6-c2m1.large、ecs.t6-c4m1.large
突发性能实例规格族t5	ecs.t5-c1m1.large、ecs.t5-c1m2.large、ecs.t5-c1m4.large、ecs.t5-lc1m1.small、ecs.t5-lc1m2.large、ecs.t5-lc1m2.small、ecs.t5-lc1m4.large、ecs.t5-lc2m1.nano

实例规格族	实例规格
上一代共享型实例规格族xn4、n4、mn4、e4	<ul style="list-style-type: none"> ecs.xn4.small ecs.n4.small、ecs.n4.large ecs.mn4.small、ecs.mn4.large ecs.e4.small、ecs.e4.large

相关文档

相关文档

- [分配辅助私网IP地址](#)
- [RunInstances](#)
- [CreateInstance](#)
- [AttachNetworkInterface](#)

6.5. 配置辅助弹性网卡

在绑定辅助弹性网卡后，部分镜像无法自动识别辅助弹性网卡的IP地址并添加路由，导致无法正常使用辅助弹性网卡。本文介绍如何在ECS实例内部配置辅助弹性网卡，以识别辅助弹性网卡的IP地址并添加路由。

前提条件

- 已将辅助弹性网卡绑定至ECS实例。
- 已远程登录ECS实例。具体操作，请参见[连接方式概述ECS远程连接操作指南](#)。

背景信息

预装了自动配置工具的镜像可以自动配置绑定的辅助弹性网卡，在使用这类镜像时您无需再自行配置辅助弹性网卡，可以跳过本文操作。支持自动配置的镜像如下：

- Alibaba Cloud Linux 3.2104 64位
- CentOS 8.0/8.1/8.2 64位
- CentOS 7.3/7.4/7.5 64位
- CentOS 6.8/6.9 64位
- Debian 10.5/10.6 64位
- Window Server 2008 R2及更高版本

操作流程

1. 查看辅助弹性网卡IP地址的识别状态。

具体操作，请参见[查看弹性网卡IP地址的识别状态](#)。如果已识别IP地址，您无需再执行后续步骤。如果尚未识别IP地址，则需要执行后续步骤配置辅助弹性网卡。

2. 获取辅助弹性网卡的信息。

在配置辅助弹性网卡时，您可能需要填写主私网IP地址、MAC地址等信息，请提前获取信息方便后续填写。具体操作，请参见[获取弹性网卡的信息](#)。

本文以下表中的示例信息为例演示步骤，请您在配置时根据实际信息修改。

信息类型	示例信息
网卡名称	eth1

信息类型	示例信息
MAC地址	00:16:3e:0f:*.**.*
主私网IP地址	192.168.**.*2
子网掩码	255.255.255.0
网关地址	192.168.**.253

3. 配置识别辅助弹性网卡的IP地址。

不同的操作系统中适用的操作存在差异，如下表所示。

操作系统	相关章节
<ul style="list-style-type: none"> Alibaba Cloud Linux 2（网络服务类型为network-scripts） CentOS RedHat 	为Alibaba Cloud Linux 2、CentOS 6/7、或RedHat系统配置辅助弹性网卡（network-scripts）
Alibaba Cloud Linux 2（网络服务类型为systemd-networkd） <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 10px;"> <p> 说明 更多信息，请参见Alibaba Cloud Linux 2实例修改网络服务的方法及影响说明。</p> </div>	为Alibaba Cloud Linux 2系统配置辅助弹性网卡（systemd-networkd）
<ul style="list-style-type: none"> Ubuntu Debian 	为Ubuntu或Debian系统配置辅助弹性网卡
<ul style="list-style-type: none"> SUSE OpenSUSE 	为SUSE或OpenSUSE系统配置辅助弹性网卡

4. 检查是否已为辅助弹性网卡配置路由。

您可以运行命令 `route -n` 检查路由信息。如果辅助弹性网卡没有路由，或者已有路由不符合实际需要，请自行配置路由。部分系统中的配置路由操作示例，请参见：

- [在Alibaba Cloud Linux 2、CentOS 7系统中配置路由](#)
- [在CentOS 8系统中配置路由](#)

查看弹性网卡IP地址的识别状态

运行以下命令查看弹性网卡IP地址的识别状态。

```
ip address show
```

查询结果示例如下：

- 下图示例为主网卡（eth0）的IP地址已识别，辅助弹性网卡（eth1）的IP地址未识别，您需要按本文操作配置辅助弹性网卡。

```
[root@ecs ~]# ip address show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
   link/ether 00:16:3e:16:***:** brd ff:ff:ff:ff:ff:ff
   inet 192.168.***:**/24 brd 192.168.45.255 scope global dynamic eth0
       valid_lft 315359900sec preferred_lft 315359900sec
   inet6 fe80::216:3eff:***:** scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
   link/ether 00:16:3e:0f:***:** brd ff:ff:ff:ff:ff:ff
[root@ecs ~]#
```

- 下图示例为主网卡（eth0）和辅助弹性网卡（eth1）的IP地址都已识别，您无需再配置辅助弹性网卡。

```
[root@ecs ~]# ip address show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
   link/ether 00:16:3e:16:***:** brd ff:ff:ff:ff:ff:ff
   inet 192.168.***:**/24 brd 192.168.***:** scope global dynamic noprefixroute eth0
       valid_lft 315285190sec preferred_lft 315285190sec
   inet6 fe80::216:3eff:***:** scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
   link/ether 00:16:3e:0f:***:** brd ff:ff:ff:ff:ff:ff
   inet 192.168.***:**/24 brd 192.168.***:** scope global dynamic noprefixroute eth1
       valid_lft 315285190sec preferred_lft 315285190sec
   inet6 fe80::c6ab:1fb5:***:** scope link noprefixroute
       valid_lft forever preferred_lft forever
[root@ecs ~]#
```

说明 其中 00:16:3e:16:***:** 为主网卡的MAC地址， 00:16:3e:0f:***:** 为辅助弹性网卡的MAC地址。

获取弹性网卡的信息

阿里云支持通过实例元数据、ECS控制台、调用API获取弹性网卡的信息。具体操作如下：

- 在ECS实例内部通过实例元数据获取
 - 获取实例所有网卡的MAC地址。

```
curl http://100.100.100.200/latest/meta-data/network/interfaces/macs/
```

说明 在获取指定弹性网卡的主私网IP地址、子网掩码、网关地址时，需要使用MAC地址。

- 获取指定弹性网卡的主私网IP地址。

```
curl http://100.100.100.200/latest/meta-data/network/interfaces/macs/00:16:3e:19:***:**/primary-ip-address
```

- 获取指定弹性网卡的子网掩码。

```
curl http://100.100.100.200/latest/meta-data/network/interfaces/macs/00:16:3e:19:***:**/netmask
```

- 获取指定弹性网卡的网关地址。

```
curl http://100.100.100.200/latest/meta-data/network/interfaces/macs/00:16:3e:19:***:**/gateway
```

示例结果如下图所示。其中 00:16:3e:16:***:** 为主网卡的MAC地址， 00:16:3e:0f:***:** 为辅助弹性网卡的MAC地址。

说明 您可以结合 ip address show 的结果，确定主网卡和辅助弹性网卡MAC地址的显示顺序。

```
[root@ecs ~]# curl http://100.100.100.200/latest/meta-data/network/interfaces/macs/
00:16:3e:0f
00:16:3e:16 curl http://100.100.100.200/latest/meta-data/network/interfaces/macs/00:16:3e:0f /primary-ip-address
192.168.1 curl http://100.100.100.200/latest/meta-data/network/interfaces/macs/00:16:3e:0f /netmask
255.255. curl http://100.100.100.200/latest/meta-data/network/interfaces/macs/00:16:3e:0f /gateway
192.168. [root@ecs ~]#
```

- 通过ECS控制台获取
 - i. 登录ECS管理控制台。
 - ii. 在左侧导航栏，选择网络与安全 > 弹性网卡。
 - iii. 在弹性网卡页面，查看弹性网卡的主私网IP地址和MAC地址。

示例结果如下图所示。

网卡ID/名称	标签	交换机/专有网络	可用区	安全组ID	绑定实例ID	公网IP地址	私网IP地址	网卡类型/MAC地址 (辅助网卡)	状态/创建时间 (全部)	操作
eni-bp1a5gjj0bzhwz7q****		vsw-bp1a5gjj0bzhwz7q****	杭州 可用区K	sg-bp1a5gjj0bzhwz7q****	i-bp1a5gjj0bzhwz7q****		192.168.1 (主私网)	辅助网卡 00:16:3e:0f	已绑定 2021年11月19日 16:17	修改 解除实例 删除 管理辅助私网IP 安全组规则检测
eni-bp1a5gjj0bzhwz7q****		vsw-bp1a5gjj0bzhwz7q****	杭州 可用区K	sg-bp1a5gjj0bzhwz7q****			192.168.1 (主私网)	辅助网卡 00:16:3e:16	可用 2021年11月17日 18:23	修改 绑定实例 删除 管理辅助私网IP
eni-bp1a5gjj0bzhwz7q****		vsw-bp1a5gjj0bzhwz7q****	杭州 可用区K	sg-bp1a5gjj0bzhwz7q****			192.168.1 (主私网) 192.168.1 (辅助私网) 192.168.1 (辅助私网)	辅助网卡 00:16:3e:0f	可用 2021年8月25日 16:48	修改 绑定实例 删除 管理辅助私网IP

- 通过阿里云CLI等工具调用API DescribeNetworkInterfaces获取

```
aliyun ecs DescribeNetworkInterfaces \
--output cols=MacAddress,PrivateIpAddress rows=NetworkInterfaceSets.NetworkInterfaceSet[] \
--RegionId 'cn-hangzhou' \
--InstanceId 'i-bp1a5gjj0bzhwz7q****'
```

示例结果如下图所示。其中 00:16:3e:16:**** 为主网卡的MAC地址， 00:16:3e:0f:**** 为辅助弹性网卡的MAC地址。

说明 您可以结合 ip address show 的结果，确定主网卡和辅助弹性网卡MAC地址的显示顺序。

```
shell@Alicloud:~$ aliyun ecs DescribeNetworkInterfaces --output cols=MacAddress,PrivateIpAddress
rows=NetworkInterfaceSets.NetworkInterfaceSet[] --RegionId 'cn-hangzhou' --InstanceId 'i-bp1a5gjj0
bzhwz7q****'
MacAddress | PrivateIpAddress
-----|-----
00:16:3e:16:**** | 192.168.1
00:16:3e:0f:**** | 192.168.1
```

为Alibaba Cloud Linux 2、CentOS 6/7、或RedHat系统配置辅助弹性网卡 (network-scripts)

对网络服务类型为network-scripts的Alibaba Cloud Linux 2、CentOS 6/7和RedHat系统，您可以通过multi-nic-util工具自动配置或者修改网卡配置文件手动配置。

- 通过multi-nic-util工具自动配置辅助弹性网卡的步骤如下：

说明 如果您通过multi-nic-util工具为CentOS系统自动配置弹性网卡，请注意仅部分镜像版本支持使用multi-nic-util工具。如果使用CentOS 6镜像，请确保镜像版本为CentOS 6.8及以上；如果使用CentOS 7镜像，请确保镜像版本为CentOS 7.3及以上。如果镜像版本不支持使用multi-nic-util工具，请通过修改网卡配置文件手动配置辅助弹性网卡。

i. 下载并安装multi-nic-util工具。

```
wget https://image-offline.oss-cn-hangzhou.aliyuncs.com/multi-nic-util/multi-nic-util-0.6.tgz && \
tar -zxvf multi-nic-util-0.6.tgz && \
cd multi-nic-util-0.6 && \
bash install.sh
```

ii. 重启弹性网卡服务。

```
systemctl restart eni.service
```

● 通过修改网卡配置文件手动配置辅助弹性网卡的步骤如下：

i. 打开辅助弹性网卡的配置文件。

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

ii. 在网卡配置文件中添加辅助弹性网卡的信息，然后保存并关闭配置文件。

添加网卡信息的示例如下：

```
DEVICE=eth1 # 表示新配置的网卡接口。
BOOTPROTO=dhcp
ONBOOT=yes
TYPE=Ethernet
USERCTL=yes
PEERDNS=no
IPV6INIT=no
PERSISTENT_DHCLIENT=yes
HWADDR=00:16:3e:0f:**:** # 必须使用您查到的网卡对应的MAC地址。
DEFROUTE=no # 表示网卡接口不是默认路由。为避免在启动（ifup）辅助弹性网卡时改变ECS实例活动的默认路由，不要将eth1设置为默认路由。
```

iii. 重启网络服务。

■ CentOS 7以前版本（例如CentOS 6）：

```
service network restart
```

■ CentOS 7及以上版本、Alibaba Cloud Linux 2：

```
systemctl restart network
```

说明

- 当您完成配置后，可以根据需要为辅助弹性网卡配置路由。具体操作，请参见[Alibaba Cloud Linux 2、CentOS 7系统中配置路由](#)。
- 当您完成配置后，如果需要创建自定义镜像，请先执行命令`/etc/eni_utils/eni-cleanup`清理`/etc/dev/rules.d/70-persistent-net.rules`和`/etc/sysconfig/network-scripts/`下的网络配置。

为Alibaba Cloud Linux 2系统配置辅助弹性网卡（systemd-networkd）

对网络服务类型为systemd-networkd的Alibaba Cloud Linux 2系统，您需要通过修改网卡配置文件手动配置。

1. 打开辅助弹性网卡的配置文件。

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

2. 在网卡配置文件中添加辅助弹性网卡的信息，然后保存并关闭配置文件。

您可以为辅助弹性网卡分配动态IP或指定静态IP，请根据需要选择一种方式。添加网卡信息的示例如下：

- o 通过DHCP分配动态IP

```
[Match]
Name=eth1 # 表示新配置的网卡接口。
[Network]
DHCP=yes
[DHCP]
UseDNS=yes
```

- o 指定静态IP

```
[Match]
Name=eth1 # 表示新配置的网卡接口。
[Network]
Address=192.168.**.*2/24 # 表示分配的静态IP和子网掩码。
```

 **说明** 示例中 192.168.**.*2 为主私网IP地址，掩码位 /24 对应子网掩码 255.255.255.0。

3. 重启网络服务。

```
systemctl restart systemd-networkd
```

为Ubuntu或Debian系统配置辅助弹性网卡

对Ubuntu和Debian系统，您需要根据镜像版本修改对应的配置文件。

- 对Ubuntu 14.04、Ubuntu 16.04及Debian，操作步骤如下：

- i. 打开网卡配置文件。

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

- ii. 在网卡配置文件中添加辅助弹性网卡的信息，然后保存并关闭配置文件。

添加网卡信息的示例如下：

```
auto eth0
iface eth0 inet dhcp
auto eth1 # 表示新配置的网卡接口。
iface eth1 inet dhcp
```

 **说明** 主网卡（eth0）和辅助弹性网卡（eth1）的配置在同一个配置文件中维护，请注意不要遗漏主网卡的信息。

- iii. 重启网络服务。

- Ubuntu 16.04以前版本（例如Ubuntu 14.04）：

```
service networking restart
```

- Ubuntu 16.04、Debian:

```
systemctl restart networking
```

如果出现以下警告，不影响配置辅助弹性网卡生效。您可以运行 `ip address show` 查看辅助弹性网卡IP地址的识别状态。

```
root@ecs:~# service networking restart
Job for networking.service failed because the control process exited with error code.
see "systemctl status networking.service" and "journalctl -xe" for details.
```

- 对Ubuntu 18.04，操作步骤如下：

- i. 打开辅助弹性网卡的配置文件。

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

- ii. 在网卡配置文件中添加辅助弹性网卡的信息，然后保存并关闭配置文件。

 **说明** 编辑配置文件时请注意以下事项：

- 配置文件为 `YAML` 文件格式，您在配置时需要遵循 `YAML` 语法规则。
- `YAML` 不支持制表符（Tab）缩进，请使用空格缩进。
- 建议您直接复制默认配置文件 `/etc/netplan/99-netcfg.yaml` 中的内容进行修改，避免产生格式问题。

添加网卡信息的示例如下：

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

- iii. 应用添加的配置。

```
netplan apply
```

为SUSE或OpenSUSE系统配置辅助弹性网卡

对SUSE和OpenSUSE系统，您需要通过修改网卡配置文件手动配置。

1. 打开网卡配置文件。

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

- 2. 在网卡配置文件中添加辅助弹性网卡的信息，然后保存并关闭配置文件。

通过DHCP分配动态IP的示例如下：

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

- 3. 重启网络服务。

- SUSE Linux Enterprise Server 12以前版本：

```
service network restart
```

- o SUSE Linux Enterprise Server 12及以上版本：

```
systemctl restart network
```

在Alibaba Cloud Linux 2、CentOS 7系统中配置路由

如果您手动配置了辅助弹性网卡但还未配置路由，或者通过multi-nic-util工具自动配置了路由但不符合您的实际需要，您可以参考本章节自行配置路由。

1. 查看路由信息。

```
route -n
```

查询结果示例如下：

- o 下图示例为仅查询到了主网卡（eth0）的路由信息，辅助弹性网卡（eth1）还未配置路由。

```
[root@ecs ~]# route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 192.168.1.1 0.0.0.0 UG 0 0 0 eth0
169.254.169.254 0.0.0.0 255.255.255.255 U 1002 0 0 eth0
192.168.1.1 0.0.0.0 255.255.255.255 U 0 0 0 eth0
```

- o 下图示例为查询到了主网卡（eth0）和辅助弹性网卡（eth1）的路由信息。如果不符合您的实际需要，也可以自行修改。

```
[root@ecs ~]# route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 192.168.1.1 0.0.0.0 UG 0 0 0 eth0
0.0.0.0 192.168.1.1 0.0.0.0 UG 1001 0 0 eth1
169.254.169.254 0.0.0.0 255.255.255.255 U 1002 0 0 eth0
169.254.169.254 0.0.0.0 255.255.255.255 U 1003 0 0 eth1
192.168.1.1 0.0.0.0 255.255.255.255 U 0 0 0 eth0
192.168.1.1 0.0.0.0 255.255.255.255 U 0 0 0 eth1
```

2. 根据您的实际需要规划默认路由。

本文以下表中的示例信息为例演示步骤。

信息	示例取值
网卡名称	eth1
主私网IP地址	192.168.**.*2
网关地址	192.168.**.253
metric	1001

3. 配置默认路由。

下方命令为eth1添加默认路由，并创建了一张路由表和一条关联至该路由表的路由策略。其中，*table 1001*为路由表（和默认路由metric取值保持一致），*192.168.**.253*为网关地址，*192.168.**.*2*为eth1的主私网IP地址。

```
ip -4 route add default via 192.168.**.253 dev eth1 metric 1001 && \
ip -4 route add default via 192.168.**.253 dev eth1 table 1001 && \
ip -4 rule add from 192.168.**.*2 lookup 1001
```

4. 查看创建的路由表和策略路由。

```
ip route list table 1001 && \
ip rule list
```

创建成功的示例结果如下图所示。

```
[root@ecs ~]# ip route list table 1001 && \
> ip rule list
default via 192.168.1.253 dev eth1
0:      from all lookup local
32765:  from 192.168.1.0/24 lookup 1001
32766:  from all lookup main
32767:  from all lookup default
[root@ecs ~]#
```

5. 配置开机时自动更新路由。

按上文为eth1配置路由后，请按以下步骤配置开机时自动更新路由，否则重启实例后该路由配置会失效。

i. 打开/etc/rc.local文件。

```
vim /etc/rc.local
```

ii. 在/etc/rc.local文件中添加配置路由的信息，然后保存并关闭文件。

```
ip -4 route add default via 192.168.**.253 dev eth1 metric 1001
ip -4 route add default via 192.168.**.253 dev eth1 table 1001
ip -4 rule add from 192.168.**.*2 lookup 1001
```

iii. 为/etc/rc.local文件添加执行权限。

```
chmod +x /etc/rc.local
```

在CentOS 8系统中配置路由

如果系统自动配置了路由但不符合您的实际需要，您可以参考本章节自行配置路由。

1. 查看路由信息。

```
route -n
```

下图示例为查询到了主网卡（eth0）和辅助弹性网卡（eth1）的路由信息。如果不符合您的实际需要，也可以自行修改。

```
[root@ecs ~]# route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 192.168.1.253 0.0.0.0 UG 100 0 0 eth0
0.0.0.0 192.168.1.253 0.0.0.0 UG 101 0 0 eth1
192.168.1.0 0.0.0.0 255.255.255.0 U 100 0 0 eth0
192.168.1.0 0.0.0.0 255.255.255.0 U 101 0 0 eth1
[root@ecs ~]#
```

2. 根据您的实际需要规划默认路由。

本文以下表中的示例信息为例演示步骤。

信息	示例取值
网卡名称	eth1
主私网IP地址	192.168.**.*2
网关地址	192.168.**.253
table	1001

3. 创建配置路由用的脚本。

i. 创建并打开/root/route.sh。

- ii. 添加配置路由的信息，然后保存并关闭 `/root/route.sh` 文件。

下方脚本内容为 `eth1` 创建了一张路由表和一条关联至该路由表的路由策略。其中，`table 1001` 为路由表，`192.168.**.253` 为网关地址，`192.168.**.2` 为 `eth1` 的主私网 IP 地址。

```
#!/bin/bash
i=0
while true; do
    /usr/sbin/ip -4 route add default via 192.168.**.253 dev eth1 table 1001
    if [ $? -eq 0 ]; then
        break
    fi
    sleep 3
    let i++
    if [ $i -gt 10 ]; then
        exit -1
    fi
done
i=0
while true; do
    /usr/sbin/ip -4 rule add from 192.168.**.2 lookup 1001
    if [ $? -eq 0 ]; then
        break
    fi
    sleep 3
    let i++
    if [ $i -gt 10 ]; then
        exit -1
    fi
done
```

4. 配置默认路由。

```
sh /root/route.sh
```

5. 查看创建的路由表和策略路由。

```
ip route list table 1001 && \
ip rule list
```

示例结果如下图所示。

```
[root@ecs ~]# ip route list table 1001 && \
> ip rule list
default via 192.168.**.253 dev eth1
0:    from all lookup local
32765: from 192.168.**.2 lookup 1001
32766: from all lookup main
32767: from all lookup default
[root@ecs ~]#
```

6. 配置开机时自动更新路由。

按上文为 `eth1` 配置路由后，请按以下步骤配置开机时自动更新路由，否则重启实例后该路由配置会失效。

- i. 打开 `/etc/rc.local` 文件。

```
vim /etc/rc.local
```

- ii. 添加配置路由的信息，然后保存并关闭 `/etc/rc.local` 文件。

```
sh /root/route.sh
```

- iii. 为`/etc/rc.local`文件添加执行权限。

```
chmod +x /etc/rc.local
```

相关文档

- [DescribeNetworkInterfaces](#)

6.6. 分配辅助私网IP地址

单张弹性网卡（包括主网卡和辅助弹性网卡）支持分配一个或多个辅助私网IP地址。本文介绍如何分配辅助私网IP地址，并在ECS实例内部配置辅助私网IP地址。

背景信息

分配辅助私网IP地址适用于以下场景：

- 多应用场景：在ECS实例上托管了多个应用时，您可以为每个应用分配各自的辅助私网IP地址，每个应用对外均呈现一个独立的IP地址，实现在同一台ECS实例上提供多项服务，提升实例的利用率。
- 故障转移场景：当实例发生故障时，您可以将辅助弹性网卡从故障实例解绑并绑定至备用实例，通过其辅助私网IP访问的请求流量也随之切换到备用实例，实现故障转移。

分配辅助私网IP地址存在如下使用限制：

- 安全组限制：专有网络类型安全组可容纳的私网IP地址数量存在限制，请合理分配辅助私网IP地址。更多信息，请参见[安全组使用限制](#)。
- 弹性网卡限制：单张弹性网卡最多支持分配的私网IP地址数量与其状态有关。
 - 弹性网卡处于可用状态时，最多支持分配10个私网IP地址。
 - 弹性网卡处于已绑定状态时，最多支持分配的私网IP地址数量不能超过实例规格的支持上限。更多信息，请参见[实例规格族](#)。

操作流程

1. 完成准备工作。

- 确保对应的实例处于运行中（Running）状态。具体操作，请参见[启动实例](#)。
- 确保已将辅助弹性网卡绑定至实例。具体操作，请参见[绑定弹性网卡](#)。

2. 在ECS管理控制台为弹性网卡分配辅助私网IP地址。

您可以在弹性网卡页面、实例页面或者安全组页面完成分配操作。具体操作，请参见：

- [在弹性网卡页面分配辅助私网IP地址](#)
- [在实例页面分配辅助私网IP地址](#)
- [在安全组页面分配辅助私网IP地址](#)

3. 在实例内部配置已分配的辅助私网IP地址。

本文介绍如何配置辅助私网IPv4地址，配置操作和操作系统类型以及IP地址类型有关。具体操作，请参见：

- [为Windows实例配置辅助私网IPv4地址](#)
- [为Linux实例配置辅助私网IPv4地址（RHEL系列）](#)
- [为Linux实例配置辅助私网IPv4地址（Debian系列）](#)
- [为Linux实例配置辅助私网IPv4地址（SLES系列）](#)

 **说明** 配置辅助私网IPv6地址的具体操作，请参见[为Windows实例配置辅助私网IPv6地址](#)和[为Linux实例配置辅助私网IPv6地址](#)。

在弹性网卡页面分配辅助私网IP地址

1. 登录[ECS管理控制台](#)。
2. 在左侧导航栏，选择网络与安全 > 弹性网卡。
3. 在顶部菜单栏左上角处，选择地域。
4. 在弹性网卡页面，找到待操作的弹性网卡，然后在操作列中单击**管理辅助私网IP**。
5. 在**管理辅助私网IP**对话框中，在**辅助私网IPv4**或者**辅助私网IPv6**参数区域单击**增加**，并根据需要分配IP地址。
 - 不设置：系统会从该弹性网卡的IPv4私网网段和IPv6私网网段中随机分配IP地址。
 - 手动填写：手动输入辅助私网IP地址，确保取值在该弹性网卡的IPv4私网网段和IPv6私网网段中即可。

The screenshot shows a dialog box titled "管理辅助私网IP" (Manage Private IP). It contains the following information and controls:

- 弹性网卡ID/名称:** eni-xxxxxx
- 实例:** 未绑定实例
- 主私网IP:** 172.x.x.x
- 辅助私网IPv4:** 交换机地址段: 172.x.x.x. 当前网卡最多支持配置 9 个为 辅助私网IPv4 地址, 当前已输入 2 个 辅助私网IPv4 地址. Below this are two input fields: one with "172.x.x.x" and another with "不设置则自动生成 辅助私网IPv4". Each has a trash icon. A "增加" (Add) button is below.
- 辅助私网IPv6:** 交换机地址段: 2408:xxxxxx. 当前网卡最多支持配置 10 个为 辅助私网IPv6 地址, 当前已输入 2 个 辅助私网IPv6 地址. Below this are two input fields: one with "2408:xxxxxx" and another with "2408:4005:325:e704:不设置则自动生成 辅助私网IPv6". Each has a trash icon. A "增加" (Add) button is below.
- At the bottom right are "确定" (Confirm) and "关闭" (Close) buttons.

6. 单击**确定**。

在实例页面分配辅助私网IP地址

在实例页面分配辅助私网IP地址时，接受分配的对象是实例的主网卡。

1. 登录[ECS管理控制台](#)。
2. 在左侧导航栏，选择实例与镜像 > 实例。
3. 在顶部菜单栏左上角处，选择地域。
4. 在实例页面，找到待操作的实例，然后在操作列中单击**更多** > **网络和安全组** > **管理辅助私网IP**。
5. 在**管理辅助私网IP**对话框，单击**分配新IP**，并根据需要分配IP地址。
 - 自动分配：保持默认，系统会从该弹性网卡的IPv4私网网段和IPv6私网网段中随机分配IP地址。
 - 手动分配：手动输入辅助私网IP地址，确保取值在该弹性网卡的IPv4私网网段和IPv6私网网段中即可。

管理辅助私网IP

您可以对此实例分配新IP或者取消分配已有IP，也可以对现有IP进行修改。（单击“分配新IP”时，若将IP地址段留空，系统将会分配一个新的IP地址）

实例：[i-4qg173kub8v6h6m6m1u9p4l](#)

主网卡ID：[eni-4qg173kub8v6h6m6m1u9p4l](#)

主私网IP地址：[192.168.1.171](#)

IPv4 私网网段：[192.168.0.0/24](#)

IPv6 私网网段：[2408:4005:340:c800::/64](#)

IPv4 地址：
当前网卡最多支持配置 6 个私网 IPv4 地址
其中 1 个为主私网IP，5 个为辅助私网IP

[分配新IP](#)

IPv6 地址：
当前网卡最多支持配置 1 个 IPv6 地址

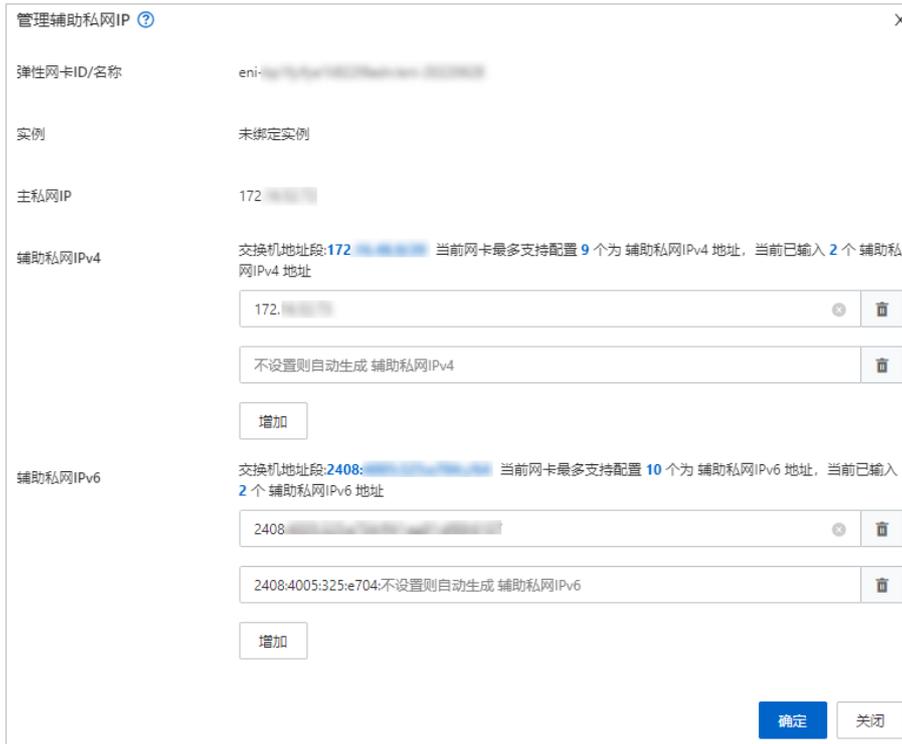
2408:4005:340:c800:

您做了如下修改：
自动分配 1 个 IPv4 地址。
自动分配 1 个 IPv6 地址。

6. 单击确定。

在安全组页面分配辅助私网IP地址

1. 登录[ECS管理控制台](#)。
2. 在左侧导航栏，选择网络与安全 > 安全组。
3. 在顶部菜单栏左上角处，选择地域。
4. 找到弹性网卡所在的安全组，在操作列中，单击管理弹性网卡。
5. 在安全组内弹性网卡页面，找到目标辅助网卡，在操作列中，单击管理辅助私网IP。
6. 在管理辅助私网IP对话框中，在辅助私网IPv4或者辅助私网IPv6参数区域单击增加，并根据需要分配IP地址。
 - 不设置：系统会从该弹性网卡的IPv4私网网段和IPv6私网网段中随机分配IP地址。
 - 手动填写：手动输入辅助私网IP地址，确保取值在该弹性网卡的IPv4私网网段和IPv6私网网段中即可。



7. 单击**确定**。

为Windows实例配置辅助私网IPv4地址

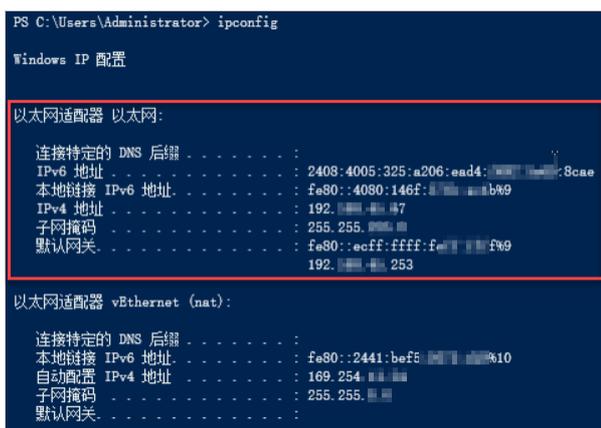
1. 远程连接ECS实例。

关于连接方式的介绍，请参见[连接方式概述ECS远程连接操作指南](#)。

2. 查询实例的子网掩码和默认网关。

- i. 打开命令提示符或Windows PowerShell工具。
- ii. 运行 `ipconfig` 命令查询ECS实例的子网掩码和默认网关。

返回示例如下图所示，当前网络连接名为以太网。



3. 打开网络和共享中心。

4. 单击**更改适配器设置**。

5. 双击当前网络连接名，例如以太网，然后在以太网状态对话框中单击**属性**。

6. 在以太网属性对话框中，双击**Internet 协议版本4 (TCP/IPv4)**。

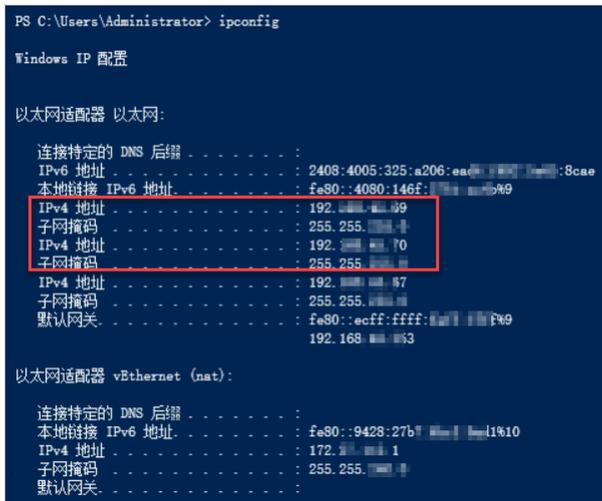
7. 在Internet 协议版本4 (TCP/IPv4) 属性对话框中，选择使用下面的IP地址，然后单击**高级**。

- 8. 在高级TCP/IP设置对话框中，设置IP地址。
 - i. 在IP地址区域，单击添加，然后输入已分配的IP地址和查询获取的子网掩码。
您可以重复该步骤为同一网卡适配器添加多个IP地址。



- ii. 在默认网关区域，单击添加，然后输入查询获取的默认网关。
- 9. 单击确定保存各对话框中的设置。

- 10. 运行 `ipconfig` 命令查看配置效果。
配置2个辅助私网IP的效果示例如下图所示。



说明

如果Windows实例配置辅助私网IP地址后无法访问公网，请参见[为什么我的Windows实例设置辅助私网IP后，无法访问公网环境？](#)。

为Linux实例配置辅助私网IPv4地址（RHEL系列）

本章节步骤说明如下：

- 适用的操作系统：Alibaba Cloud Linux 2/3、CentOS 6/7/8、Red Hat 6/7/8、Anolis 7/8、Fedora 33/34。
- 示例网卡：以主网卡 `eth0` 为例演示操作。如果您的操作对象为辅助弹性网卡，请根据实际情况修改网卡标识符。
 1. 远程连接ECS实例。
关于连接方式的介绍，请参见[连接方式概述ECS远程连接操作指南](#)。
 2. 使用 `ifconfig` 命令查询子网掩码，并使用 `route -n` 命令查询默认网关。
查询示例如下图所示。

```
[root@ecs ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.1 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::216:3eff:1:1 prefixlen 64 scopeid 0x20<link>
    ether 00:16:3e:1b:1:1 txqueuelen 1000 (Ethernet)
    RX packets 52842 bytes 77066906 (73.4 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4983 bytes 560229 (547.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@ecs ~]# route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 192.168.1.253 0.0.0.0 UG 0 0 0 eth0
169.254.169.254 0.0.0.0 255.255.255.255 U 1002 0 0 eth0
192.168.1.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
```

其中，net mask对应的 255.255.**.** 为IPv4子网掩码，Gateway对应的 192.**.**.253 为默认网关。

 **说明** 如果部分Linux发行版不支持 `ifconfig` 命令，可以使用 `ip a` 或 `ip addr show` 命令。

3. 修改网络配置文件。

- 如果配置单个私网IPv4地址，运行 `vi /etc/sysconfig/network-scripts/ifcfg-eth0:0` 命令，并添加相应的配置项。

配置项示例如下所示：

```
DEVICE=eth0:0
TYPE=Ethernet
BOOTPROTO=static
ONBOOT=yes
IPADDR=<分配的辅助私网IPv4地址1>
NETMASK=<IPv4子网掩码>
```

- 如果需要继续配置更多私网IPv4地址，递增DEVICE对应的序号并继续添加配置项即可。

例如运行 `vi /etc/sysconfig/network-scripts/ifcfg-eth0:1` 命令，添加配置项示例如下所示：

```
DEVICE=eth0:1
TYPE=Ethernet
BOOTPROTO=static
ONBOOT=yes
IPADDR=<分配的辅助私网IPv4地址2>
NETMASK=<IPv4子网掩码>
```

4. 根据操作系统类型运行相应的命令使配置生效。

操作系统	命令
<ul style="list-style-type: none"> Alibaba Cloud Linux 2 CentOS 7 Red Hat 7 Anolis 7 	运行以下任一种命令重启网络服务： <ul style="list-style-type: none"> <code>service network restart</code> <code>systemctl restart network</code>

操作系统	命令
<ul style="list-style-type: none"> ◦ CentOS 6 ◦ Red Hat 6 	运行 <code>service network restart</code> 命令重启网络服务。
<ul style="list-style-type: none"> ◦ Alibaba Cloud Linux 3 ◦ CentOS 8 ◦ Red Hat 8 ◦ Anolis 8 ◦ Fedora 33/34 	按以下步骤操作： <ol style="list-style-type: none"> i. 运行 <code>systemctl restart NetworkManager</code> 命令重启网络服务。 ii. 运行 <code>nmcli device reapply eth0</code> 命令重连 eth0网卡，或者运行 <code>reboot</code> 命令重启实例。

5. 运行 `ifconfig` 查看配置效果。

配置2个辅助私网IP的效果示例如下图所示。

```
[root@ecs ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.4.1 netmask 255.255.255.0 broadcast 192.168.4.255
    ether 00:16:3e:0f:00:00 txqueuelen 1000 (Ethernet)
    RX packets 3435 bytes 4093615 (3.9 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1161 bytes 184416 (180.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth0:0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.4.2 netmask 255.255.255.0 broadcast 192.168.4.255
    ether 00:16:3e:0f:00:00 txqueuelen 1000 (Ethernet)

eth0:1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.4.3 netmask 255.255.255.0 broadcast 192.168.4.255
    ether 00:16:3e:0f:00:00 txqueuelen 1000 (Ethernet)
```

为Linux实例配置辅助私网IPv4地址（Debian系列）

本章节步骤说明如下：

- 适用的操作系统：Ubuntu 18/20、Ubuntu 14/16、Debian 8/9/10。
 - 示例网卡：以主网卡 `eth0` 为例演示操作。如果您的操作对象为辅助弹性网卡，请根据实际情况修改网卡标识符。
1. 远程连接ECS实例。
关于连接方式的介绍，请参见[连接方式概述ECS远程连接操作指南](#)。
 2. 使用 `ifconfig` 命令查询子网掩码，并使用 `route -n` 命令查询默认网关。
查询示例如下图所示。

```
[root@ecs ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.1 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::216:3eff:1:1 prefixlen 64 scopeid 0x20<link>
    ether 00:16:3e:1b:1:1 txqueuelen 1000 (Ethernet)
    RX packets 52842 bytes 77066906 (73.4 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4983 bytes 560229 (547.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@ecs ~]# route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 192.168.1.253 0.0.0.0 UG 0 0 0 eth0
169.254.169.254 0.0.0.0 255.255.255.255 U 1002 0 0 eth0
192.168.1.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
```

其中，net mask对应的 255.255.**.* 为IPv4子网掩码，Gateway对应的 192.**.**.253 为默认网关。

 **说明** 如果部分Linux发行版不支持 `ifconfig` 命令，可以使用 `ip a` 或 `ip addr show` 命令。

3. 根据实例操作系统，选择配置辅助私网IP地址的方式。

o Debian系列：Ubuntu 18/20

- a. 禁用cloud-init网络配置，运行 `vim /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg` 命令，并添加相应的配置项。

配置项示例如下所示：

```
network: {config: disabled}
```

- b. 运行 `vim /etc/netplan/50-cloud-init.yaml` 命令打开网络配置文件，将原有的DHCP方式改为静态IP。

配置项示例如下所示：

```
network:
  version: 2
  ethernets:
    eth0:
      match:
        macaddress: 00:16:3e:36:**:**
      addresses:
        - <主私网IPv4地址>/<掩码位>
        - <分配的辅助私网IPv4地址1>/<掩码位>
        - <分配的辅助私网IPv4地址2>/<掩码位>
      gateway4: <默认网关>
```

 **说明** 其中，<掩码位> 替换为子网掩码对应的掩码位，例如子网掩码 255.255.255.0 对应掩码位 /24。

- c. 运行 `netplan apply` 命令重启网络服务。

d. 运行 `ip -a` 查看配置效果。

配置2个辅助私网IP的效果示例如下图所示。

```

root@ecs:~# ip a
1: lo: <LOOPBACK,UP,LOWER UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:16:3e:0f:00:00 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.1/24 brd 192.168.45.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet 192.168.1.2/24 brd 192.168.45.255 scope global secondary eth0
        valid_lft forever preferred_lft forever
    inet 192.168.1.3/24 brd 192.168.45.255 scope global secondary eth0
        valid_lft forever preferred_lft forever
    inet6 2408:4005:325:a206:0000:0000:0000:0000:5:8cae/128 scope global dynamic noprefixroute
        valid_lft 127787sec preferred_lft 84587sec
    inet6 fe80::216:3eff:fe00:0000/64 scope link
        valid_lft forever preferred_lft forever

```

o Debian系列：Ubuntu 14/16、Debian 8/9/10

a. 运行 `vi /etc/network/interfaces` 命令打开网络配置文件，并添加相应的配置项。

配置项示例如下所示：

```

auto eth0:0
iface eth0:0 inet static
address <分配的辅助私网IPv4地址1>
netmask <IPv4掩码>
auto eth0:1
iface eth0:1 inet static
address <分配的辅助私网IPv4地址2>
netmask <IPv4掩码>

```

b. 运行 `reboot` 命令重启实例。

c. 运行 `ifconfig` 命令查看配置效果。

配置2个辅助私网IP后的效果如下图所示。

```

root@ecs:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:16:3e:0f:00:00
          inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4146 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2373 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4046275 (4.0 MB)  TX bytes:299061 (299.0 KB)

eth0:0    Link encap:Ethernet  HWaddr 00:16:3e:0f:00:00
          inet addr:192.168.1.2  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

eth0:1    Link encap:Ethernet  HWaddr 00:16:3e:0f:00:00
          inet addr:192.168.1.3  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

```

为Linux实例配置辅助私网IPv4地址（SLES系列）

本章节步骤说明如下：

- 适用的操作系统：SUSE 11/12/15、OpenSUSE 15/42。
- 示例网卡：以主网卡 `eth0` 为例演示操作。如果您的操作对象为辅助弹性网卡，请根据实际情况修改网卡标识符。

1. 远程连接ECS实例。

关于连接方式的介绍，请参见[连接方式概述ECS远程连接操作指南](#)。

2. 使用 `ifconfig` 命令查询子网掩码，并使用 `route -n` 命令查询默认网关。

查询示例如下图所示。

```
[root@ecs ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.1 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::216:3eff:1:1:: prefixlen 64 scopeid 0x20<link>
    ether 00:16:3e:1b:1:1 txqueuelen 1000 (Ethernet)
    RX packets 52842 bytes 77066906 (73.4 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4983 bytes 560229 (547.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@ecs ~]# route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 192.168.1.253 0.0.0.0 UG 0 0 0 eth0
169.254.169.0 0.0.0.0 255.255.255.0 U 1002 0 0 eth0
192.168.1.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
```

其中，net mask对应的 255.255.**.** 为IPv4子网掩码，Gateway对应的 192.**.**.253 为默认网关。

 **说明** 如果部分Linux发行版不支持 `ifconfig` 命令，可以使用 `ip a` 或 `ip addr show` 命令。

- 运行 `vi /etc/sysconfig/network/ifcfg-eth0` 命令打开网络配置文件，添加如下配置项。

```
IPADDR_0=<分配的辅助私网IPv4地址1>
NETMASK_0=<IPv4子网掩码>
LABEL_0='0'
IPADDR_1=<分配的辅助私网IPv4地址2>
NETMASK_1=<IPv4子网掩码>
LABEL_1='1'
```

- 运行 `service network restart` 或 `systemctl restart network` 命令重启网络服务。
- 运行 `ifconfig` 查看配置效果。
配置2个辅助私网IP后的效果如下图所示。

```
ecs:~ # ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1 brd 127.255.255.255 scope host lo
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:16:3e:0f:1:1 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.1/24 brd 192.168.1.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet 192.168.1.9/24 brd 192.168.1.255 scope global secondary eth0:0
        valid_lft forever preferred_lft forever
    inet 192.168.1.10/24 brd 192.168.1.255 scope global secondary eth0:1
        valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 00:16:3e:12:1:1 brd ff:ff:ff:ff:ff:ff
```

相关文档

- [AssignPrivateIPAddresses](#)

6.7. 回收辅助私网IP地址

如果您的弹性网卡不再需要辅助私网IP地址，您可以回收弹性网卡上已分配的一个或多个辅助私网IP地址。

前提条件

回收辅助私网IP地址之前，请确认以下信息：

- 弹性网卡已分配辅助私网IP地址。
- 弹性网卡处于可用（Available）或者已绑定（InUse）状态。

- 回收主网卡上分配的辅助私网IP地址时，主网卡绑定的实例必须处于运行中（Running）或者已停止（Stopped）状态。

在弹性网卡页面回收辅助私网IP地址

- 登录[ECS管理控制台](#)。
- 在左侧导航栏，选择网络与安全 > 弹性网卡。
- 在顶部菜单栏左上角处，选择地域。
- 在弹性网卡页面，找到目标弹性网卡，在操作列，单击管理辅助私网IP。
- 在管理辅助私网IP对话框，找到要回收的一个或多个辅助私网IP地址，单击IP地址所在行的图标。
- 单击确定。

在实例页面回收辅助私网IP地址

在实例页面回收辅助私网IP地址时，效果是为实例的主网卡回收辅助私网IP地址。

- 登录[ECS管理控制台](#)。
- 在左侧导航栏，选择实例与镜像 > 实例。
- 在顶部菜单栏左上角处，选择地域。
- 在实例页面，找到目标实例，在操作列，单击更多 > 网络和安全组 > 管理辅助私网IP。
- 在管理辅助私网IP对话框，找到要回收的一个或多个辅助私网IP地址，单击对应的取消分配。
- 单击确定。

在安全组页面回收辅助私网IP地址

- 登录[ECS管理控制台](#)。
- 在左侧导航栏，选择网络与安全 > 安全组。
- 在顶部菜单栏左上角处，选择地域。
- 找到弹性网卡所在的安全组，在操作列中，单击管理弹性网卡。
- 在安全组内弹性网卡页面，找到目标辅助网卡，在操作列中，单击管理辅助私网IP。
- 在管理辅助私网IP对话框，找到要回收的一个或多个辅助私网IP地址，单击对应的取消分配。
- 单击确定。

相关文档

- [UnassignPrivateIpAddresses](#)

6.8. 修改弹性网卡

您可以根据需要修改弹性网卡的属性。辅助网卡支持修改网卡名称、描述信息以及辅助弹性网卡所属的安全组。主网卡仅支持修改网卡名称和描述信息，主网卡所属安全组需要通过变更ECS实例所在的安全组来更换。

前提条件

将主网卡加入到新的安全组前，请确保主网卡与新安全组属于同一个专有网络VPC和同一可用区。更多信息，请参见[弹性网卡概述](#)。

背景信息

如果您需要修改弹性网卡所在的安全组，ECS实例和弹性网卡对所属的安全组类型有以下要求：

- 一台ECS实例不能同时加入普通安全组和企业安全组。

- 一张弹性网卡不能同时加入普通安全组和企业安全组。
- 弹性网卡绑定到ECS实例时，两者的所属安全组类型必须相同。

关于安全组的更多信息，请参见[安全组概述](#)。

在弹性网卡页面修改网卡属性信息

以下步骤指导您在弹性网卡页面修改主网卡和辅助弹性网卡的名称、描述信息，以及辅助弹性网卡所属的安全组。

1. 登录[ECS管理控制台](#)。
2. 在左侧导航栏，选择**网络与安全 > 弹性网卡**。
3. 在顶部菜单栏左上角处，选择地域。
4. 找到目标弹性网卡，按照如下操作修改属性信息。
 - 网卡名称：在**弹性网卡ID/名称**列将鼠标悬浮至弹性网卡名称处，然后单击图标，按页面提示要求设置新的网卡名称。
 - 描述信息：在**弹性网卡ID/名称**列单击弹性网卡ID，在**基本信息**区域中，将鼠标悬浮至**描述**后，然后单击图标，按页面提示要求修改网卡描述。
 - 辅助弹性网卡所属安全组：在**辅助弹性网卡操作**列，单击**修改安全组**。在**修改安全组**对话框中选择加入新的安全组，或者从已有的安全组中移除，需至少保留一个安全组。
5. 单击**确定**。
刷新列表，查看辅助网卡的属性信息已变更，表示修改成功。

在安全组页面修改主网卡所属安全组

同一ECS实例的辅助网卡与主网卡可以属于不同的安全组，ECS实例变更安全组仅影响主网卡而不影响辅助弹性网卡。以下步骤指导您在安全组页面修改主网卡所属的安全组。

1. 登录[ECS管理控制台](#)。
2. 在左侧导航栏，选择**网络与安全 > 安全组**。
3. 在顶部菜单栏左上角处，选择地域。
4. 找到目标安全组，在**操作**列中，单击**管理实例**。
5. 在**安全组内实例列表**页面，您可以修改主网卡所属的安全组：
 - 按以下步骤将主网卡加入到新的安全组：
 - a. 在**安全组内实例列表**页面，单击**批量导入实例**。
 - b. 在**添加实例**对话框，选择主网卡绑定的实例ID，单击**确定**。
您可以同时选择多个ECS实例，主网卡会随着选择的ECS实例加入新的安全组。
 - 按以下步骤将主网卡移出已有的安全组：
 - a. 在**安全组内实例列表**页面，选择一台或多台实例，单击列表下方的**移出安全组**。
 - b. 在**ECS实例移出安全组**对话框，单击**确定**。
主网卡会随着ECS实例移出已有的安全组。ECS实例以及主网卡需至少保留一个安全组。

修改完成后，您可以前往**网络与安全 > 弹性网卡**页面，查看主网卡所属安全组已变更，表示修改成功。

在安全组页面修改网卡属性信息

以下步骤指导您在安全组页面修改主网卡和辅助弹性网卡的名称、描述信息，以及辅助弹性网卡所属的安全组。

1. 登录[ECS管理控制台](#)。
2. 在左侧导航栏，选择**网络与安全 > 安全组**。
3. 在顶部菜单栏左上角处，选择地域。

4. 找到目标安全组，在操作列中，单击**管理弹性网卡**。
5. 在**安全组内弹性网卡**页面，找到目标弹性网卡，按照如下操作修改属性信息。
 - 网卡名称：在**弹性网卡ID/名称**列将鼠标悬浮至弹性网卡名称处，然后单击图标，按页面提示要求设置新的网卡名称。
 - 描述信息：在**弹性网卡ID/名称**列单击弹性网卡ID，在**基本信息**区域中，将鼠标悬浮至**描述**后，然后单击图标，按页面提示要求修改网卡描述。
 - 辅助弹性网卡所属安全组：在**辅助弹性网卡操作列**，单击**修改安全组**。在**修改安全组**对话框中选择加入新的安全组，或者从已有的安全组中移除，需至少保留一个安全组。
6. 单击**确定**。
修改完成后，您可以前往**网络与安全 > 弹性网卡**页面，查看辅助网卡的属性信息已变更，表示修改成功。

相关文档

相关文档

- [ModifyNetworkInterfaceAttribute](#)

6.9. 编辑弹性网卡标签

标签用于标识具有相同特征的资源，例如所属组织相同或用途相同的弹性网卡，您可以基于标签方便地检索和管理资源。本文介绍如何编辑已有弹性网卡的标签。

背景信息

标签的使用说明、支持资源、使用限制等信息，请参见[标签概述](#)和[标签使用限制](#)。

操作步骤

1. 登录[ECS管理控制台](#)。
2. 在左侧导航栏，选择**网络与安全 > 弹性网卡**。
3. 在顶部菜单栏左上角处，选择地域。
4. 找到目标弹性网卡，在**标签列**将鼠标悬浮至图标，然后单击**编辑标签**。
5. 在**编辑标签**对话框，选择已有标签或新建标签，然后单击**确定**。

后续步骤

绑定标签后，您可以基于标签筛选弹性网卡并完成各种管理动作，例如为一类弹性网卡分配辅助私网IP、解绑一类弹性网卡等。

6.10. 解绑弹性网卡

如果您的实例不需要绑定弹性网卡，您可以解绑辅助弹性网卡。

前提条件

解绑弹性网卡之前，请确认以下信息：

- 要解绑的弹性网卡为辅助弹性网卡。主网卡不支持从实例上解绑。
- 要解绑弹性网卡的实例必须处于**已停止**或**运行中**状态。

 **说明** 部分实例规格只在已停止状态下，才支持解绑辅助弹性网卡。实例规格信息，请参见[需要停止实例的ECS实例规格](#)。

背景信息

弹性网卡支持创建、绑定、解绑、删除弹性网卡的操作完成事件，您可以通过在云监控中设置弹性网卡事件通知以获取创建弹性网卡的操作结果。更多信息，请参见[弹性网卡事件通知](#)。

在弹性网卡页面解绑弹性网卡

1. 登录[ECS管理控制台](#)。
2. 在左侧导航栏，选择[网络与安全](#) > [弹性网卡](#)。
3. 在顶部菜单栏左上角处，选择地域。
4. 找到状态为已绑定的网卡，在操作列中，单击[解绑实例](#)。
5. 在[解绑实例](#)对话框中，确认信息后，单击[确定](#)。
刷新列表，当弹性网卡的状态显示为可用时，表示已成功从实例上解绑弹性网卡。

在安全组页面解绑弹性网卡

1. 登录[ECS管理控制台](#)。
2. 在左侧导航栏，选择[网络与安全](#) > [安全组](#)。
3. 在顶部菜单栏左上角处，选择地域。
4. 找到弹性网卡所在的安全组，在操作列中，单击[管理弹性网卡](#)。
5. 在[安全组内弹性网卡](#)页面，找到状态为已绑定的弹性网卡，在操作列中，单击[解绑实例](#)。
6. 在[解绑实例](#)对话框中，确认信息后，单击[确定](#)。
刷新列表，当弹性网卡的状态显示为可用时，表示已成功从实例上解绑弹性网卡。

后续步骤

您可以对可用状态的弹性网卡执行以下操作：

- [绑定弹性网卡](#)
- [删除弹性网卡](#)
- [修改弹性网卡](#)

相关文档

- [DetachNetworkInterface](#)

6.11. 删除弹性网卡

如果您不再需要某个弹性网卡，可以删除弹性网卡。但您只能删除辅助网卡，不能删除主网卡。

前提条件

- 待删除的弹性网卡必须为可用状态。
- 如果弹性网卡已经绑定ECS实例，您必须先解绑弹性网卡。具体操作，请参见[解绑弹性网卡](#)。

 **说明** 实例被释放时，如果弹性网卡未从实例上解绑，那么弹性网卡也会随实例一起删除。

背景信息

删除弹性网卡会有以下影响：

- 该弹性网卡上的所有私有IP地址都会自动释放。
- 该弹性网卡会退出所有已加入的安全组。

弹性网卡支持创建、绑定、解绑、删除弹性网卡的操作完成事件，您可以通过在云监控中设置弹性网卡事件通知以获取创建弹性网卡的操作结果。更多信息，请参见[弹性网卡事件通知](#)。

在弹性网卡页面删除弹性网卡

1. 登录[ECS管理控制台](#)。
2. 在左侧导航栏，选择[网络与安全](#) > [弹性网卡](#)。
3. 在顶部菜单栏左上角处，选择地域。
4. 找到状态为可用的网卡，在操作列中，单击删除。
5. 在弹出的对话框里，单击**确定**。
刷新列表，如果网卡列表中不再出现该弹性网卡，说明您已经成功删除网卡。

在安全组页面删除弹性网卡

1. 登录[ECS管理控制台](#)。
2. 在左侧导航栏，选择[网络与安全](#) > [安全组](#)。
3. 在顶部菜单栏左上角处，选择地域。
4. 找到弹性网卡所在的安全组，在操作列中，单击[管理弹性网卡](#)。
5. 在安全组内[弹性网卡](#)页面，找到状态为可用的弹性网卡，在操作列中，单击删除。
6. 在弹出的对话框里，单击**确定**。
刷新列表，如果网卡列表中不再出现该弹性网卡，说明您已经成功删除网卡。

相关文档

- [DeleteNetworkInterface](#)

6.12. 基于弹性网卡操作完成事件实现业务自动化处理

在对弹性网卡完成创建、绑定、解绑或删除操作时，系统会产生弹性网卡操作完成事件，您可以通过阿里云云监控与消息服务，实现对弹性网卡操作完成事件通知的业务自动化处理。本文以Java代码为例，介绍基于弹性网卡操作完成事件实现业务自动化处理的相关操作。

背景信息

阿里云云监控支持在设置事件通知时关联消息服务MNS。当您通过云监控关联了弹性网卡操作完成事件和消息服务MNS时，可以同步将事件通知发送至消息服务MNS，然后您可以通过消息服务MNS（例如队列）获取该事件相关的信息，并根据消息内容触发后续动作，实现业务自动化处理。本最佳实践主要分为以下几步：

1. 在配置业务自动化处理之前，您需要分别创建队列以及云监控的报警规则，用于监控并收集弹性网卡操作完成事件。具体操作，请参见[准备工作](#)。
2. 配置业务自动化处理。本文以Java代码为例，轮询队列中的每一条消息，并将消息中包含的弹性网卡操作完成事件打印输出。具体操作，请参见[基于Java代码自动化处理弹性网卡操作完成事件](#)。

 **说明** 弹性网卡操作完成事件正在邀测中，如需使用，请[提交工单](#)。

准备工作

1. 创建消息服务MNS队列。
本文仅介绍最佳实践所必需的操作步骤，关于创建队列的更多信息，请参见[创建队列](#)。
 - i. 登录[消息服务MNS控制台](#)。

- ii. 在左侧导航栏，单击队列列表。
- iii. 在顶部菜单栏，选择地域。
队列所属地域需要和弹性网卡所属地域一致。例如，您需要监控的弹性网卡所属地域为华东1（杭州），则需要华东1（杭州）地域创建队列。
- iv. 单击创建队列。
- v. 在创建队列面板中，完成队列相关配置。
本示例中，自定义队列名称为eni-operate-completed-event，其他配置项保持默认配置。
- vi. 单击确定。
成功创建的队列如下图所示。

名称	可用消息	定时中消息	日志功能	创建时间	操作
eni-operate-completed-event 消息保存时长: 4天	0	0	未启用	2021年12月17日	详情 更多

2. 创建云监控报警事件。

本文仅介绍最佳实践所必需的操作步骤，关于创建事件报警的更多信息，请参见[设置事件通知](#)。

- i. 登录[云监控管理控制台](#)。
- ii. 在左侧导航栏，单击事件监控。
- iii. 在事件监控页面，单击报警规则页签，然后单击创建事件报警。
- iv. 在创建/修改事件报警页面，完成以下配置。
 - 报警规则名称：自定义名称。本示例中，自定义事件通知名称为eni-event-test-rule。
 - 事件类型：选择系统事件。
 - 产品类型：选择云服务器ECS。
 - 事件类型：选择状态通知。
 - 事件等级：选择信息。
 - 事件名称：选择网卡操作完成。
 - 资源范围：本示例保持默认配置。您可以根据需要自行设置。
 - 报警方式：本示例仅选中消息服务队列，并根据已经创建好的队列信息，设置地域与队列。您可以根据需要自行设置多种报警方式。
- v. 单击确定。
创建成功的报警规则如下图所示。

规则名称	启用	规则描述	资源范围	目标	操作
<input type="checkbox"/> eni-event-test-rule	已启用	云服务器ECS INFO NetworkInterface:NetworkInterfaceOperateCompleted	全部资源	消息服务队列 澳大利亚(悉尼) eni-operate-completed-event	修改 调试 禁用 删除

基于Java代码自动化处理弹性网卡操作完成事件

本文提供的Java代码示例均基于JDK 1.8完成测试，在实际处理过程中请基于您所使用的开发工具、编程语言等情况自行调整并测试。

消息服务MNS提供了关于队列操作的完整代码示例。更多信息，请参见[Java SDK版本说明](#)。

1. 在本地主机当前的用户目录下，手动创建名为`.aliyun-mns.properties`的文件，并在文件内添加接入点和AccessKey信息。

说明

- Linux系统用户目录为`/home/<username>/`；Windows系统用户目录为`C:\Users\<username>`。
- 文件名称必须为`.aliyun-mns.properties`，其中`.properties`是该文件的格式后缀。

```
mns.accountendpoint=<队列的公网接入点URL>
mns.accesskeyid=<yourAccessKeyId>
mns.accesskeysecret=<yourAccessKeySecret>
```

变量说明如下：

- <队列公网接入点>：获取队列公网接入点的具体操作，请参见[获取接入点](#)。
- <yourAccessKeyId>：您的阿里云账号的AccessKey ID信息。获取AccessKey的具体操作，请参见[获取AccessKey](#)。
- <yourAccessKeySecret>：您的阿里云账号的AccessKey Secret信息。

2. 基于Java开发工具创建Maven项目。

在配置业务自动化处理前，请确保已通过开发工具（Eclipse、IntelliJ IDEA等）创建了一个Maven项目。

3. 在pom.xml文件的 <dependencies></dependencies> 标记对中，添加阿里云SDK的Maven依赖。

 **说明** 如果您需要获取多种编程语言的新版SDK，请参见[OpenAPI开发者门户SDK中心](#)。

依次添加以下阿里云SDK的Maven依赖：

◦ SDK核心库

```
<dependency>
  <groupId>com.aliyun</groupId>
  <artifactId>aliyun-java-sdk-core</artifactId>
  <version>4.5.18</version>
</dependency>
```

◦ 云服务器ECS SDK

```
<dependency>
  <groupId>com.aliyun</groupId>
  <artifactId>aliyun-java-sdk-ecs</artifactId>
  <version>4.23.10</version>
</dependency>
```

◦ 消息服务MNS SDK

```
<dependency>
  <groupId>com.aliyun.mns</groupId>
  <artifactId>aliyun-sdk-mns</artifactId>
  <version>1.1.9</version>
</dependency>
```

◦ fastjson依赖

```
<dependency>
  <groupId>com.alibaba</groupId>
  <artifactId>fastjson</artifactId>
  <version>1.2.73</version>
</dependency>
```

4. 创建实体类，用于定义弹性网卡操作完成事件的结构体。

本示例中实体类命名为 `EniEventMessage`。关于弹性网卡操作完成事件通知结构体的说明，请参见[弹性网卡事件通知](#)。

说明 本文示例代码中均忽略了 `package` 信息，您在实际使用代码时注意自行添加 `package` 信息。

```
import java.util.Map;
public class EniEventMessage {
    private String resourceId;
    private String product;
    private String ver;
    private String instanceName;
    private String regionId;
    private String eventTime;
    private String name;
    private String ruleName;
    private String id;
    private String status;
    private Map<String, String> content;
    public String getResourceId() {
        return resourceId;
    }
    public void setResourceId(String resourceId) {
        this.resourceId = resourceId;
    }
    public String getProduct() {
        return product;
    }
    public void setProduct(String product) {
        this.product = product;
    }
    public String getVer() {
        return ver;
    }
    public void setVer(String ver) {
        this.ver = ver;
    }
    public String getInstanceName() {
        return instanceName;
    }
    public void setInstanceName(String instanceName) {
        this.instanceName = instanceName;
    }
    public String getRegionId() {
        return regionId;
    }
    public void setRegionId(String regionId) {
        this.regionId = regionId;
    }
    public String getEventTime() {
        return eventTime;
    }
    public void setEventTime(String eventTime) {
        this.eventTime = eventTime;
    }
    public String getName() {
        return name;
    }
    public void setName(String name) {
```

```
        this.name = name;
    }
    public String getRuleName() {
        return ruleName;
    }
    public void setRuleName(String ruleName) {
        this.ruleName = ruleName;
    }
    public String getId() {
        return id;
    }
    public void setId(String id) {
        this.id = id;
    }
    public String getStatus() {
        return status;
    }
    public void setStatus(String status) {
        this.status = status;
    }
    public Map<String, String> getContent() {
        return content;
    }
    public void setContent(Map<String, String> content) {
        this.content = content;
    }
}
```

5. 创建弹性网卡操作完成事件的业务自动化处理代码文件。

本示例中，实现业务自动化处理的类名为 `ConsumerDemo`，主要实现了获取消息服务MNS的队列消息，并输出事件通知的主要信息，最后清除已获取的队列消息。

```
import com.aliyun.mns.client.CloudAccount;
import com.aliyun.mns.client.CloudQueue;
import com.aliyun.mns.client.MNSClient;
import com.aliyun.mns.common.ClientException;
import com.aliyun.mns.common.ServiceException;
import com.aliyun.mns.common.utils.ServiceSettings;
import com.aliyun.mns.model.Message;
import java.util.Map;
public class ConsumerDemo {
    public static void main(String[] args) {
        // 与MNS的队列建立连接。
        CloudAccount account = new CloudAccount(
            ServiceSettings.getMNSAccessKeyId(),
            ServiceSettings.getMNSAccessKeySecret(),
            ServiceSettings.getMNSAccountEndpoint());
        MNSClient client = account.getMNSClient();
        try{
            // 获取名为eni-operate-completed-event队列的消息。
            CloudQueue queue = client.getQueueRef("eni-operate-completed-event");
            // 模拟轮询队列中的消息，实现业务自动化处理。
            for (int time = 0; time < 100; time++)
            {
                // 获取队列中的消息。
                Message popMsg = queue.popMessage();
                if (popMsg != null){
                    System.out.println("message handle: " + popMsg.getReceiptHandle());
                }
            }
        } catch (Exception e) {
            e.printStackTrace();
        }
    }
}
```

```
System.out.println("message body: " + popMsg.getMessageBodyAsString());
System.out.println("message id: " + popMsg.getMessageId());
System.out.println("message dequeue count:" + popMsg.getDequeueCount());
// 反序列化队列中的消息主体。
EniEventMessage messageBody = com.alibaba.fastjson.JSON.parseObject(popMs
g.getMessageBodyAsString(), EniEventMessage.class);
// 获取消息主体中包含的弹性网卡操作完成事件的内容。
Map<String, String> messageContent = messageBody.getContent();
// 获取弹性网卡ID信息。
String eniId = messageContent.get("eniId");
// 获取弹性网卡状态信息。
String eniStatus = messageContent.get("eniStatus");
// 获取操作结果。
String result = messageContent.get("result");
// 获取操作名称。
String operation = messageContent.get("operation");
// 获取操作弹性网卡请求ID。
String requestId = messageContent.get("requestId");
// 输出相关信息。
System.out.println("ENI ID: " + eniId);
System.out.println("ENI status: " + eniStatus);
System.out.println("result: " + result);
System.out.println("operation: " + operation);
System.out.println("requestId: " + requestId);
// 成功获取到弹性网卡事件内容后, 清除队列中对应的消息。
queue.deleteMessage(popMsg.getReceiptHandle());
System.out.println("delete message successfully.\n");
    }
}
} catch (ClientException ce)
{
    System.out.println("Something wrong with the network connection between client an
d MNS service."
        + "Please check your network and DNS availablity.");
    ce.printStackTrace();
} catch (ServiceException se)
{
    if (se.getErrorCode().equals("QueueNotExist"))
    {
        System.out.println("Queue is not exist.Please create queue before use");
    } else if (se.getErrorCode().equals("TimeExpired"))
    {
        System.out.println("The request is time expired. Please check your local mach
ine timeclock");
    }
    se.printStackTrace();
} catch (Exception e)
{
    System.out.println("Unknown exception happened!");
    e.printStackTrace();
}
client.close();
}
```

后续步骤

通过运行 `ConsumerDemo` 中的 `main` 函数，您可以获取订阅队列中的弹性网卡操作完成事件的通知内容，并根据相应的弹性网卡信息实现业务自动化处理。运行代码后的返回结果示例如下图所示，表示成功完成删除弹性网卡的操作。

```
message handle: AC1ADA4236BF42A579935-MyAxNjM5NzIzODYxNTQwIDMwMDAwIDIgMCMCBzbXFzZHN1
message body: {"resourceId":"acs:ecs:ap-southeast-au49-a01:eni/eni-p0wfdmoab","product":"ECS"
message id: AC1ADA4236BF42A57993559
message dequeue count:1
ENI ID: eni-p0wfdmoab
ENI status: Deleted
result: success
operation: DeleteNetworkInterface
requestId: 3A96ABC6-24AA-3397-9495-C6D67C54
delete message successfully.
```

7.弹性RDMA网卡

7.1. 使用ERI

弹性RDMA网卡（ERI）是一种可以绑定到ECS实例的虚拟网卡，ERI必须依附于弹性网卡（ENI）开启RDMA设备。ERI完全复用了弹性网卡所属的网络，让您无需改变业务组网，即可在原有网络下使用RDMA功能，体验RDMA带来的超低延迟。本文介绍如何在ECS实例上配置ERI。

背景信息

ERI基于神龙架构，使用ERI具有以下优势：

- 超低延迟：RDMA功能绕过内核协议栈，将数据直接从用户态程序转移到HCA中进行网络传输，极大地降低了CPU负载和延迟。ERI使弹性网卡具有传统RDMA网卡的优点，您可以在阿里云VPC中体验超低的延迟。
- 规模部署：传统的RDMA功能依赖于网络的无损特性，在规模部署时难度高且成本高。而ERI采用了自研的拥塞控制（CC）算法，容忍VPC网络中的传输质量变化（例如延迟、丢包等），在有损的网络环境中依然拥有良好的性能表现。
- 弹性扩展：ERI依附于弹性网卡，您可以随时创建支持ERI的弹性网卡并绑定到ECS实例，轻松实现弹性扩展。

ERI支持的接口和库：Libfabric 1.13.1、Intel MPI 2021.2、OpenMPI 4.1.1、EPSL v1.10、RSocket（自带RSocket，无需额外安装）。

操作步骤

1. 创建支持ERI的实例。

具体操作，请参见[使用向导创建实例](#)。在创建支持ERI的实例时，请注意下表中的配置项。

配置项	说明
地域及可用区	选择华北2（北京），可用区K。
实例规格	选择RDMA增强型实例规格族c7re的实例规格。
镜像	按需从以下镜像中选择一款镜像： <ul style="list-style-type: none"> ◦ Alibaba Cloud Linux 2/3 ◦ CentOS 7.9 ◦ Ubuntu 18.04/20.04 ◦ Debian 9.9

2. 创建启用ERI的弹性网卡。

具体操作，请参见[创建弹性网卡](#)。在创建启用ERI的弹性网卡时，请注意打开弹性RDMA接口开关。ERI会共用该弹性网卡的设置，包括弹性网卡的IP、应用于弹性网卡的安全组规则等。

 **说明** 只能在创建弹性网卡时启用ERI，不支持通过修改弹性网卡的属性启用ERI。

创建弹性网卡 创建弹性网卡说明
✕

网卡名称:

长度为2-128个字符，不能以http://或https://开头，必须以大小字母或中文开头，可包含数字，“_”或“-”。

* 专有网络:

* 交换机:

选择的交换机的可用区，需要和将绑定的实例相同
交换机地址段: 192.168.1.0/24 (vsw-...)

弹性RDMA接口

3. 将弹性网卡绑定至实例。

具体操作，请参见[绑定弹性网卡](#)。将启用ERI的弹性网卡绑定至实例后，如需解绑，必须先停止实例。

? 说明 单台实例最多绑定一个启用ERI的弹性网卡。

4. 远程连接实例。

具体操作，请参见[通过密码或密钥认证登录Linux实例](#)。

5. 在实例内配置弹性网卡。

部分镜像无法自动识别新绑定的辅助弹性网卡。您可以执行 `ifconfig` 命令查看，如果不能显示该网卡，请手动配置弹性网卡，具体操作，请参见[配置辅助弹性网卡](#)。

6. 在实例内安装ERI驱动。

i. 运行以下命令，更新前置软件包。

- Alibaba Cloud Linux 2/3、CentOS:

```
yum update -y
```

- Ubuntu、Debian: 无需更新

ii. (可选) 如果涉及kernel子版本的更新，需要重启实例生效，重启后请重新远程连接实例。

查看是否涉及kernel子版本的更新方法：

- a. 执行 `rpm -qa | grep kernel` 命令查看最新的kernel包版本。
- b. 执行 `uname -r` 命令查看操作系统的内核版本。

如果二者的版本不一致，说明涉及kernel子版本的更新，则需要重启实例。

iii. 运行以下命令，安装依赖的软件包。

- Alibaba Cloud Linux 2/3、CentOS:

```
yum install gcc-c++ dkms cmake kernel-devel kernel-headers libnl3 libnl3-devel
```

- Ubuntu、Debian:

```
apt-get install dkms cmake libnl-3-dev libnl-route-3-dev kernel-headers
```

iv. 运行以下命令，下载驱动安装包。

```
wget http://elastic-rdma.oss-cn-hangzhou.aliyuncs.com/erdma_installer.tar.gz
```

v. 运行以下命令，解压安装包并进入文件目录。

```
tar -xvf erdma_installer.tar.gz && cd erdma_installer
```

vi. 运行以下命令，安装驱动。

- 安装过程需要手动确认相关卸载步骤及自动下载步骤

```
sh install.sh
```

- 安装过程无需手动确认相关卸载步骤及自动下载步骤

```
sh install.sh --batch
```

当出现如下信息时，表示安装成功。

```
[root@i-01xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx]# sh install.sh --batch
Installing erdma for Linux
Starting installation at Thu Jun 16 08:19:56 PM CST 2022...
Checking for Linux headers availability...
Verifying dependencies...
Removing erdma package
start to uninstall rdma-core libraries
generate command: rpmbuild --rebuild --define '_dist .alinux3' --define '_target_cpu x86_64'
'KSRC /lib/modules/5.10.84-10.4.al8.x86_64/build' --define '_topdir /tmp/ERDMA.15011' --define
.al7.src.rpm
/root/erdma_installer/SRPMS/erdma-1.0.0-1.al8.src.rpm
/root/erdma_installer/SRPMS/erdma-1.0.0-1.el7.src.rpm
/root/erdma_installer/SRPMS/erdma-1.0.0-1.el8.src.rpm
erdma_ker_rpms: /root/erdma_installer/RPMS/alinux3/x86_64/erdma-1.0.0-1.al8.x86_64.rpm
package_dir: /root/erdma_installer
dist_rpm: alinux3
Installing erdma
Reloading erdma modules
Installation finished successfully.
```

7.2. 在RDMA增强型实例上部署Redis

使用弹性RDMA网卡（ERI）可以获得超低的延迟，更快地处理请求。本文介绍在RDMA增强型实例上分别部署eRDMA版Redis和社区版Redis，并压测处理请求的能力。

部署eRDMA版Redis

本步骤中以实例A作为Redis客户端，实例B作为Redis服务端。eRDMA版Redis需要配合已启用ERI的网卡使用（本文中简称RDMA网卡），实例配置示例如下：

- 规格：ecs.c7re.8xlarge
- 镜像：Alibaba Cloud Linux 2.1903 LTS 64位
- 实例属于同一安全组，默认内网互通
- 实例挂载了RDMA网卡，设备号为eth1

 **说明** 请确保实例已完成ER相关的配置，具体操作，请参见[使用ERI](#)。

- 实例B RDMA网卡的主私有IP：192.168.5.44
 1. [远程连接实例A和实例B](#)。
 2. 分别为实例A和实例B安装eRDMA版Redis。

i. 下载eRDMA版Redis的安装包。

```
wget https://redis-demo.oss-cn-hangzhou.aliyuncs.com/redis-rdma-betal.tar.gz
```

ii. 解压安装包。

```
tar -xf redis-rdma-betal.tar.gz
```

解压后得到redis-server、redis-cli、redis-benchmark文件。

iii. 查看实例的路由表，如果未优先使用RDMA网卡，则需要修改路由表设置。

示例如下图所示，实例所在网段为192.168.5.0，但192.168.5.0网段收发请求会优先使用主网卡（eth0），因此需要修改路由表，确保优先使用RDMA网卡（eth1）。

```
[root@redis-6.2.5]# route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
default gateway 0.0.0.0 UG 0 0 0 eth0
default gateway 0.0.0.0 UG 1001 0 0 eth1
link-local 0.0.0.0 255.255.0.0 U 1002 0 0 eth0
link-local 0.0.0.0 255.255.0.0 U 1003 0 0 eth1
192.168.5.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
192.168.5.0 0.0.0.0 255.255.255.0 U 0 0 0 eth1
```

修改路由表的命令示例如下：

```
route del -net 192.168.5.0 netmask 255.255.255.0 metric 0 dev eth0 && \
route add -net 192.168.5.0 netmask 255.255.255.0 metric 1000 dev eth0
```

3. 在实例B上启动Redis服务端。

```
./redis-server --rdma-bind 192.168.5.44 --rdma-port 6389 --protected-mode no --save
```

说明 192.168.5.44为实例B RDMA网卡的主私有IP，6389为需要监听的端口，请您在自行测试时按实际情况替换。

您也可以使用taskset命令将进程运行在指定的CPU上，例如：

```
taskset -c 0-1 ./redis-server --rdma-bind 192.168.5.44 --rdma-port 6389 --protected-mode no --save
```

```
[root@redis-server-rdma ~]# ./redis-server --rdma-bind 192.168.5.44 --rdma-port 6389 --protected-mode no --save
Hello Alibaba Cloud!
2370:C 02 Nov 2021 10:41:26.397 # oO00o000o000o Redis is starting oO00o000o000o
2370:C 02 Nov 2021 10:41:26.397 # Redis version=255.255.255, bits=64, commit=b1dac00c, modified=1, pid=2370, just started
2370:C 02 Nov 2021 10:41:26.397 # Configuration loaded
2370:M 02 Nov 2021 10:41:26.397 * monotonic clock: POSIX clock_gettime
2370:M 02 Nov 2021 10:41:26.411 # Redis listening socket *:6379
2370:M 02 Nov 2021 10:41:26.411 # Redis listening socket :::6379
2370:M 02 Nov 2021 10:41:26.411 # Redis listening rsocket 192.168.5.44:6389

Redis 255.255.255 (b1dac00c/1) 64 bit
Running in standalone mode
TCP Port: 6379
RDMA Port: 6389
PID: 2370
https://redis.io

2370:M 02 Nov 2021 10:41:26.413 # Server initialized
2370:M 02 Nov 2021 10:41:26.413 # WARNING overcommit memory is set to 0! Background save may fail under low memory condition. To fix this issue add 'vm.overcommit_memory = 1' to /etc/sysctl.conf and then reboot or run the command 'sysctl vm.overcommit_memory=1' for this to take effect.
2370:M 02 Nov 2021 10:41:26.413 * Ready to accept connections
```

4. 在Redis客户端上测试连接和访问Redis服务端。

i. 连接Redis服务端。

```
./redis-cli -h 192.168.5.44 -p 6389 --rdma
```

ii. 使用redis-benchmark进行压测。

以下命令模拟从100个客户端向服务端发送1,000,000次SET命令的请求：

```
./redis-benchmark -h 192.168.5.44 -p 6389 --rdma -n 1000000 -t set -c 100
```

您也可以启动多个压测进程进行混合压测，参考以上步骤再部署1个Redis客户端，在2个Redis客户端上分别启动多个压测进程，然后在Redis服务端上查看OPS。

● 在Redis客户端上同时启动8个SET压测进程的示例命令：

```
./redis-benchmark -h 192.168.5.44 -p 6389 --rdma -n 100000000 -t set --threads 8 -c 100
```

● 在Redis客户端上同时启动8个GET压测进程的示例命令：

```
./redis-benchmark -h 192.168.5.44 -p 6389 --rdma -n 100000000 -t get --threads 8 -c 100
```

● 在Redis服务端上查看OPS的示例命令：

```
./redis-cli -h 192.168.5.44 -p 6389 --rdma info | grep instantaneous_ops_per_sec
```

 **说明** 请新打开一个远程连接窗口，然后输入查看命令。

部署社区版Redis

本步骤中以实例C作为Redis客户端，实例D作为Redis服务端。实例配置示例如下：

- 规格：ecs.c7re.8xlarge
- 镜像：Alibaba Cloud Linux 2.1903 LTS 64位
- 实例属于同一安全组，默认内网互通
- 实例D主网卡的主私有IP：192.168.5.49

1. 远程连接实例C和实例D。

2. 分别为实例C和实例D安装社区版Redis。

i. 下载社区版Redis的安装包。

```
wget https://github.com/redis/redis/archive/refs/tags/6.2.5.zip
```

更多版本，请参见[Redis Github项目地址](#)。

ii. 解压安装包并进入文件目录。

```
unzip 6.2.5.zip && cd redis-6.2.5
```

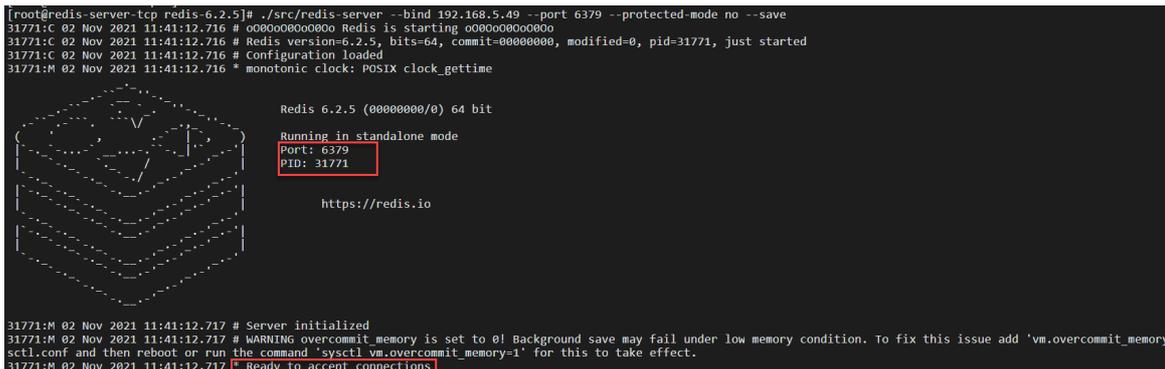
iii. 编译安装Redis。

```
make -j
```

3. 在实例D上启动Redis服务端。

```
./src/redis-server --bind 192.168.5.49 --port 6379 --protected-mode no --save
```

 **说明** 192.168.5.49为实例D主网卡的主私有IP，6379为需要监听的端口，请您在自行测试时按实际情况替换。



4. 在Redis客户端上测试连接和访问Redis服务端。

- i. 连接Redis服务端。

```
./src/redis-cli -h 192.168.5.49 -p 6379
```

- ii. 使用redis-benchmark进行压测。

以下命令模拟从100个客户端向服务端发送1,000,000次SET命令的请求：

```
./src/redis-benchmark -h 192.168.5.49 -p 6379 -n 1000000 -t set -c 100
```

您也可以启动多个压测进程进行混合压测，参考以上步骤再部署1个Redis客户端，在2个Redis客户端上分别启动多个压测进程，然后在Redis服务端上查看OPS。

- 在Redis客户端上同时启动8个SET压测进程的示例命令：

```
./src/redis-benchmark -h 192.168.5.49 -p 6379 -n 100000000 -t set --threads 8 -c 100
```

- 在Redis客户端上同时启动8个GET压测进程的示例命令：

```
./src/redis-benchmark -h 192.168.5.49 -p 6379 -n 1000000 -t get --threads 8 -c 100
```

- 在Redis服务端上查看OPS的示例命令：

```
./src/redis-cli -h 192.168.5.49 -p 6379 info | grep instantaneous_ops_per_sec
```

说明 请新打开一个远程连接窗口，然后输入查看命令。

7.3. 基于RDMA增强型实例部署HPC应用

使用弹性RDMA网卡（ERI）可以获得超低的延迟，更快地处理请求。本文介绍如何创建以RDMA增强型实例作为计算节点的HPC集群，并部署IMB测试基于eRDMA的通信性能。

背景信息

Intel® oneAPI是一个统一的编程模型，致力于为跨CPU、GPU、FPGA、专用加速器等不同计算架构的应用程序提供统一的编程体验，同时基于该模型提供了Intel® oneAPI Base Toolkit、Intel® oneAPI HPC Toolkit、Intel® AI Analytics Toolkit等一系列产品。

IMB（Intel® MPI Benchmarks）用于评估HPC集群在不同消息粒度下节点间点对点、全局通信的效率。

步骤一：准备HPC集群

使用弹性高性能计算创建HPC集群以及用户。

1. 登录弹性高性能计算控制台。

2. 创建HPC集群。

- i. 在集群页面右上角，单击创建集群。
- ii. 按向导顺序逐步完成硬件、软件、基本配置。

本文示例配置如下表所示，完整配置项的说明，请参见[使用向导创建集群](#)。

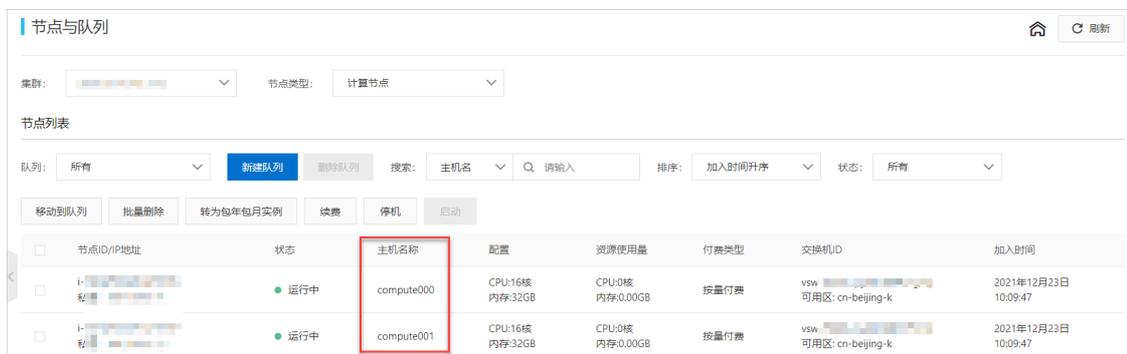
配置类型	配置项	示例配置
硬件配置	可用区	必须选择支持c7re规格族的可用区，目前邀测地域为华北2（北京）可用区K。
	部署方式	本文以精简为例，登录节点、管控节点混合部署在一台实例上。
	计算节点	必须为计算节点选择c7re规格（ecs.c7re.4xlarge），节点数量为2。
	登录节点	可以根据需要选择实例规格。
软件配置	镜像类型、镜像	本文以公共镜像和CentOS_7.6_64为例。
	调度器	本文以pbs为例。
	域账号服务	本文以nis为例。
	名称	本文以c7recluster为例。
基础配置	登录节点方式	选择密码方式，并输入和确认密码。 <div style="border: 1px solid #ccc; padding: 5px; background-color: #e6f2ff;"> ? 说明 该配置项对应root用户的密码。 </div>

- iii. 选中E-HPC服务条款，然后在页面右上角单击确认。

3. 查看计算节点的名称。

- i. 在集群页面中找到新创建的HPC集群（下文统一称为c7recluster集群），单击右上角的节点。
- ii. 在节点与队列页面，查看主机名称列中的名称。

本文中2个计算节点的名称分别为compute000和compute001。



4. 创建用户。

- i. 在左侧导航栏，选择资源管理 > 用户。
- ii. 单击新增用户。

iii. 在新增用户对话框，完成用户配置。

配置项	示例配置
用户名	本文以c7reclusterUser为例。新增用户后，在所有节点中均会创建一个普通用户，对应的路径为/home/c7reclusterUser。
用户组	需要执行sudo命令安装软件，必须选择sudo权限组。
密码	输入和确认该普通用户的登录密码。

iv. 单击确定。

步骤二：准备工具

您需要提前下载以下工具的安装文件：

- multi-nic-util：用于在Cent OS 7.6镜像中配置识别弹性网卡。
- ERI驱动：用于启用ERI。
- Intel® oneAPI安装包：用于部署IMB。
 1. 登录[弹性高性能计算控制台](#)。
 2. 下载multi-nic-util以及ER驱动。
 - i. 在集群页面找到c7recluster集群，在右上角单击远程连接。
 - ii. 在远程连接面板，输入普通用户的用户名c7reclusterUser及其密码，然后单击ssh连接。
 - iii. 分别运行以下命令下载multi-nic-util工具和ER驱动。

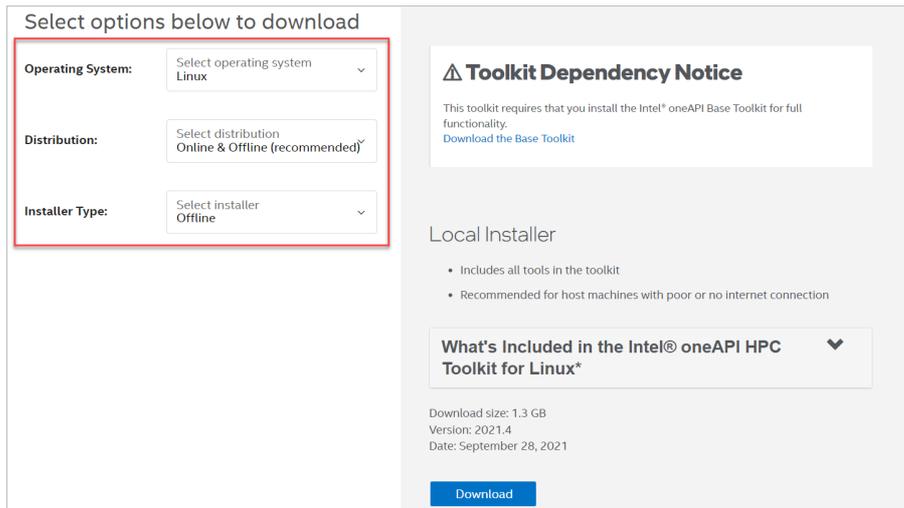
```
wget https://image-offline.oss-cn-hangzhou.aliyuncs.com/multi-nic-util/multi-nic-util-0.6.tgz
wget https://erdma.oss-cn-hangzhou.aliyuncs.com/aliyun-erdma-installer-1.0.0.tar.gz
```

 **说明** 在登录节点下载文件后，会自动同步到其他节点。

3. 下载Intel® oneAPI。

下载地址和相关说明，请参见[Intel® oneAPI下载页面](#)。本文以Offline的方式安装Intel® oneAPI 2021版本，在下载页面的选项如下图所示，下载的安装包名称示例为L_HPCKit_p_2021.4.0.3347_offline.sh。

 **说明** 您可以在本地下载后，通过OSS等方式传输到登录节点。



步骤三：为计算节点启用ERI

如需使用ERI，必须为计算节点绑定弹性RDMA网卡，并安装相应驱动以启用ERI。

1. 登录[ECS管理控制台](#)。
2. 创建弹性RDMA网卡。

重复以下步骤，创建2张弹性RDMA网卡。

- i. 在左侧导航栏，单击网络与安全 > 弹性网卡。
- ii. 在顶部菜单栏左上角处，选择地域华北2（北京）。
- iii. 在弹性网卡页面，单击创建弹性网卡。
- iv. 在创建弹性网卡对话框，完成弹性网卡配置。

本文示例配置如下表所示，完整配置项的说明，请参见[创建弹性网卡](#)。

配置项	示例配置
专有网络	选择和c7recluster集群相同的专有网络。
交换机	选择和c7recluster集群相同的交换机。
弹性RDMA接口	打开弹性RDMA接口开关。
安全组	选择和c7recluster集群相同的安全组。

- v. 单击确定。
3. 将弹性RDMA网卡绑定至c7recluster集群的计算节点。
重复以下步骤，分别为计算节点compute000和compute001绑定弹性RDMA网卡。
 - i. 找到新创建的弹性RDMA网卡，在操作列中，单击绑定实例。
 - ii. 选择计算节点对应的实例，然后单击确定。
 4. 为计算节点配置弹性网卡并安装ERI驱动。

Cent OS 7.6不支持自动识别辅助弹性网卡，因此需要手动配置。

- i. 在左侧导航栏，单击实例与镜像 > 实例。

- ii. 找到并远程连接计算节点对应的实例。

远程连接实例的方法介绍，请参见[连接方式概述ECS远程连接操作指南](#)。

 **说明** 登录实例时输入普通用户的用户名c7reclusterUser及其密码。

如下图所示，multi-nic-util和ER驱动的安装文件已同步到计算节点。

```
> c7reclusterUser@compute001:~$
Last login: Thu Dec 23 15:23:49 2021 from 100.100.100.100
Welcome to Alibaba Cloud Elastic Compute Service !

[c7reclusterUser@compute001 ~]$ ls
aliyun-erdma-installer-1.0.0.tar.gz multi-nic-util-0.6.tgz
```

- iii. 分别运行以下命令配置弹性网卡。

```
tar -zxvf multi-nic-util-0.6.tgz
cd multi-nic-util-0.6
sudo bash install.sh
sudo systemctl restart eni.service
```

 **说明** 包含 `sudo` 的命令可能要求输入root用户的密码，按提示输入即可。

- iv. 返回普通用户的目录。

本文中以普通用户c7reclusterUser登录，示例命令如下：

```
cd /home/c7reclusterUser
```

- v. 分别运行以下命令安装ER驱动。

```
tar -xf aliyun-erdma-installer-1.0.0.tar.gz
cd aliyun-erdma-installer
sudo sh ./erdma_install.sh -y
```

 **说明** 包含 `sudo` 的命令可能要求输入root用户的密码，按提示输入即可。

步骤四：在集群登录节点上部署IMB

1. 切换至登录节点的远程连接窗口（普通用户登录）。
2. 安装Intel® oneAPI。

以将下载的 `_l_HPCKit_p_2021.4.0.3347_offline.sh` 安装至 `/home/c7reclusterUser/oneAPIDIR` 目录为例，示例命令如下：

```
sh ./l_HPCKit_p_2021.4.0.3347_offline.sh -a --silent --eula accept --components intel.oneapi.lin.mpi.devel --install-dir /home/c7reclusterUser/oneAPIDIR --ignore-errors
```

 **说明** 更多安装操作的说明，请参见[Intel® oneAPI安装指南](#)。

3. 设置环境变量。

```
source /home/c7reclusterUser/oneAPIDIR/setvars.sh
```

4. 分别运行以下命令编译IMB。

```
cd /home/c7reclusterUser/oneAPI/mpi/latest/benchmarks/imb/src_c
make
```

编译成功后，会生成名为 *IMB-MPI1* 的可执行文件。

步骤五：在计算节点上执行IMB测试

1. 切换至计算节点的远程连接窗口（普通用户登录）。
2. 修改 */home/c7reclusterUser/.bashrc* 文件。

在文件尾部添加以下内容：

```
export FI_VERBS_RX_IOV_LIMIT=1
```

3. 修改 */etc/security/limits.conf* 文件。

在文件尾部添加以下内容：

```
* hard memlock unlimited
* soft memlock unlimited
```

 **说明** 该步骤需要在所有计算节点上执行。

4. 关闭当前的远程连接窗口，重新登录任一个计算节点（普通用户登录）。
5. 执行IMB测试。

基于启用了ERI的计算节点 *compute000* 和 *compute001* 执行IMB测试，了解在HPC集群中MPI点到点消息通讯的延迟和带宽，示例命令如下：

```
source /home/c7reclusterUser/oneAPI/mpi/latest/benchmarks/imb/src_c
cd /home/c7reclusterUser/oneAPI/mpi/latest/benchmarks/imb/src_c
mpirun -n 2 -hosts compute001,compute000 -ppn 1 ./IMB-MPI1 pingpong
```

 **说明** 可执行文件路径、计算节点名称必须和上方步骤保持一致。

7.4. 基于RDMA增强型实例部署Spark集群

使用弹性RDMA网卡（ERI）可以获得超低的延迟，更快地处理请求。本文介绍如何创建以RDMA增强型实例作为节点的Spark集群，并部署Benchmark测试Spark集群处理负载的性能。

背景信息

Benchmark是一种基准性能测试工具，主要用于测试负载的执行时间、传输速度、吞吐量和资源占用率等。

步骤一：安装Hadoop大数据集群

安装Hadoop大数据集群。具体操作，请参见[通过Fast MR自动拉起大数据集群](#)。

部署Hadoop大数据集群时，推荐的环境信息如下：

- Hadoop版本：Hadoop 2.7.7
- Spark版本：Spark 2.4.0
- ECS实例规格：RDMA增强型实例规格族c7re

关于该实例的更多信息，请参见[RDMA增强型实例规格族c7re](#)。

步骤二：配置RDMA

1. 登录集群主节点上的ECS实例。

具体操作，请参见[通过密码或密钥认证登录Linux实例](#)。

2. 在实例内完成RDMA相关配置。

o 网络配置

a. 运行以下命令，打开`/etc/hosts`文件。

```
vim /etc/hosts
```

b. 按键进入编辑模式，在配置文件中修改以下内容：

```
192.168.13.31 worker1 master1
192.168.13.32 worker2
192.168.13.33 worker3
192.168.13.34 worker4
192.168.13.36 worker5
192.168.13.37 worker6
192.168.13.38 worker7
192.168.13.39 worker8
```

 **说明** 请根据实际情况，将IP地址替换为实际RDMA网卡对应的IP地址。

c. 按`Esc`键退出编辑模式，输入`:wq`并按下`Enter`键，保存并退出文件。

o yarn配置

运行以下命令，进行yarn配置。

```
RDMA_IP=`ip addr show eth1 | grep "inet\b" | awk '{print $2}' | cut -d/ -f1`
export YARN_NODEMANAGER_OPTS="-Dyarn.nodemanager.hostname=$RDMA_IP"
export SPARK_LOCAL_IP=$RDMA_IP
```

 **说明** 请根据实际情况，将`eth1`替换为实际RDMA网卡名称。

o Spark配置

运行以下命令，进行Spark配置。

```
export SPARK_LOCAL_IP=`/sbin/ip addr show eth1 | grep "inet\b" | awk '{print $2}' | cut -d/ -f1`
```

 **说明** 请根据实际情况，将`eth1`替换为实际RDMA网卡名称。

3. 运行以下命令，启动hdfs和yarn。

```
`${HADOOP_HOME}/sbin/start-all.sh
```

步骤三：执行Benchmark测试

1. 登录集群主节点上的ECS实例。

具体操作，请参见[通过密码或密钥认证登录Linux实例](#)。

2. 单击[Benchmark安装包](#)，下载Benchmark安装包至本地，并上传到`/root`目录。

安装包文件介绍：

- o `rdmalib`：运行spark-rdma需要的native库，对应文件包括`libdisni.so`和`liblic.so`。

- plugin-sparkrdma: 支持spark rdma的插件, 对应文件为 *spark-rdma-for-spark-2.4.0-jar-with-dependencies.jar*。
 - benchmark-tpcxhs: 大数据benchmark, 对应文件为 *TPCx-HS-Runtime-Suite*。
3. 运行以下命令, 配置环境变量。

```
export LD_LIBRARY_PATH=/path/to/rdmalib
```

4. 配置Spark。

- i. 运行以下命令, 打开配置文件 *spark-defaults.conf*。

```
vim /opt/spark-2.4.0-bin-hadoop2.7/conf/spark-defaults.conf
```

- ii. 按键进入编辑模式, 将配置文件修改为以下内容:

```
spark.master                yarn
spark.eventLog.enabled      true
spark.eventLog.dir          hdfs://master1:9000/sparklogs
spark.eventLog.compress     true
spark.yarn.historyServer.address master1:18080
spark.eventLog.compress     false
spark.serializer            org.apache.spark.serializer.KryoSerializer
spark.driver.memory         5g
spark.executor.memory       20g
spark.executor.instances    48
spark.default.parallelism   384
spark.executor.memoryOverhead 5g
spark.executor.heartbeatInterval 60s
#spark.network.timeout      3600s
spark.shuffle.compress      true
spark.shuffle.spill.compress true
spark.driver.extraClassPath /path/to/spark-rdma-for-spark-2.4.0-jar-with-dependencies.jar
spark.executor.extraClassPath /path/to/spark-rdma-for-spark-2.4.0-jar-with-dependencies.jar
spark.shuffle.manager org.apache.spark.shuffle.rdma.RdmaShuffleManager
spark.shuffle.rdma.recvQueueDepth 128
spark.executor.cores        4
```

 **说明** 将 `spark.shuffle.compress` 设置为 `false` 会得到更好的加速比。

- i. 按 *Esc* 键退出编辑模式, 输入 `:wq` 并按下 *Enter* 键, 保存并退出文件。

5. 依次运行以下命令, 生成数据。

```
cd /root/fk/ss/TPCx-HS-Runtime-Suite
spark-submit --class HSGen --properties-file spark-config.rdmanew.jverbs TPCx-HS-master_Spark.jar.2.4 60000000000 /user/root/TPCx-HS-benchmark/HSort-input
```

 **说明** `60000000000` 代表生成的数据量大小, 单位为KB, 请您根据实际集群规模调整。

6. 运行以下命令, 执行Benchmark测试。

```
spark-submit --class HSort --properties-file spark-config.rdmanew.jverbs TPCx-HS-master_Spark.jar.2.4 /user/root/TPCx-HS-benchmark/HSort-input /user/root/TPCx-HS-benchmark/HSort-output
```

当出现如下类似结果时，表示测试完成，您可以从测试结果中查看Spark集群处理负载的执行时间。

```

22/06/10 15:35:40 INFO scheduler.TaskSetManager: Finished task 371.0 in stage 1.0 (TID 755) in 31 ms on c7re4x004 (executor 1) (372/384)
22/06/10 15:35:40 INFO scheduler.TaskSetManager: Finished task 372.0 in stage 1.0 (TID 756) in 29 ms on c7re4x004 (executor 1) (373/384)
22/06/10 15:35:40 INFO scheduler.TaskSetManager: Finished task 376.0 in stage 1.0 (TID 760) in 23 ms on c7re4x004 (executor 1) (374/384)
22/06/10 15:35:40 INFO scheduler.TaskSetManager: Finished task 374.0 in stage 1.0 (TID 758) in 27 ms on c7re4x004 (executor 1) (375/384)
22/06/10 15:35:40 INFO scheduler.TaskSetManager: Finished task 373.0 in stage 1.0 (TID 757) in 31 ms on c7re4x004 (executor 1) (376/384)
22/06/10 15:35:40 INFO scheduler.TaskSetManager: Finished task 377.0 in stage 1.0 (TID 761) in 24 ms on c7re4x004 (executor 1) (377/384)
22/06/10 15:35:40 INFO scheduler.TaskSetManager: Finished task 375.0 in stage 1.0 (TID 759) in 29 ms on c7re4x004 (executor 1) (378/384)
22/06/10 15:35:40 INFO scheduler.TaskSetManager: Finished task 381.0 in stage 1.0 (TID 765) in 53 ms on c7re4x004 (executor 1) (379/384)
22/06/10 15:35:40 INFO scheduler.TaskSetManager: Finished task 380.0 in stage 1.0 (TID 764) in 55 ms on c7re4x004 (executor 1) (380/384)
22/06/10 15:35:40 INFO scheduler.TaskSetManager: Finished task 379.0 in stage 1.0 (TID 763) in 56 ms on c7re4x004 (executor 1) (381/384)
22/06/10 15:35:40 INFO scheduler.TaskSetManager: Finished task 382.0 in stage 1.0 (TID 766) in 55 ms on c7re4x004 (executor 1) (382/384)
22/06/10 15:35:40 INFO scheduler.TaskSetManager: Finished task 378.0 in stage 1.0 (TID 762) in 56 ms on c7re4x004 (executor 1) (383/384)
22/06/10 15:35:40 INFO scheduler.TaskSetManager: Finished task 383.0 in stage 1.0 (TID 767) in 53 ms on c7re4x004 (executor 1) (384/384)
22/06/10 15:35:40 INFO cluster.YarnScheduler: Removed TaskSet 1.0, whose tasks have all completed, from pool
22/06/10 15:35:40 INFO scheduler.DAGScheduler: ResultStage 1 (runJob at SparkHadoopWriter.scala:78) finished in 1.599 s
22/06/10 15:35:40 INFO scheduler.DAGScheduler: Job 0 finished: runJob at SparkHadoopWriter.scala:78, took 7.308027 s
22/06/10 15:35:40 INFO io.SparkHadoopWriter: Job job_20220610153533_0002 committed.
22/06/10 15:35:40 INFO server.AbstractConnector: Stopped Spark@1cfd3b14{HTTP/1.1,[http/1.1]}{192.168.145.101:4040}
22/06/10 15:35:40 INFO ui.SparkUI: Stopped Spark web UI at http://c7re4x001:4040
22/06/10 15:35:40 INFO cluster.YarnClientSchedulerBackend: Interrupting monitor thread
22/06/10 15:35:41 INFO cluster.YarnClientSchedulerBackend: Shutting down all executors
22/06/10 15:35:41 INFO cluster.YarnSchedulerBackend$YarnDriverEndpoint: Asking each executor to shut down
22/06/10 15:35:41 INFO cluster.SchedulerExtensionServices: Stopping SchedulerExtensionServices
(serviceOption=None,
services=List(),
started=false)
22/06/10 15:35:41 INFO cluster.YarnClientSchedulerBackend: Stopped
22/06/10 15:35:41 INFO spark.MapOutputTrackerMasterEndpoint: MapOutputTrackerMasterEndpoint stopped!
22/06/10 15:35:41 INFO memory.MemoryStore: MemoryStore cleared
22/06/10 15:35:41 INFO storage.BlockManager: BlockManager stopped
22/06/10 15:35:41 INFO storage.BlockManagerMaster: BlockManagerMaster stopped
22/06/10 15:35:41 INFO scheduler.OutputCommitCoordinator$OutputCommitCoordinatorEndpoint: OutputCommitCoordinator stopped!
22/06/10 15:35:41 INFO spark.SparkContext: Successfully stopped SparkContext
22/06/10 15:35:41 INFO util.ShutdownHookManager: Shutdown hook called
22/06/10 15:35:41 INFO util.ShutdownHookManager: Deleting directory /mnt/data/spark_tmp/spark-d363e35b-badc-43ba-9fa9-476a9301f65c
22/06/10 15:35:41 INFO util.ShutdownHookManager: Deleting directory /tmp/spark-87ef4db1-7c2f-4f23-b989-f27b9bd9ac28

```

后续步骤

您可以按照以上方法，依次登录集群的其他节点，测试Spark集群的性能。

8. 前缀列表

8.1. 前缀列表概述

前缀列表是一些网络前缀（即CIDR地址块）的集合，您可以在配置其他资源的网络规则时引用前缀列表。通过将一些常用的CIDR地址块加入前缀列表，可以避免您在配置网络规则时，为不同的CIDR地址块重复添加多条规则，提升运维效率。前缀列表目前支持在配置安全组规则时被引用。

前缀列表常见概念

概念	说明
最大条目容量	前缀列表中CIDR地址块数量的上限。条目由CIDR地址块和相关描述信息组成。
地址族	前缀列表条目的地址族，支持IPv4或IPv6。一个前缀列表中的条目，必须属于同一种地址族。
CIDR地址块	<p>CIDR（Classless Inter-Domain Routing）是互联网中一种新的寻址方式，与传统的A类、B类和C类寻址模式相比，CIDR在IP地址分配方面更为高效。CIDR采用斜线记法，表示为：IP地址/网络ID的位数。</p> <ul style="list-style-type: none"> 示例一：CIDR格式换算为IP地址网段 <p>例如10.0.0.0/8，换算为32位二进制地址： 00001010.00000000.00000000.00000000。其中/8表示8位网络ID，即32位二进制地址中前8位是固定不变的，对应网段为： 00001010.00000000.00000000.00000000~00001010.11111111.11111111.11111111。则换算为十进制后，10.0.0.0/8表示：子网掩码为255.0.0.0，对应网段为10.0.0.0~10.255.255.255。</p> 示例二：IP地址网段换算为CIDR格式 <p>例如192.168.0.0~192.168.31.255，后两段IP换算为二进制地址： 00000000.00000000~00011111.11111111，可以得出前19位（$8*2+3$）是固定不变的，则换算为CIDR格式后，表示为：192.168.0.0/19。</p>
关联资源	引用前缀列表的其他资源。

使用限制

限制项	限制	提升额度方式
一个账号在每个地域的前缀列表数量上限	100	无
一个前缀列表中设置的条目数量上限	200	无
一个前缀列表的关联资源数量上限	1000	无

应用场景

您在前缀列表中维护CIDR地址块，在其他资源的规则中引用前缀列表。如果在前缀列表中修改条目信息，将直接在对应该规则上生效，避免多处维护，提高运维效率。

例如在添加安全组规则时，您可以引用前缀列表，此时这条规则对前缀列表中所有的CIDR地址块都生效。

8.2. 创建前缀列表

前缀列表是一些网络前缀（即CIDR地址块）的集合，您可以在配置其他资源的网络规则时引用前缀列表。本文介绍如何新建一个前缀列表。

前提条件

如果您使用RAM用户，请为RAM用户添加前缀列表相关权限。具体操作，请参见[为RAM用户授予前缀列表相关权限](#)。

操作步骤

1. 登录[ECS管理控制台](#)。
2. 在左侧导航栏，选择网络与安全 > 前缀列表。
3. 在顶部菜单栏左上角处，选择地域。
4. 单击创建前缀列表。
5. 在创建前缀列表对话框中，设置前缀列表参数。

创建前缀列表

* 名称: test

描述:

* 地址族: IPv4 IPv6 创建后将无法修改。

* 最大条目容量: 10 条 前缀列表支持的最大条目容量限制1-200条，创建后将无法修改。

前缀列表条目 + 增加条目

CIDR地址块	描述	操作
192.168.0.0/24	测试环境-应用	删除
192.168.1.0/24	测试环境-数据库	删除
192.168.2.100	堡垒机	删除

创建 取消

参数	描述
名称	设置前缀列表的名称。
描述	设置前缀列表的描述信息，建议填写前缀列表的使用用途等信息。
地址族	选择IPv4或者IPv6地址族，创建后不可更改。 <ul style="list-style-type: none"> ◦ 如果选择IPv4地址族，在前缀列表条目中只能设置IPv4的CIDR地址块。 ◦ 如果选择IPv6地址族，在前缀列表条目中只能设置IPv6的CIDR地址块。
最大条目容量	设置前缀列表的最大条目容量，创建后不可更改。 取值范围：1~200

参数	描述
前缀列表条目	<p>设置前缀列表的CIDR地址块信息。您可以单击增加条目新增CIDR地址块和描述信息。</p> <p>前缀列表条目的约束如下：</p> <ul style="list-style-type: none"> 总条目数量不能超过最大条目容量。 支持批量输入多个CIDR地址块，每个CIDR地址块之间以空格或半角逗号(,)分隔。 条目中的CIDR地址块类型根据地址族决定，一个前缀列表不能同时包含IPv4和IPv6的CIDR地址块。 条目中的CIDR地址块不能重复。例如，您不能设置两个192.168.1.0/24。 支持设置IP地址，系统会自动转换为CIDR地址块的形式。 例如，当您设置192.168.1.100时，系统会自动转换成192.168.1.100/32。 设置IPv6 CIDR地址块时，系统会自动转换成零压缩表示形式。 例如，您设置2001:0DB8:0000:0000:0000:0000:0000/32，系统会自动转换成2001:db8::/32。

6. 单击创建。

后续步骤

创建前缀列表后，您可以进行以下操作：

- 维护前缀列表，如果需要变更前缀列表名称、前缀列表条目等信息，请参见[管理前缀列表条目](#)。
- 引用前缀列表，如果需要在安全组规则中引用前缀列表，请参见[添加安全组规则](#)。

相关文档

- [CreatePrefixList](#)

8.3. 克隆前缀列表

当需要在多个地域创建相同的前缀列表时，您可以使用克隆前缀列表功能，快速地在多个地域创建相同的前缀列表。

前提条件

如果您使用RAM用户，请为RAM用户添加前缀列表相关权限。具体操作，请参见[为RAM用户授予前缀列表相关权限](#)。

操作步骤

- 登录[ECS管理控制台](#)。
- 在左侧导航栏，选择网络与安全 > 前缀列表。
- 在顶部菜单栏左上角处，选择地域。
- 在前缀列表页面，找到目标前缀列表，在操作列单击克隆。
- 在克隆前缀列表对话框中，修改地域、名称和描述信息。
- 单击克隆。
克隆完成后，您可以切换到目标地域查看克隆后的前缀列表。

8.4. 管理前缀列表条目

条目由CIDR地址块和描述构成，您可以在前缀列表详情页中新增、修改或删除条目。

前提条件

如果您使用RAM用户，请为RAM用户添加前缀列表相关权限。具体操作，请参见[为RAM用户授予前缀列表相关权限](#)。

新增前缀列表的条目

在前缀列表的详情页，您可以新增前缀列表的条目。

1. 登录[ECS管理控制台](#)。
2. 在左侧导航栏，选择网络与安全 > 前缀列表。
3. 在顶部菜单栏左上角处，选择地域。
4. 在前缀列表页面，找到目标前缀列表，单击前缀列表的ID。
5. 在前缀列表详情页，新增条目。

- i. 单击新增。
- ii. 在条目输入框中添加CIDR地址块和描述信息。

前缀列表条目的约束如下：

- 总条目数量不能超过最大条目容量。
- 支持批量输入多个CIDR地址块，每个CIDR地址块之间以空格或半角逗号（,）分隔。
- 条目中的CIDR地址块类型根据地址族决定，一个前缀列表不能同时包含IPv4和IPv6的CIDR地址块。
- 条目中的CIDR地址块不能重复。例如，您不能设置两个192.168.1.0/24。
- 支持设置IP地址，系统会自动转换为CIDR地址块的形式。

例如，当您设置192.168.1.100时，系统会自动转换成192.168.1.100/32。

- 设置IPv6 CIDR地址块时，系统会自动转换成零压缩表示形式。

例如，您设置2001:0DB8:0000:0000:0000:0000:0000/32，系统会自动转换成2001:db8::/32。

- iii. 单击保存。

如果需要添加多个条目，请重复以上步骤。

修改前缀列表的条目

在前缀列表的详情页，您可以修改前缀列表的条目。

1. 在左侧导航栏，选择网络与安全 > 前缀列表。
2. 在顶部菜单栏左上角处，选择地域。
3. 在前缀列表页面，找到目标前缀列表，单击前缀列表的ID。
4. 在前缀列表详情页，找到目标条目，单击编辑。
5. 修改条目的CIDR地址块和描述信息。

前缀列表条目的限制如下：

- 支持批量输入多个CIDR地址块，每个CIDR地址块之间以空格或半角逗号（,）分隔。
- 条目中的CIDR地址块类型根据地址族决定，一个前缀列表不能同时包含IPv4和IPv6的CIDR地址块。
- 条目中的CIDR地址块不能重复。例如，您不能设置两个192.168.1.0/24。
- 支持设置IP地址，系统会自动转换为CIDR地址块的形式。

例如，当您设置192.168.1.100时，系统会自动转换成192.168.1.100/32。

- 设置IPv6 CIDR地址块时，系统会自动转换成零压缩表示形式。

例如，您设置2001:0DB8:0000:0000:0000:0000:0000/32，系统会自动转换成2001:db8::/32。

6. 单击保存。

删除前缀列表的条目

在前缀列表的详情页，您可以删除前缀列表的条目。

1. 在左侧导航栏，选择网络与安全 > 前缀列表。
2. 在顶部菜单栏左上角处，选择地域。
3. 在前缀列表页面，找到目标前缀列表，单击前缀列表的ID。
4. 在前缀列表详情页，找到目标条目，删除单个条目或批量删除多个条目。
 - 删除单个条目：在目标条目的操作列，单击删除。
 - 批量删除条目：选中多个目标条目，单击底部的删除。

相关文档

- [ModifyPrefixList](#)

8.5. 删除前缀列表

如果您不再使用某些前缀列表，可以对其进行删除。

前提条件

- 前缀列表无关联资源。如果前缀列表已经被其他资源引用，则不能直接删除前缀列表。您需要在其他资源的配置页面中，解除对该前缀列表的引用，再删除前缀列表。
- 如果您使用RAM用户，请为RAM用户添加前缀列表相关权限。具体操作，请参见[为RAM用户授予前缀列表相关权限](#)。

操作步骤

1. 登录[ECS管理控制台](#)。
2. 在左侧导航栏，选择网络与安全 > 前缀列表。
3. 在顶部菜单栏左上角处，选择地域。
4. 在前缀列表页面，找到目标前缀列表并删除。
 - 删除单个前缀列表：在目标前缀列表的操作列，单击删除。
 - 批量删除前缀列表：选中多个目标前缀列表，单击底部的批量删除。

相关文档

- [DeletePrefixList](#)

8.6. 为RAM用户授予前缀列表相关权限

通过RAM用户可以让您避免与其他用户共享阿里云账号密钥，按需为用户分配最小权限，从而降低企业的信息安全风险。本文介绍如何为RAM用户授予前缀列表相关权限。

背景信息

本文仅介绍为RAM用户授予前缀列表相关权限，如果您需要在控制台使用其他资源，还需要为RAM用户设置对应的权限策略，例如系统策略中的AliyunECSReadOnlyAccess（只读访问云服务器服务（ECS）的权限）等。

操作步骤

1. 使用阿里云账号登录[RAM控制台](#)。

2. 创建前缀列表相关权限策略。具体操作，请参见[创建自定义权限策略](#)。

* 策略名称

备注

配置模式

可视化配置

脚本配置

策略内容

```
1 {
2   "Statement": [
3     {
4       "Action": [
5         "ecs:CreatePrefixList",
6         "ecs:ModifyPrefixList",
7         "ecs:DescribePrefixLists",
8         "ecs:DescribePrefixListAssociations",
9         "ecs:DescribePrefixListAttributes",
10        "ecs>DeletePrefixList"
11      ],
12      "Resource": "*",
13      "Effect": "Allow"
14    }
15  ],
```

确定 返回

创建一个PrefixListPolicy权限策略，策略内容如下所示。

```
{
  "Statement": [
    {
      "Action": [
        "ecs:CreatePrefixList",
        "ecs:ModifyPrefixList",
        "ecs:DescribePrefixLists",
        "ecs:DescribePrefixListAssociations",
        "ecs:DescribePrefixListAttributes",
        "ecs>DeletePrefixList"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }
  ],
  "Version": "1"
}
```

 **说明** 此处仅提供前缀列表的相关鉴权规则，更多ECS相关的鉴权规则，请参见[鉴权规则](#)。

3. 为RAM用户设置前缀列表相关权限。具体操作，请参见[为RAM用户授权](#)。

* 授权范围

云账号全部资源

指定资源组

请选择或输入资源组名称进行搜索

* 被授权主体

com X

* 选择权限

系统策略 自定义策略 + 新建权限策略

Prefix

权限策略名称	备注
PrefixListPolicy	

已选择 (2) 清空

- PrefixListPolicy X
- AliyunECSReadOnlyAccess X

确定 取消

设置完成后，您可以通过RAM用户管理前缀列表。

8.7. 使用前缀列表提高安全组规则管理的效率

本文介绍如何使用前缀列表，来更高效地进行安全组规则的管理。

背景信息

前缀列表是一些网络前缀（即CIDR地址块）的集合，您可以在配置安全组规则时引用前缀列表。对前缀列表条目的修改，等效于直接修改安全组规则。通过将一些常用地址放入前缀列表，可以避免您维护仅有授权对象不同的多条安全组规则，来降低您管理安全组规则的工作量。关于前缀列表的更多介绍，请参见[前缀列表概述](#)。

应用场景

为了云上资源的安全，您为购买的云上资源划分了多个安全域，每个安全域对应一个安全组。您多个安全域中的资源，需要被另外一个公共资源（例如云下的办公网络）访问，这个公共资源的网络地址段数量众多，且会经常发生变动。

在不使用前缀列表的情况下，您需要在多个安全组中维护仅有授权对象不同的多条安全组规则。在授权公共资源的网络地址发生变动时，您需要对多个安全域的安全组进行规则调整，安全组和网络地址数量越多，管理的工作量越大。

使用前缀列表后，您可以将公共资源的若干网络地址放入前缀列表，并在配置安全组规则时将授权对象设置为该前缀列表。在网络地址发生变动时，您只需要修改前缀列表中的网络地址，即可等效于修改已关联安全组的访问控制规则，无需再关注每个安全组中的规则，降低管理复杂度，提高效率。

当您的云上资源分布在多个阿里云地域时，您可以使用前缀列表克隆功能，来将一个已有的前缀列表克隆到其他地域。

操作步骤

本步骤以修改放行2个IP为例，为您演示通过前缀列表指定允许远程连接实例的IP，并在初次设置完成后修改远程连接授权的整个操作流程。

 **说明** 如果通过RAM用户操作，请为RAM用户添加前缀列表相关权限。具体操作，请参见[为RAM用户授予前缀列表相关权限](#)。

1. 登录[ECS管理控制台](#)。
2. 创建前缀列表。
 - i. 在左侧导航栏，选择**网络与安全 > 前缀列表**。
 - ii. 在顶部菜单栏左上角处，选择地域。
 - iii. 单击**创建前缀列表**。
 - iv. 在**创建前缀列表**对话框中，设置前缀列表的参数，单击**创建**。

本文以包括2个IPv4条目为例，参数示例如下所示：

- 名称：RemoteLogon
- 描述：允许该前缀列表中的IP远程连接安全组的实例
- 地址族：IPv4
- 最大条目容量：2条

 **说明** 已关联资源（例如安全组）计算规则配额时，将使用最大条目容量计算，而非实际条目数，请合理设置。

- 前缀列表条目：单击**增加条目**，分别添加 `192.168.1.0/24`、`192.168.2.0/24`。

由于采用了CIDR地址块的形式，上述条目实际对应了多个IP：

- `192.168.1.0/24`：即 `192.168.1.0` ~ `192.168.1.255`。
- `192.168.2.0/24`：即 `192.168.2.0` ~ `192.168.2.255`。

3. 在安全组规则中使用前缀列表。

重复以下步骤为多个安全组添加安全组规则，放行对远程连接端口的访问，并将前缀列表RemoteLogon作为授权对象。

- i. 在左侧导航栏，选择**网络与安全 > 安全组**。
- ii. 找到目标安全组，在操作列单击**配置规则**。
- iii. 在入方向页签中，单击**手动添加**。

 **说明** 本文以专有网络安全组的操作为例，如果为经典网络安全组，请根据是否为公网IP选择对应的页签。

iv. 设置安全组规则的参数，然后单击**保存**。

本文以允许通过SSH和RDP方式远程连接安全组内实例为例，参数示例如下表所示：

- 授权策略：**允许**
- 优先级：**1**
- 协议类型：**自定义TCP**
- 端口范围：**选择SSH (22)和RDP (3389)**
- 授权对象：**选择前缀列表RemoteLogon**

添加该安全组规则后，安全组放行前缀列表中的IP远程连接安全组内实例。

4. 修改前缀列表的条目。

如果在添加安全组规则后，您需要取消一些IP的远程连接授权，进一步缩小授权范围以降低风险，则无需逐一修改多个安全组的安全组规则，修改前缀列表RemoteLogon的条目即可。例如，您使用私有IP为 192.168.1.1、192.168.2.1 的实例作为跳板机，需要限制仅允许通过跳板机远程连接安全组内实例，则按以下步骤修改前缀列表的条目。

- i. 在左侧导航栏，选择**网络与安全 > 前缀列表**。
- ii. 找到前缀列表RemoteLogon，在**操作列**单击**详情**。
- iii. 单击**前缀列表条目**页签。
- iv. 找到前缀列表条目，在**操作列**单击**编辑**。
- v. 设置CIDR地址块参数，然后单击**保存**。

修改2个已有条目，CIDR地址块参数分别设置为 192.168.1.1/32 、 192.168.2.1/32 。

修改前缀列表的条目后即时生效，使用前缀列表RemoteLogon的安全组规则也随之变化，安全组仅放行 192.168.1.1/32 、 192.168.2.1/32 远程连接安全组内实例。

更多操作场景

本章节通过对比多个场景中的操作次数，体现前缀列表在提升效率上的优势。假设您管理50个安全组中的资源，下表列出了使用前缀列表前后的操作次数。

场景	安全组规则中指定固定IP	安全组规则中指定一个前缀列表
停止放行5个IP	分别为50个安全组删除5条安全组规则，操作250次。即使批量删除，也需要操作50次。	为前缀列表删除5个条目，操作5次。如果批量删除，操作1次即可。
修改放行5个IP	分别为50个安全组修改5条安全组规则，操作250次。	为前缀列表修改5个条目，操作5次。
新增放行5个IP	分别为50个安全组新增5条安全组规则，操作250次。即使批量新增，也需要操作50次。	为前缀列表新增5个条目，操作5次。如果批量新增，操作1次即可。
修改放行5个IP，并新增放行5个IP	分别为50个安全组修改5条安全组规则，并新增5条安全组规则，总计操作500次。即使批量新增，总计也需要操作300次。	为前缀列表修改5个条目，并新增5个条目，总计操作10次。如果批量新增，总计操作6次即可。

9. 更换ECS实例的VPC

本章节介绍VPC网络类型的ECS实例如何更换到其他VPC。如果您在创建ECS实例时选错VPC或者需要重新规划网络，可以通过此功能更换单个或多个ECS实例的VPC。

前提条件

- ECS实例已处于停止状态。如何停止ECS实例，请参见[停止实例](#)。

 **说明** 对于创建后未重启过的ECS实例，您需要先重启实例，再停止实例。

- ECS实例未加入SLB的后端服务器。SLB中如何移除后端服务器，请参见[移除后端服务器](#)。
- ECS实例已卸载弹性网卡和多IP。如何卸载弹性网卡和多IP，请参见[解绑弹性网卡](#)和[回收辅助私网IP地址](#)。
- 已准备好更换的目标VPC、交换机和安全组。

使用场景

- 前期VPC规划不合理，随着业务的逐渐扩大，原来的VPC不能满足需求，需要通过ECS实例更换VPC操作进行重新规划。
- 前期只规划一个VPC，不同的项目和使用环境共用此VPC，存在数据操作风险。现在希望按项目、使用环境划分为单独的VPC，需要通过ECS实例更换VPC操作进行项目迁移。
- 希望跨账号VPC互联，但ECS实例在不同账号的默认VPC中，由于地址冲突无法建立跨账号互联。此时需要ECS实例更换VPC，解决地址冲突问题后，才能跨账号VPC互联。

使用限制

- 实例不能在其它云服务中被使用。例如，实例不能在迁移中、不能已在更换VPC或实例内部署的数据库不能被DTS服务管理等。
- ECS实例变更前后的交换机必须在同一可用区。
- ECS实例变更可选择1~5个目标安全组，但目标安全组类型必须一致（都是普通安全组或都是企业安全组）。
- 如果目标VPC开启了高级网络特性，则部分ECS实例规格族不支持更换。不支持的ECS实例规格族请参见[不支持VPC高阶特性的实例规格族](#)。
- 批量更换ECS实例的VPC时，单次最多支持20个ECS实例。
- 更换ECS实例的VPC后，此ECS实例无法直接和原有VPC内的其他ECS实例互通。如果需要实现互通，请参见[什么是高速通道](#)。
- 不支持配置了EIP网卡可见模式或多EIP网卡可见模式的实例。
- 不支持绑定高可用虚拟IP（HaVip）的实例。
- 不支持交换机绑定了自定义路由表的实例。
- 不支持开通了全球加速（GA）的实例。
- 不支持绑定辅助网卡的实例。
- 不支持已分配IPv6地址的实例。
- 不支持主网卡有多IP的实例。

操作步骤

1. 登录[ECS管理控制台](#)。
2. 在左侧导航栏，选择实例与镜像 > 实例。
3. 在顶部菜单栏左上角处，选择地域。
4. 单个或批量更换ECS实例的VPC。
 - 更换单个ECS实例的VPC

找到目标ECS实例，在操作列中单击**更多 > 网络和安全组 > 更换专有网络**。

o 批量更换多个ECS实例的VPC

选中多个目标ECS实例，单击底部的**更多 > 网络和安全组 > 更换专有网络**。

5. 在**更换专有网络配置向导**页面，按照指引更换ECS实例的专有网络。

实例名称/实例Id	可用区	专有网络Id	主私网IP
-/i-t	华东 1 可用区 I	vpc-bj	

- i. 在**变更准备**阶段，查看变更前的网络信息和注意事项，单击**下一步**。
- ii. 在**选择专有网络**阶段，选择ECS需要切换的目标**专有网络**、**目标交换机**和**目标安全组**，单击**下一步**。
- iii. （可选）在**配置主私网IP**阶段，设置ECS切换后的**主私网IP**地址。
 - 设置的主私网IP需要在目标交换机的网段内。
 - 如果您不手动设置主私网IP，则主私网IP由系统自动分配。
- iv. 单击**确定**。

切换完成后，您可以单击ECS实例ID，在**实例详情**页面的**网络信息**中查看切换后的**专用网络**和**虚拟交换机**。

相关文档

- [ModifyInstanceVpcAttribute](#)

10. 配置网卡多队列

网卡多队列指实例规格支持的最大网卡队列数。单台ECS实例vCPU处理网络中断存在性能瓶颈时，您可以将实例中的网络中断分散给不同的vCPU处理，从而提升性能。

前提条件

操作前请确认以下信息：

- 确认您的实例规格支持网卡多队列功能。支持多队列的实例规格请参见[实例规格族](#)，多队列数值大于1时，表示支持网卡多队列。

说明 在使用持久内存型实例规格族re6p的ECS实例中，如果存在网络中断没有分散给不同的vCPU处理的情况，建议您升级最新的 `ecs_mq` 配置脚本。

- 确认您的镜像支持网卡多队列且默认未开启。阿里云提供的以下公共镜像支持网卡多队列，镜像是否支持网卡多队列与操作系统的位数无关。

说明

- 即使您使用的是列表中提及的操作系统，但因系统更新的原因，部分早期上架的公共镜像可能不支持网卡多队列。建议您使用最新的公共镜像。如果您使用的镜像已默认开启网卡多队列功能，请跳过此章节内容。
- 本文操作仅适用于Linux系统的ECS实例。Windows 2012及以上操作系统的ECS实例会自动配置网卡多队列，您无需配置。

公共镜像	是否支持多队列	是否默认开启多队列
CentOS 6.8/6.9/7.2/7.3/7.4/8.*	是	是
Ubuntu 14.04/16.04/18.04/20.04	是	是
Debian 8.9/9.2/10.*	是	是
SUSE Linux Enterprise Server 12 SP1/12 SP2/15 SP1/15 SP2	是	是
Red Hat Enterprise Linux 6.9/7.4/7.5	是	否
OpenSUSE 42.3/15.*	是	否
Alibaba Cloud Linux 2.1903	是	是
Windows 2012及以上	是	是

背景信息

网卡多队列是一种技术手段，可以解决网络I/O带宽QoS（Quality of Service）问题。网卡多队列驱动将各个队列通过中断绑定到不同的核上，从而解决网络I/O带宽升高时单核CPU的处理瓶颈，提升网络PPS和带宽性能。经测试，在相同的网络PPS和网络带宽的条件下，与1个队列相比，2个队列最多可提升性能达50%到100%，4个队列的性能提升更大。

自动配置

1. 远程连接ECS实例。

关于连接方式的介绍，请参见[连接方式概述ECS远程连接操作指南](#)。

2. 下载自动配置脚本 `ecs_mq` 。

```
wget https://ecs-image-tools.oss-cn-hangzhou.aliyuncs.com/ecs_mq/ecs_mq_latest.tgz
```

3. 解压脚本。

```
tar -xzf ecs_mq_latest.tgz
```

4. 更换工作路径。

```
cd ecs_mq/
```

5. 运行脚本。

不同的镜像版本的命令格式不同，例如CentOS 7.6镜像运行 `bash install.sh centos 7` 。

```
bash install.sh <系统名称> <系统主版本号>
```

6. 启动服务。

```
systemctl start ecs_mq
```

手动配置

本节以CentOS 7.6镜像为例，假设ECS实例主网卡名称为eth0，辅助弹性网卡名称为eth1，介绍如何手动配置网卡多队列。

1. 运行 `ethtool -l eth0` 命令查看主网卡支持多队列的情况。

```
[root@localhost ~]# ethtool -l eth0
Channel parameters for eth0:
Pre-set maximums:
RX: 0
TX: 0
Other: 0
Combined: 2 # 表示最多支持设置2个队列
Current hardware settings:
RX: 0
TX: 0
Other: 0
Combined: 1 # 表示当前生效的是1个队列
```

 **说明** 如果返回信息中，两个Combined字段取值相同，则表示弹性网卡已开启支持多队列。

2. 运行 `ethtool -L eth0 combined 2` 命令开启网卡的多队列功能。

此命令作用是设置主网卡eth0使用两个队列。

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

3. 设置辅助网卡的多队列。

```
# 查看辅助网卡eth1支持多队列的情况
[root@localhost ~]# ethtool -l eth1
Channel parameters for eth1:
Pre-set maximums:
RX: 0
TX: 0
Other: 0
Combined: 4 # 表示最多支持设置4个队列
Current hardware settings:
RX: 0
TX: 0
Other: 0
Combined: 1 # 表示当前生效的是1个队列
# 设置辅助网卡eth1使用4个队列
[root@localhost ~]# ethtool -L eth1 combined 4
```

11. 设置网卡MTU值

最大传输单元MTU（Maximum Transmission Unit）决定了单次可传输数据包的最大尺寸，本文介绍如何使用ecs-utls-jumboframe脚本为ECS实例的网卡设置MTU值。

背景信息

建议将网络MTU值与本地MTU值设置为一致，可以充分利用单次传输数据包大小的上限，同时避免因数据包过大而必须拆分数数据包导致的额外时间消耗。

 **注意** ecs-utls-jumboframe脚本中没有直接调用重启网卡或者网络服务的指令，但不同系统中可能使用不同类型的网络服务和网卡驱动，不能完全排除出现瞬时网络断流的可能。如果您的业务严格要求实时网络不能中断，请参考脚本内容慎重评估后再决定是否使用。

使用限制

- 仅VPC实例支持使用ecs-utls-jumboframe脚本，且ecs-utls-jumboframe脚本依赖实例元数据服务检测实例规格是否支持Jumbo Frame特性。使用该脚本前请勿禁用网络和实例元数据服务相关端口（100.100.100.200:80）。
- 目前仅7代及之后的实例支持Jumbo Frame特性，允许设置的网卡MTU值上限为8500。ecs-utls-jumboframe脚本会根据实例规格判断允许设置的MTU值上限，您也可以使用该脚本为其它实例规格设置网卡MTU值，但上限为1500。
- Jumbo Frame特性仅限同VPC内7代及之后的实例之间使用TCP协议直接通信的场景，不支持经过SLB等其他中间节点。

在Linux实例中设置网卡MTU值

确保Linux实例的镜像为以下版本之一：

- CentOS 6.x、CentOS 7.x、CentOS 8.x
- Debian 9.x、Debian 10.x
- SUSE Linux Enterprise Server 15
- Ubuntu 16.x、18.x、20.x

1. [远程连接ECS实例](#)。
2. 下载ecs-utls-jumboframe-linux.sh脚本。

```
wget https://ecs-image-tools.oss-cn-hangzhou.aliyuncs.com/jumboframe/ecs-utls-jumboframe-linux.sh
```

3. 赋予脚本可执行权限。

```
chmod +x ./ecs-utls-jumboframe-linux.sh
```

您可以执行 `./ecs-utls-jumboframe-linux.sh -h` 查看帮助信息。

```
[root@i-xxxxx ~]# chmod +x ./ecs-utls-jumboframe-linux.sh
[root@i-xxxxx ~]# ./ecs-utls-jumboframe-linux.sh -h
Usage: ecs-utls-jumboframe-linux.sh [-h] [-p] IFNAME MTU
-h          Print this help.
-p          Also configure new MTU value persistently.
```

4. 查看系统网卡设备列表和网卡的当前MTU值。

```
ip addr show
```

```
[root@i~]# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 
   inet  scope host lo
       valid_lft forever preferred_lft forever
   inet6  scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
   link/ether 
   inet 1  scope global dynamic eth0
       valid_lft 315359892sec preferred_lft 315359892sec
   inet6  scope link
       valid_lft forever preferred_lft forever
```

5. 设置网卡MTU值。

- 临时设置MTU值：如果您需要临时测试Jumbo Frame特性，可以临时设置网卡MTU值，重启ECS实例后网卡MTU值会恢复默认设置。格式如下：

```
./ecs-utils-jumboframe-linux.sh <网卡> <目标MTU值>
```

例如，将eth0网卡的MTU值临时设置为8500：

```
./ecs-utils-jumboframe-linux.sh eth0 8500
```

- 永久设置MTU值：如果您需要永久启用Jumbo Frame特性，在设置网卡MTU值时指定模式即可。永久设置完成后，重启ECS实例后网卡MTU值仍保持您设置的值。格式如下：

```
./ecs-utils-jumboframe-linux.sh -p <网卡> <目标MTU值>
```

例如，将eth0网卡的MTU值永久设置为8500：

```
./ecs-utils-jumboframe-linux.sh -p eth0 8500
```

设置完成后，您可以执行 `ip addr show` 查看网卡信息，eth0网卡的MTU值已变为8500。

```
[root@iz~]# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 
   inet  scope host lo
       valid_lft forever preferred_lft forever
   inet6  scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 8500 qdisc mq state UP group default qlen 1000
   link/ether 
   inet 1  scope global dynamic eth0
       valid_lft 315359722sec preferred_lft 315359722sec
   inet6  scope link
       valid_lft forever preferred_lft forever
```

在Windows实例中设置网卡MTU值

确保Windows实例满足以下要求：

- 镜像为Windows Server 2012或以上版本。
- 已安装PowerShell。
 - 远程连接ECS实例。
 - 下载 `ecs-utils-jumboframe-windows.ps1` 脚本。
在浏览器中访问 [下载链接](#) 即可。
 - 打开PowerShell。
 - 切换至脚本所在目录。
以脚本位于桌面为例：

```
cd C:\Users\Administrator\Desktop
```

您可以执行 `Get-Help .\ecs-utils-jumboframe-windows.ps1` 查看帮助信息。

```
PS C:\Users\Administrator\Desktop> Get-Help .\ecs-utils-jumboframe-windows.ps1
名称
C:\Users\Administrator\Desktop\ecs-utils-jumboframe-windows.ps1
摘要
Configure network adapter MTU to enable Jumbo Frame feature on ECSv7 instances.
语法
C:\Users\Administrator\Desktop\ecs-utils-jumboframe-windows.ps1 [-NetworkAdapter] <String> [-NewMTUValue] <Int32> []
说明
The ecs-jumboframe-tool-win.ps1 script configures the MTU limitation of network
adapter. Setting it between 1500 and 8500 can enable Jumbo Frame feature on
ECSv7 instances.
相关链接
备注
若要查看示例, 请键入: "get-help C:\Users\Administrator\Desktop\ecs-utils-jumboframe-windows.ps1 -examples"
有关详细信息, 请键入: "get-help C:\Users\Administrator\Desktop\ecs-utils-jumboframe-windows.ps1 -detailed"
若要获取技术信息, 请键入: "get-help C:\Users\Administrator\Desktop\ecs-utils-jumboframe-windows.ps1 -full".
```

5. 查看系统网卡设备列表。

```
Get-NetAdapter
```

```
PS C:\Users\Administrator\Desktop> Get-NetAdapter
```

Name	InterfaceDescription	ifIndex	Status	MacAddress	LinkSpeed
以太网	Red Hat VirtIO Ethernet Adapter	3	Up	08-00-27-00-00-00	10 Gbps

6. 设置网卡MTU值。

 **说明** Windows实例中仅支持永久设置MTU值。永久设置后, 重启ECS实例后网卡MTU值仍保持您设置的值。

格式如下:

```
.\ecs-utils-jumboframe-windows.ps1 -NetworkAdapter <"网卡名称"> -NewMTUValue <目标MTU值>
```

例如, 将以太网网卡的MTU值设置为8500:

```
.\ecs-utils-jumboframe-windows.ps1 -NetworkAdapter "以太网" -NewMTUValue 8500
```

设置完成后, 您可以执行 `Get-NetAdapterAdvancedProperty -Name "以太网" -RegistryKeyword "MTU"` 查看以太网网卡的MTU信息, MTU值已变为8500。

```
PS C:\Users\Administrator\Desktop> Get-NetAdapterAdvancedProperty -Name "以太网" -RegistryKeyword "MTU"
```

Name	DisplayName	DisplayValue	RegistryKeyword	RegistryValue
以太网	Init.MTUSize	8500	MTU	{8500}

12.经典网络迁移到专有网络（新版）

12.1. ECS实例从经典网络迁移到专有网络

相比经典网络，专有网络（VPC）中的ECS实例更加安全并且支持更丰富的功能，例如支持绑定弹性公网IP（EIP）。本文介绍如何使用实例迁移计划功能将一台或多台ECS实例从经典网络迁移到专有网络。

前提条件

迁移前，请确保经典网络中的源ECS实例满足以下条件：

- 磁盘条件：ECS实例没有挂载本地盘。如果ECS实例挂载了本地盘，请[提交工单](#)咨询迁移方式。
- 带宽条件：ECS实例公网带宽大于0 Mbps。如果ECS实例分配了公网IP地址，但公网带宽为0 Mbps，需要先升级公网带宽。具体操作，请参见[修改公网带宽](#)。
- 地域条件：位于支持ECS实例迁移计划功能的地域，包括华北1（青岛）、华北2（北京）、华东1（杭州）、华东2（上海）、华南1（深圳）、中国（香港）、美国（硅谷）、新加坡。

 **说明** 华东1（杭州）地域可用区C中的部分ECS实例不支持迁移。

迁移影响

影响项目	说明
迁移时长	<p>从源ECS实例停机到迁移后的ECS实例启动，约耗时15分钟。</p> <p> 说明 迁移后的ECS实例启动，代表计算网络资源已迁移完成。如果跨可用区迁移，在ECS实例启动后还会继续迁移磁盘数据，通常情况下迁移100 GiB的磁盘数据耗时4小时左右，期间磁盘I/O性能会短暂下降，且暂时不支持快照和磁盘相关的操作。</p>
实例状态变化	迁移过程中会停止并重新启动ECS实例，建议您预约业务低谷的时间段进行迁移。
网络类型变化	从经典网络迁移至VPC。更多VPC的介绍，请参见 什么是专有网络 。
软件授权码变化	迁移后，软件授权码可能会发生变化。
IP地址	<ul style="list-style-type: none"> ● 公网IP保持不变。 <p> 注意 VPC中的ECS实例没有公网网卡，通过NAT方式访问公网，在ECS实例内只能查看到内网IP。如果应用依赖操作系统中可见的公网IP，请谨慎评估是否迁移。</p> <ul style="list-style-type: none"> ● 支持自定义是否保留内网IP。您也可以在迁移完成后自行修改内网IP，具体操作，请参见修改私有IP地址。
磁盘识别名称	<p>部分ECS实例会在迁移的同时升级底层虚拟化技术，可能导致磁盘识别名称会发生变化。在Linux实例中，磁盘会被识别为vda、vdb、vdc等名称。</p> <ul style="list-style-type: none"> ● 如果源ECS实例的磁盘识别名称已经是vda、vdb、vdc等，不会发生变化。 ● 如果源ECS实例的磁盘识别名称是xvda、xvdb、xvdc，迁移后会被识别为vda、vdb、vdc等。阿里云会为Linux实例自动修复/etc/fstab文件，但您仍需关注其他应用是否依赖旧的磁盘识别名称。

影响项目	说明
费用	<ul style="list-style-type: none">迁移本身不额外计费。包年包月ECS实例从新的计费周期（迁移完成）开始，实例规格的单价会发生变化，同等配置条件下VPC实例的费用低于经典网络实例。取消未生效和未支付的续费变配订单，您可以重新操作续费变配。
其他	<ul style="list-style-type: none">ECS实例的ID、用户名、登录密码不变。如果负载均衡SLB的虚拟服务器组（VServerGroup）中添加了源ECS实例，迁移后的ECS实例不会自动添加，您需要手动添加。具体操作，请参见编辑虚拟服务器组。

迁移准备工作

1. 为源ECS实例的磁盘创建快照并备份数据。
具体操作，请参见[创建一个云盘快照](#)。
2. （可选）如果源ECS实例关联了云数据库，需要提前将云数据库设置为混访模式。
混访模式的云数据库可以同时接受经典网络类型和VPC类型ECS实例的访问，更多信息，请参见[云数据库混访概述](#)。
3. （可选）如果源ECS实例关联了具有白名单功能的云数据库服务（例如云数据库RDS），需要提前将目标虚拟交换机的网段加入白名单。
具体操作，请参见[设置白名单](#)。
4. （可选）建议将应用服务设置为开机自启动，并做好可用性监控，方便在迁移后更快地恢复业务。
5. 关闭或卸载源ECS实例上的服务器安全软件。

 **说明** 迁移时会更新ECS实例的设备驱动，因此需要暂时关闭或卸载已安装的服务器安全软件，例如安全狗、护士神、云锁。

6. 对源ECS实例的系统盘，确保预留500 MiB以上的空间。
7. 对目标VPC的虚拟交换机，确保预留内网IP地址的数量不少于待迁移ECS实例的数量。

步骤一：创建迁移计划

1. 登录[ECS管理控制台](#)。
2. 在左侧导航栏，选择[运维与监控 > 实例迁移计划](#)。
3. 在顶部菜单栏左上角处，选择地域。
4. 单击[创建迁移计划](#)。
5. 在配置迁移计划页面，配置目标VPC、网络属性、网络连通性相关的信息，然后单击下一步。

i. 设置目标可用区与专有网络。

1 配置迁移计划

目标可用区与专有网络

请输入计划名称

默认迁移计划

选择目标可用区

杭州 可用区I 找不到可用区

选择迁移的目标专有网络，或先**创建专有网络**

(默认)系统自动创建专有网络 网段: 10.0.0.0/8 C

配置项	说明
请输入计划名称	自定义迁移计划名称。
选择目标可用区	<p>从下拉列表中选择迁移后ECS实例所属的目标可用区。可选的可用区由系统根据资源情况自动规划，如果您需要将源ECS实例迁移至指定的可用区，但下拉列表中没有该可用区，请提交工单咨询。</p> <div style="background-color: #e6f2ff; padding: 5px; border: 1px solid #d9e1f2;"> <p>说明 一个实例迁移计划仅支持选择一个目标可用区。如果您需要将多台源ECS实例分别迁移至多个目标可用区，请根据需要分别创建多个迁移计划。</p> </div>
选择迁移的目标专有网络	<p>从下拉列表中选择迁移后ECS实例所属的目标专有网络。目标专有网络的网段设置决定了能否保留源ECS实例的内网IP，如下所示：</p> <ul style="list-style-type: none"> ■ 如果需要保留源ECS实例的内网IP，必须选择网段为10.0.0.0/8的VPC。根据是否自行创建了此类VPC选择： <ul style="list-style-type: none"> ■ 如果您尚未创建网段为10.0.0.0/8的VPC，选择（默认）系统自动创建专有网络，网段：10.0.0.0/8即可，系统将自动创建网段为10.0.0.0/8的VPC。 ■ 如果您已经创建了网段为10.0.0.0/8的VPC，则选择该VPC。 ■ 如果无需保留源ECS实例的内网IP：根据自己的网络规划，选择网段不是10.0.0.0/8的其他VPC。

ii. 设置实例网络属性。

实例网络属性

* 目标安全组

(默认)克隆经典实例安全组 进一步了解克隆

指定安全组

* 优先保留 Mac 地址策略

(默认)私网 Mac

公网 Mac

配置项	说明
目标安全组	<p>选择迁移后ECS实例所属的安全组。</p> <ul style="list-style-type: none"> (默认) 克隆经典实例安全组：克隆源ECS实例所属的经典网络安全组，目标安全组的安全组规则和该经典网络安全组保持一致。 <p>如果您将选择迁移的目标专有网络设置为(默认)系统自动创建专有网络，网段：10.0.0.0/8，则仅支持选中该选项自动克隆经典网络安全组。</p> <div style="border: 1px solid #add8e6; padding: 5px; margin: 5px 0;"> <p>? 说明 不支持克隆存在组授权规则的安全组。</p> </div> <ul style="list-style-type: none"> 指定安全组：从下拉列表中选择您已经创建的安全组。 <div style="border: 1px solid #add8e6; padding: 5px; margin: 5px 0;"> <p>? 说明 如果该安全组的安全组规则设置不当，在迁移后会影响ECS实例的网络访问，请确保安全组规则设置符合您对网络访问的预期。</p> </div>
优先保留MAC地址策略	<p>在经典网络中，如果ECS实例分配了公网IP，会同时拥有公网MAC地址和私网MAC地址；在专有网络中，ECS实例则只拥有私网MAC地址，通过NAT方式映射实现访问公网。因此，您需要选择迁移后使用哪一个MAC地址，请根据业务系统需要选择保留私网MAC或公网MAC。</p> <ul style="list-style-type: none"> 如果业务系统绑定了MAC地址，例如业务系统中直接配置了MAC地址、部分软件采用绑定MAC地址的方式注册，请选择保留对应的MAC地址。 如果业务系统没有绑定MAC地址，则任选一项保留即可。

iii. 设置实例网络连通性。

实例网络连通性

* 保留实例内网 IP

(默认)是

创建虚拟交换机策略 自动 手动

系统将在目标专有网络里，根据经典实例的内网 IP 自动规划 16 网段的交换机，如因网段占用，交换机数量限制导致无法创建，请选择手动

否

* 已迁移实例和该计划内还未迁移的经典实例保持内网联通

(默认)否

是

配置项	说明
-----	----

配置项	说明
保留实例内网IP	<p>选择是否保留源ECS实例的内网IP地址。如果保留，需要设置如何创建虚拟交换机；如果不保留，需要选择已创建的虚拟交换机。</p> <ul style="list-style-type: none"> ■ 是：保留源ECS实例的内网IP地址。这时需要继续设置创建虚拟交换机策略： <ul style="list-style-type: none"> ■ 创建虚拟交换机策略为自动时，由系统根据内网IP地址自动创建网段符合要求的虚拟交换机。请确保对应的网段未被其他虚拟交换机占用，否则虚拟交换机会创建失败。 <p>说明 如果您将选择迁移的目标专有网络设置为（默认）系统自动创建专有网络，网段：10.0.0.0/8，则系统自动保留源ECS实例内网IP并自动创建虚拟交换机，创建虚拟交换机策略仅支持设置为自动。</p> ■ 创建虚拟交换机策略为手动时，您需要自行创建符合目标可用区、源ECS实例的内网IP地址要求的虚拟机交换机。 <p>说明 仅在选择迁移的目标专有网络设置为自行创建的网段为10.0.0.0/8的VPC时，才支持将创建虚拟交换机策略设置为手动。</p> <ul style="list-style-type: none"> ■ 否：不保留源ECS实例的内网IP地址，继续从下拉列表中选择您希望使用的虚拟交换机即可。 <p>说明 如果在下拉列表中找到您已经创建的虚拟交换机，可能原因是该虚拟交换机不在迁移ECS实例的目标可用区，请在目标可用区重新创建虚拟交换机。具体操作，请参见创建和管理交换机。</p>
已迁移实例和该计划内还未迁移的经典实例保持内网联通	<p>在迁移计划包括了多台ECS实例时，已迁移至VPC的ECS实例和经典网络中其他尚未迁移的源ECS实例是否保持内网联通，内网联通的设置方法由是否保留了源ECS实例的内网IP地址决定。</p> <ul style="list-style-type: none"> ■ 保留了源ECS实例的内网IP地址 <ul style="list-style-type: none"> ■ 无需内网联通：选择否。 ■ 需要内网联通：选择是，并在下一步选择待迁移实例页面中添加所有需要内网联通的源ECS实例（您可以分别设置迁移时间控制迁移顺序）。 <p>说明 未添加至迁移计划的源ECS实例将无法通过内网与迁移至VPC的ECS实例联通，且预约迁移后，将不能继续添加ECS实例或删除已添加的ECS实例。</p> ■ 不保留源ECS实例的内网IP地址 <ul style="list-style-type: none"> ■ 无需内网联通：无需额外配置，继续下一步操作即可。 ■ 需要内网联通：请在启动迁移前自行行为源ECS实例配置ClassicLink链接，具体操作，请参见经典网络和专有网络互通。

6. 在选择待迁移实例页面，添加待迁移的源ECS实例，然后单击下一步。

如果您将保留实例内网IP设置为是，并且需要已迁移至VPC的ECS实例和经典网络中其他尚未迁移的源ECS实例保持内网联通，必须添加所有需要内网联通的源ECS实例（您可以分别设置迁移时间控制迁移顺序）。

说明 未添加至迁移计划的源ECS实例将无法通过内网与迁移至VPC的实例联通，且预约迁移后，将不能继续添加ECS实例或删除已添加的ECS实例。

示例如下图所示，①为需要先迁移的ECS实例，②为需要后迁移的ECS实例。



7. 在预约迁移页面，设置迁移的时间，然后单击**创建验证**。

在迁移过程中需要停止并重新启动ECS实例，建议您预约业务低谷时间段。支持为各ECS实例分别设置迁移时间：

- 为单台ECS实例设置迁移时间：在该ECS实例的操作列，单击**预约迁移时间**进行配置。
- 为多台ECS实例批量设置迁移时间：选中多个实例，然后单击**批量预约迁移时间**进行配置。
- 为全量ECS实例设置统一的迁移时间：单击**设置统一迁移时间**进行配置。

注意

- 对需要暂时保留在经典网络并进行内网联通的ECS实例，请设置较晚的迁移时间，并且在迁移启动前再次评估是否需要将这些ECS实例也迁移到VPC。
- 可设置的迁移时间限制如下：
 - 不得早于当前时间。
 - 不得晚于ECS实例的到期时间。

另外创建迁移计划后，部分磁盘需要先进行三副本校验，校验时长取决于磁盘大小和校验队列排队情况，待校验完成后才开始迁移。请您根据系统提示设置预约迁移时间。

8. 在创建验证对话框，查看迁移注意事项，并验证迁移计划配置是否符合要求。

- 如果迁移计划配置符合要求：选中迁移提示信息，然后单击**确认并创建**。
- 如果迁移计划配置不符合要求：系统将提示错误信息，您可以根据错误信息定位问题，并重新创建迁移计划。

步骤二：完成迁移

迁移计划创建完成后，系统将在您预约的时间启动迁移，自动将ECS实例从经典网络迁移至VPC。



迁移过程如下：

1. 源ECS实例停机。
2. 迁移ECS实例的计算网络资源。
3. 迁移后的ECS实例启动。
4. 继续迁移磁盘数据。
5. 完成迁移。

说明 如果跨可用区迁移，在迁移完计算网络资源并启动ECS实例后，还会继续迁移磁盘数据。通常情况下迁移100 GiB的磁盘数据耗时4小时左右，期间磁盘I/O性能会短暂下降，且暂时不支持快照和磁盘相关的操作。

步骤三：检查迁移结果

1. 在左侧导航栏，选择实例与镜像 > 实例。
2. 找到已迁移的ECS实例，单击实例ID。
3. 在实例详情页面，查看实例的网络类型。

如果网络类型为专有网络，说明该ECS实例已成功迁移到VPC。



4. 检查内网环境和业务运行环境。

场景	迁移计划	后续操作

场景	迁移计划	后续操作
经典网络中的ECS实例全部迁移到VPC	<ul style="list-style-type: none"> 将选择迁移的目标专有网络设置为（默认）系统自动创建专有网络，网段：10.0.0.0/8。 将已迁移实例和该计划内还未迁移的经典实例保持内网联通设置为否。 	检查业务系统运行是否正常。
部分ECS实例迁移到VPC，部分ECS实例保留在经典网络	<ul style="list-style-type: none"> 将选择迁移的目标专有网络设置为（默认）系统自动创建专有网络，网段：10.0.0.0/8。 将已迁移实例和该计划内还未迁移的经典实例保持内网联通设置为是。 	检查业务系统运行是否正常。
其他场景	将选择迁移的目标专有网络设置为其他网段不是10.0.0.0/8的VPC。	<ul style="list-style-type: none"> i. 根据需要检查网络连通性。 ii. 该场景下不支持保留源ECS实例的内网IP。如果业务中通过内网IP对接，需要配置为新的内网IP。 iii. 检查业务系统运行是否正常。

后续步骤

- 如果ECS实例使用Linux系统，并且未保留内网IP，需要修改ECS实例的`/etc/hosts`文件。

```

::1      localhost        localhost.localdomain  localhost6        localhost6.localdomain6
127.0.0.1  localhost        localhost.localdomain  localhost4        localhost4.localdomain4
72.16.    ecs             ecs

```

- 执行命令 `vi /etc/hosts` 打开文件。
 - 按 `Enter` 进入编辑模式。
 - 将原内网IP修改为新的内网IP。
 - 按 `Esc` 退出编辑模式。
 - 输入 `:wq`，然后按回车键（Enter）。
- 如果未保留内网IP，还需要在其他云产品的白名单中移除废弃的原内网IP地址。
例如，RDS、SLB、OSS、容器服务等支持设置白名单的云产品。
- 如果跨可用区迁移ECS实例，可能影响和云数据库RDS、云数据Redis、云数据MongoDB等产品的联通性。请及时调整应用的配置，例如将对应的RDS实例等迁移至同一个可用区，确保能够持续提供服务。
具体操作，请参见[迁移可用区](#)。
- 如果源ECS实例长时间未重启或升级过内核，迁移后的ECS实例可能会有文件系统检查fsck（File System Check）、相关配置改动失效、启动失败等问题。
- （可选）处理因网卡被删除发生的授权码变化。
在ECS实例上的软件绑定了MAC地址时，如果软件供应商认可阿里云的迁移证明，您可以重新授权；如果授权存在问题，请根据实际情况订正或者选择回滚。
- （可选）如果长时间未重启ECS实例，或者升级内核后未重启ECS实例，在重新启动ECS实例时系统会检查文件系统和更新相关配置。如果出现启动失败等问题，请及时[提交工单](#)联系阿里云。

常见问题

- 迁移后无法打开网站、服务不可用或者无法读写数据库，为什么？

可能是目标安全组没有开启相应通信端口，建议您尝试克隆原有的安全组规则。具体操作，请参见[克隆安全组](#)。

- 迁移后无法正常使用软件，提示授权码过期、授权码无效或者没有授权码，为什么？

可能原因如下：

- 该应用没有迁移许可计划：建议您联系软件供应商或者渠道伙伴提交验证表单，重新授权。
- 该应用通过绑定MAC地址注册：部分软件采用绑定MAC地址注册合法环境。由于迁移专有网络VPC后，只保留一个MAC地址（公网MAC地址或私网MAC地址），如果没有保留已绑定的MAC地址，会出现授权失败的情况。建议您联系软件供应商，确认在ECS实例上注册该软件时是否以绑定MAC地址的形式，并重新绑定MAC地址。更多信息，请参见[弹性网卡概述](#)。

- 迁移前能使用FTP服务，迁移后不能用了，为什么？

迁移到VPC的ECS实例不再保留公网网卡，会导致FTP服务不可用。建议您：

- 转换实例公网IP为弹性公网IP（EIP）。
- 设置EIP网卡可见模式。

 **说明** 部分已停售的实例规格和上一代入门级实例规格不支持挂载弹性网卡，这时建议您升级为具有兼容性的实例规格后采用以上方案，具体操作，请参见[升降配方式概述](#)。

- 部分Windows实例迁移后，实例内部找不到数据盘，为什么？

迁移后，部分Windows实例的云盘处于脱机状态，建议您通过以下方式批量设置云盘自动联机。更多信息，请参见[Windows系统的ECS实例磁盘脱机处理方法](#)。

- 登录[ECS管理控制台](#)。
- 在左侧导航栏，选择[运维与监控 > 发送命令/文件（云助手）](#)。
- 单击[创建/执行命令](#)，然后创建并执行以下云助手命令。

云助手命令设置示例如下表所示，其他参数保持默认值即可。更多参数的说明，请参见[立即执行命令](#)。

参数	取值
命令类型	PowerShell
命令内容	@("san policy=onlineall") diskpart
选择实例	选中待修复Windows实例。

- 单击[执行并保存](#)。

- ECS实例从经典网络迁移到VPC后，使用FTP传输文件失败，为什么？

经典网络中的ECS实例会有公网网卡和私网网卡，而VPC中的ECS实例只有私网网卡。因此，如果您的应用必须识别公网IP，就需要进行特殊配置。

大部分客户端会使用FTP被动模式访问FTP Server，该模式下需要FTP Server将其IP地址告知客户端，由于专有网络下无法直接识别公网IP，就将内网IP告知了客户端，客户端使用该内网IP尝试访问就会失败。

因此，使用VPC中ECS实例作为FTP Server时，建议主动将ECS实例的公网IP告知FTP Server程序。由于FTP Server程序类型众多，设置方式也存在差异，请您根据使用的程序类型搜索设置方法。以常见的vsftpd为例，打开vsftpd的配置文件，并加入以下内容：

```
listen_ipv6=NO
pasv_address=<PublicIP>
```

说明 将<PublicIP>替换为ECS实例的公网IP地址，推荐使用弹性公网IP。

相关文档

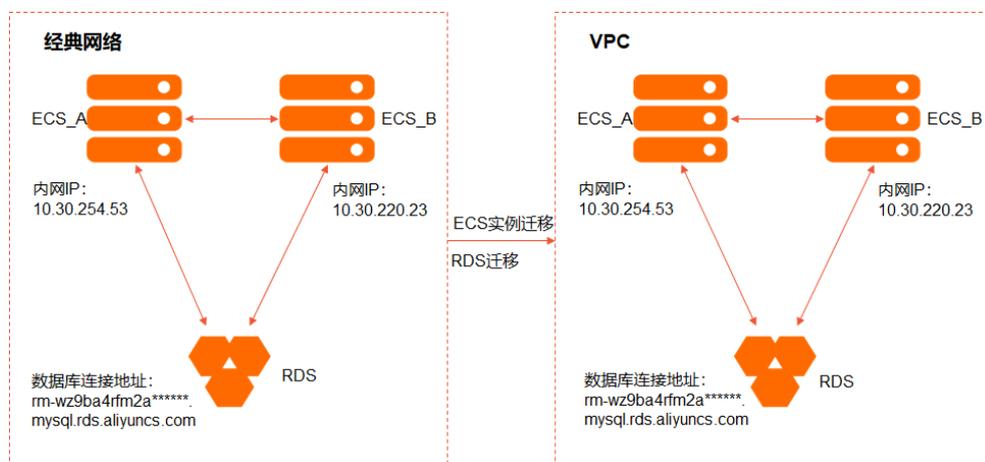
- 云数据库Redis切换为专有网络
- 云数据库RDS切换为专有网络
- 云数据库RDS临时混访方案（同时保留经典网络和专有网络地址）

12.2. 经典网络实例全部迁移到VPC最佳实践

本文介绍如何将经典网络中的ECS实例和RDS实例全部迁移到VPC，并且在迁移完成后业务环境快速可用。

背景信息

您在经典网络中，已购买ECS实例（ECS_A和ECS_B）和RDS实例，其中ECS实例作为应用服务器，RDS实例作为数据库服务器，各实例之间通过内网连接。由于业务发展需要，需要将ECS实例和RDS实例全部迁移到VPC。为了保持业务稳定，希望不改变实例的内网IP地址。应用场景如下图所示。



准备工作

在迁移前，建议完成如下操作：

- 为ECS实例创建快照，备份数据。具体操作，请参见[创建一个云盘快照](#)。
- 迁移时会重启ECS实例，建议您将应用服务设置为开机自启动，并做好可用性监控。

更多信息，请参见[迁移影响](#)和[迁移准备工作](#)。

步骤一：迁移ECS实例

通过实例迁移计划，将应用服务器（ECS_A和ECS_B）迁移到VPC网络，具体操作如下所示。

- 登录[ECS管理控制台](#)。
- 在左侧导航栏，单击[运维与监控](#) > [实例迁移计划](#)。
- 在顶部菜单栏左上角处，选择地域。
- 单击[创建迁移计划](#)。
- 在[配置迁移计划](#)引导页，配置目标网络等信息，单击下一步。

i. 选择迁移的目标可用区与专有网络。

1 配置迁移计划

目标可用区与专有网络

请输入计划名称

* 选择目标可用区

深圳 可用区B
找不到可用区 ?

* 选择迁移的目标专有网络，或先创建专有网络 ?

(默认)系统自动创建专有网络, 网段: 10.0.0.0/8
C

配置项	说明
请输入计划名称	设置迁移计划名称，例如ECS_c2v_demo。
选择目标可用区	<p>从下拉列表中选择需要迁移的目标可用区，例如迁移到深圳 可用区B。</p> <div style="background-color: #e6f2ff; padding: 10px; border: 1px solid #d9e1f2;"> <p>? 说明</p> <ul style="list-style-type: none"> ■ 可用区选项是系统根据资源自动规划，您只能在下拉列表中选择对应可用区。 ■ 一个实例迁移计划只能设置一个可用区，如果您需要设置多个可用区，需要创建多个迁移计划。 </div>
选择迁移的目标专有网络	从下拉列表中选择（默认）系统自动创建专有网络，网段：10.0.0.0/8，系统自动创建目标专有网络。

ii. 设置安全组和MAC地址。

实例网络属性

* 目标安全组

(默认)克隆经典实例安全组 [进一步了解克隆](#)

指定安全组

* 优先保留 Mac 地址策略

(默认)私网 Mac

公网 Mac

配置项	说明
目标安全组	系统自动选择（默认）克隆经典实例安全组 <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px;"> ? 说明 不支持克隆存在组组授权规则的安全组。 </div>
优先保留Mac地址策略	选择需要保留的MAC地址，可选私网Mac或公网Mac。 原业务环境中未绑定MAC地址，此处选择私网Mac。

iii. 设置保留实例的内网IP。

实例网络连通性

* 保留实例内网 IP

(默认)是

创建虚拟交换机策略 自动 手动

系统将在目标专有网络里，根据经典实例的内网 IP 自动规划 16 网段的交换机，如因网段占用，交换机数量限制导致无法创建，请选择手动

否

* 已迁移实例和该计划内还未迁移的经典实例保持内网联通

(默认)否

是

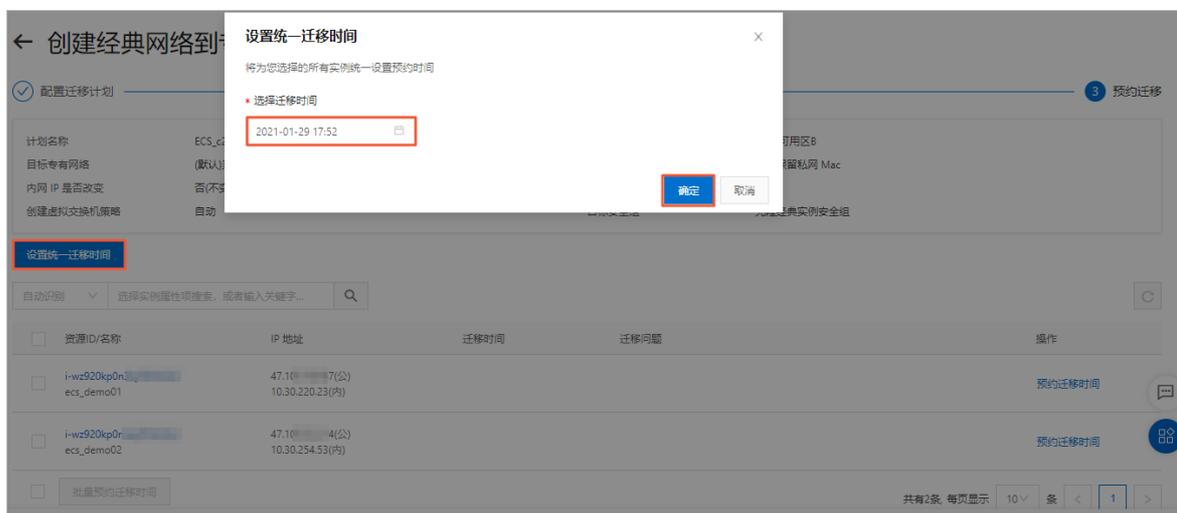
配置项	说明
保留实例内网 IP	系统默认选择是，保留ECS实例原来的内网IP地址。 创建虚拟交换机策略默认选择自动，系统自动创建虚拟交换机。
已迁移实例和该计划内还未迁移的经典实例保持内网联通	所有ECS实例全部迁移到VPC，所以不需要和原经典网络保持互通，此处选择否。

6. 在选择待迁移实例引导页，选中待迁移的ECS实例，单击下一步。



7. 在预约迁移引导页，为实例设置统一的迁移时间，单击创建验证。

说明 在迁移时需要重启ECS实例，建议您设置业务低谷的时间段进行迁移。



- i. 单击设置统一迁移时间。
- ii. 在设置统一迁移时间对话框中，选择迁移时间。
- iii. 单击确定。

8. 在创建验证对话框中，您可以查看迁移注意事项，并单击确认并创建。

说明 如果您的迁移计划不符合要求，系统将提示错误信息。此时您可以根据错误信息修改问题后重新创建迁移计划。

迁移计划创建完成后，系统将在指定时间自动为您迁移ECS实例。正常迁移完成后，如下图所示。如果迁移过程中出现问题，请参见[常见问题](#)。



迁移完成后，您可以在左侧导航栏选择**实例与镜像 > 实例查看ECS**。此时，ECS实例的网络类型已经变为VPC，内网IP地址保持不变。

实例列表						
检查到安全组中包含允许对特定端口进行不受限制访问的规则，存在潜在高危风险。 查看详情						
选择实例属性项搜索，或者输入关键字识别搜索						
实例ID/名称	监控	可用区	IP地址	状态	网络类型	配置
<input type="checkbox"/> i-wz920kp0n3 ecs_demo02		深圳 可用区B	47.106 (公) 10.30.254.53 (私有)	运行中	专有网络	1 vCPU 1 GiB (I/O优化) ecs.xn4.small 5Mbps (峰值)
<input type="checkbox"/> i-wz920kp0n3 ecs_demo01		深圳 可用区B	47.106 (公) 10.30.220.23 (私有)	运行中	专有网络	1 vCPU 1 GiB (I/O优化) ecs.xn4.small 5Mbps (峰值)

步骤二：迁移RDS实例

通过RDS切换网络类型功能，将数据库服务器（RDS实例）迁移到VPC网络，具体操作如下所示。更多信息，请参见[更改网络类型](#)。

1. 获取系统自动创建的VPC信息。
 - i. 选择**实例与镜像 > 实例**。
 - ii. 单击已迁移到VPC的实例ID。
 - iii. 在实例详情页，单击专有网络ID和虚拟交换机ID，获取专有网络ID、虚拟交换机ID和虚拟交换机的可用区信息。

网络信息		绑定辅助弹性网卡	
网络类型	专有网络	RDMA IP	-
弹性网卡	eni-wz9ccqxi3	弹性IP实例ID	-
专有网络	vpc-wz9avqy2	虚拟交换机	vsw-wz98loggfq88msu
主私网IP	10.30	辅助私网IP	-
IPv6 地址	该实例规格暂不支持IPv6地址分配，查看 支持 IPv6 的实例规格		

名称	示例
专有网络ID	vpc-wz9avqy2c3fw8w4*****
虚拟交换机	vsw-wz98loggfq88msu*****
虚拟交换机可用区信息	深圳 可用区B

2. 获取经典网络RDS的网络信息。
 - i. 登录[RDS管理控制台](#)。
 - ii. 在左侧导航栏单击**实例列表**。
 - iii. 在顶部菜单栏左上角处，选择地域。
 - iv. 单击目标RDS实例ID。

v. 查看RDS实例的地域及可用区信息。



- 如果可用区和上一步骤中虚拟交换机的可用区一致，则执行下一步。
- 如果可用区和上一步骤中虚拟交换机的可用区不一致，则需要先创建同一可用区的虚拟交换机，再执行下一步。关于如何创建虚拟交换机，请参见[创建和管理交换机](#)。

说明 本示例中，虚拟交换机和RDS都在华南1（深圳）可用区B，无需新建虚拟交换机。

3. 在左侧导航栏单击数据库连接。

4. 单击切换专有网络。

5. 在弹出的对话框中，选择VPC和交换机，以及是否保留经典网络地址。



配置项	说明
选择VPC	选择步骤1中查询的VPC ID（例如vpc-wz9avqy2c3fw8w4*****）。
选择虚拟交换机	选择同可用区的虚拟交换机ID（例如vsw-wz98loggfq88msu*****）。 说明 如果是新建的虚拟交换机，请选择新的虚拟交换机ID。

6. 单击确定。

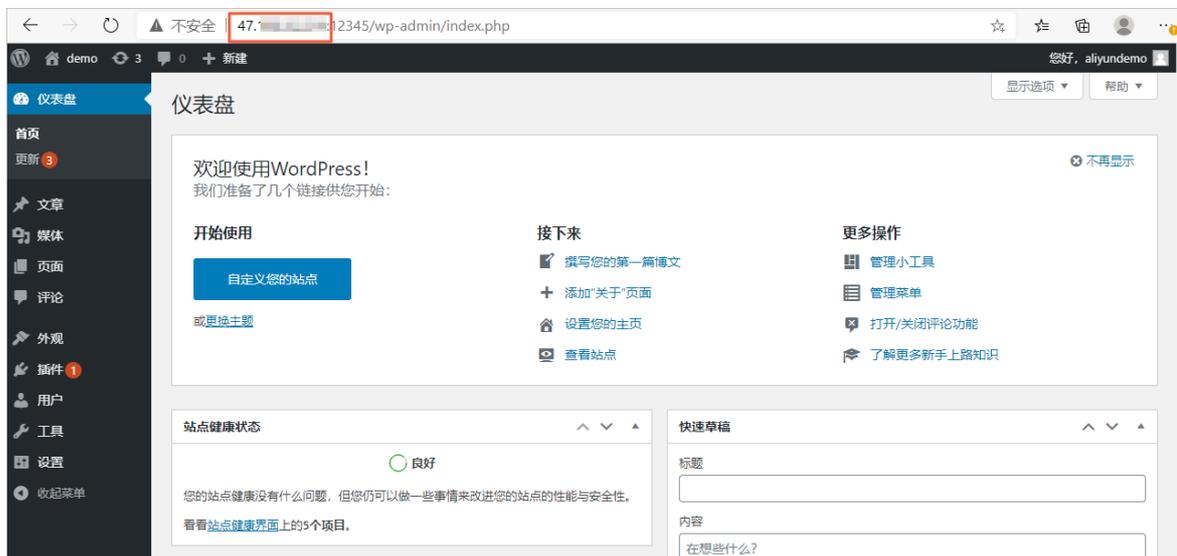
迁移完成后，您可以在左侧导航栏单击数据库连接。此时，RDS的网络类型已经变成专有网络，内网连接串地址保持不变。



步骤三：检查迁移结果

完成网络迁移后，通过访问业务系统，检查业务系统是否正常运行。

1. 通过浏览器访问Web应用。
2. 查看Web应用是否能够正常访问。



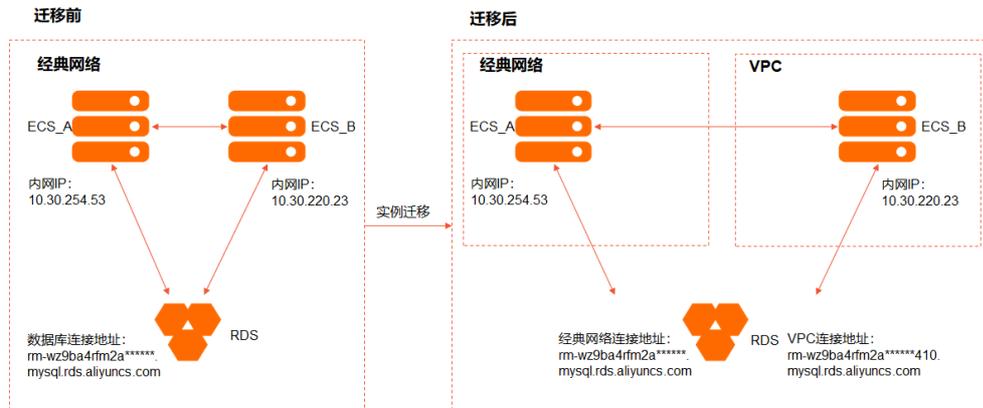
如上图所示，ECS实例和RDS实例都迁移到VPC后，无需修改配置文件，业务系统即能够正常运行。

12.3. 经典网络实例部分迁移到VPC最佳实践

本文介绍如何将经典网络中的ECS实例和RDS实例部分迁移到VPC，并且实现内网互通。

背景信息

您在经典网络中，已购买ECS实例（ECS_A和ECS_B）和RDS实例，其中ECS实例作为应用服务器，RDS实例作为数据库服务器，各实例之间通过内网连接。由于业务发展需要，需要将ECS实例（ECS_B）迁移到VPC，ECS实例（ECS_A）还是保留在经典网络。为了保持业务稳定，希望不改变ECS实例的内网IP地址，各实例之间内网能够互通。应用场景如下图所示。



注意 已迁移ECS实例只支持和同一个实例迁移计划中的经典网络实例内网互通，不支持和实例迁移计划外的经典网络实例内网互通。

具体的迁移案例，请参见[混访混挂迁移示例](#)。

准备工作

在迁移前，建议完成如下操作：

- 为ECS实例创建快照，备份数据。具体操作，请参见[创建一个云盘快照](#)。
- 迁移时会重启ECS实例，建议您将应用服务设置为开机自启动，并做好可用性监控。

更多信息，请参见[迁移影响](#)和[迁移准备工作](#)。

注意事项

- 部分ECS实例从经典网络迁移到VPC网络，如果需要持续保持互通，需要在迁移计划中设置已迁移实例和该计划内还未迁移的经典实例保持内网互通。
- 云数据库迁移过程中，需开启保留原经典网络功能。云数据库可以同时提供VPC网络和经典网络两个网络地址，以确保VPC网络实例和经典网络实例访问不受影响。更多信息，请参见[云数据库混访和其它云产品混访支持](#)。
- 迁移到VPC的ECS实例和云数据库实例，必须在同一个VPC下，才可以保持内网互通。
- 不同云产品迁移后可能需要修改配置参数，会出现一定时间内服务不可用的情况，请提前做好迁移规划。

步骤一：迁移ECS实例

通过实例迁移计划，将应用服务器（ECS_B）迁移到VPC网络，具体操作如下所示。

1. 登录[ECS管理控制台](#)。
2. 在左侧导航栏，单击[运维与监控](#) > [实例迁移计划](#)。
3. 在顶部菜单栏左上角处，选择地域。
4. 单击[创建迁移计划](#)。
5. 在[配置迁移计划](#)引导页，配置目标网络等信息，单击[下一步](#)。

i. 选择迁移的目标可用区与专有网络。

1 配置迁移计划

目标可用区与专有网络

请输入计划名称

* 选择目标可用区

深圳 可用区B
▼
找不到可用区 ?

* 选择迁移的目标专有网络，或先创建专有网络 ?

(默认)系统自动创建专有网络, 网段: 10.0.0.0/8
▼
C

配置项	说明
请输入计划名称	设置迁移计划名称，例如ECS_c2v_demo。
选择目标可用区	<p>从下拉列表中选择需要迁移的目标可用区，例如迁移到深圳 可用区B。</p> <div style="background-color: #e6f2ff; padding: 10px; border: 1px solid #d9e1f2;"> <p>? 说明</p> <ul style="list-style-type: none"> ■ 可用区选项是系统根据资源自动规划，您只能在下拉列表中选择对应可用区。 ■ 一个实例迁移计划只能设置一个可用区，如果您需要设置多个可用区，需要创建多个迁移计划。 </div>
选择迁移的目标专有网络	<ul style="list-style-type: none"> ■ 如果需要跟其他云产品（例如云数据库RDS）互相访问，需选择云产品所在的专有网络。 ■ 如果不需要，从下拉列表中选择（默认）系统自动创建专有网络，网段：10.0.0.0/8，系统自动创建目标专有网络。

ii. 设置安全组和MAC地址。

实例网络属性

* 目标安全组

(默认)克隆经典实例安全组 [进一步了解克隆](#)

指定安全组

* 优先保留 Mac 地址策略

(默认)私网 Mac

公网 Mac

配置项	说明
目标安全组	系统自动选择（默认）克隆经典实例安全组 ? 说明 不支持克隆存在组授权规则的安全组。
优先保留MAC地址策略	选择需要保留的MAC地址，可选私网MAC或公网MAC。 原业务环境中未绑定MAC地址，此处选择私网MAC。

iii. 设置保留实例的内网IP和内网互通。

实例网络连通性

* 保留实例内网 IP

(默认)是

否

创建虚拟交换机策略 自动 手动

系统将在目标专有网络里，根据经典实例的内网 IP 自动规划 16 网段的交换机，如因网段占用，交换机数量限制导致无法创建，请选择手动

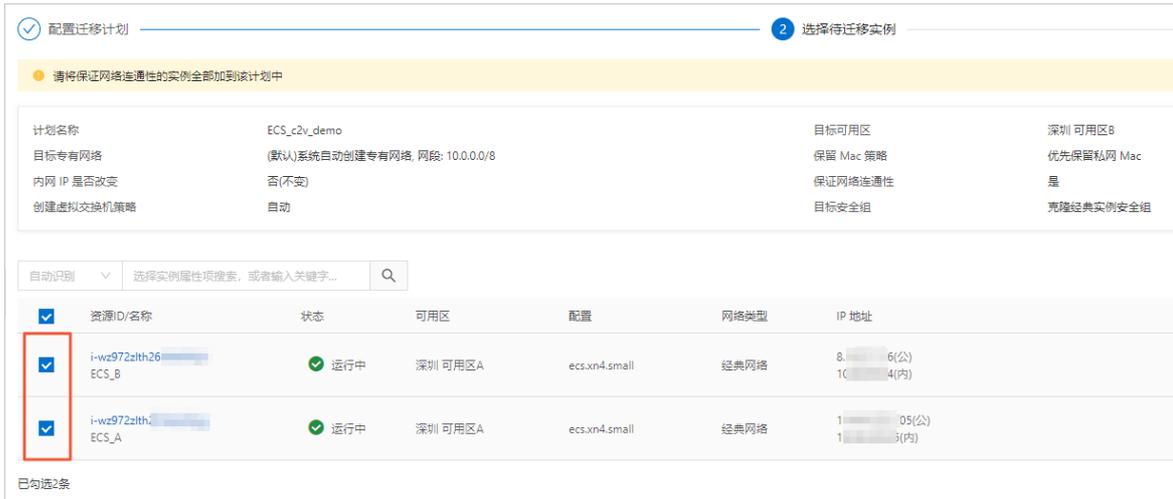
* 已迁移实例和该计划内还未迁移的经典实例保持内网联通

(默认)否

是

配置项	说明
保留实例内网 IP	系统默认选择是，保留ECS实例原来的内网IP地址。 创建虚拟交换机策略默认选择自动，系统自动创建虚拟交换机。
已迁移实例和该计划内还未迁移的经典实例保持内网联通	需要ECS_A和ECS_B互通，此处选择是。

6. 在选择待迁移实例引导页，选中ECS实例，单击下一步。

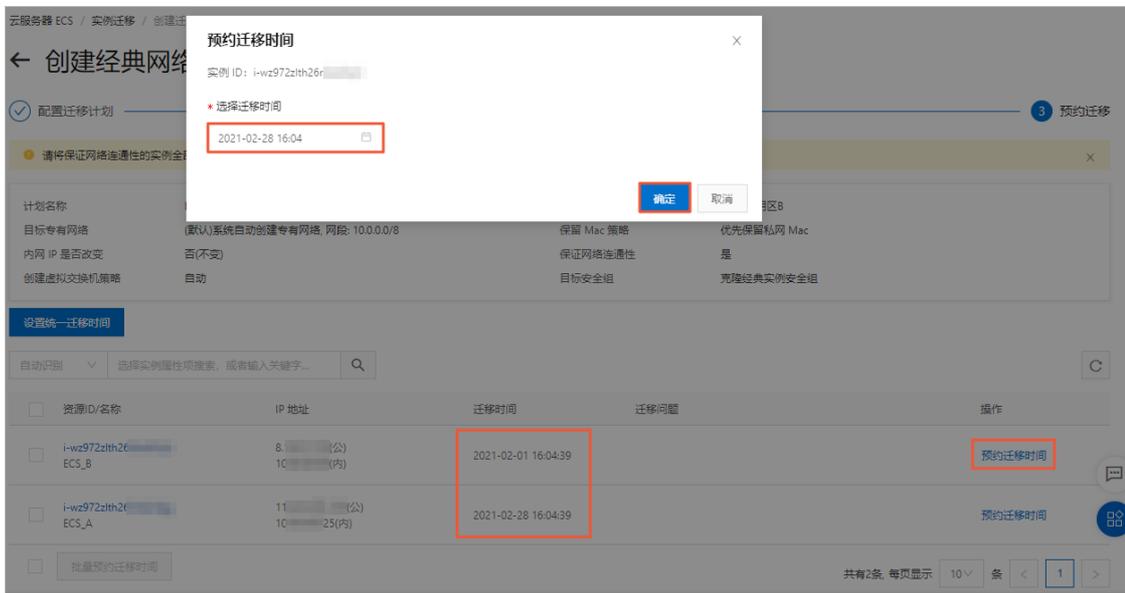


7. 在预约迁移引导页，为实例设置迁移时间，单击创建验证。

说明 在迁移时需要重启ECS实例，建议您设置业务低谷的时间段进行迁移。

- i. 在实例的操作列，单击预约迁移时间。
- ii. 在预约迁移时间对话框中，选择迁移时间。

注意 只有在实例迁移计划中的经典网络实例才能和已迁移实例内网互通。因此，对于需要保留在经典网络的实例（ECS_A），您需要设置一个较长的预约迁移时间，让实例保留在实例迁移计划中。在预约时间临近时，如果ECS实例还需要保留在经典网络中，您需要重新设置预约迁移时间。建议您安排计划将经典网络中的实例迁移到VPC。



iii. 单击确定。

8. 在创建验证对话框中，您可以查看迁移注意事项，并单击确认并创建。

说明 如果您的迁移计划不符合要求，系统将提示错误信息。此时您可以根据错误信息修改问题后重新创建迁移计划。

迁移计划创建完成后，系统将在指定时间自动为您迁移ECS实例。ECS_B正常迁移完成后，如下图所示。如果迁移过程中出现问题，请参见[常见问题](#)。



迁移完成后，您可以在左侧导航栏选择实例与镜像 > 实例查看ECS实例。此时，ECS实例的网络类型已经变为VPC，内网IP地址保持不变。



步骤二：迁移RDS实例

通过RDS切换网络类型功能，将数据库服务器（RDS实例）迁移到VPC网络，具体操作如下所示。更多信息，请参见[更改网络类型](#)。

1. 获取系统自动创建的VPC信息。
 - i. 选择实例与镜像 > 实例。
 - ii. 单击已迁移到VPC的实例ID。
 - iii. 在实例详情页，单击专有网络ID和虚拟交换机ID，获取专有网络ID、虚拟交换机ID和虚拟交换机的可用区信息。



名称	示例
专有网络ID	vpc-wz9avqy2c3fw8w4*****
虚拟交换机	vsw-wz98loggfq88msu*****
虚拟交换机可用区信息	深圳 可用区B

2. 获取经典网络RDS的网络信息。
 - i. 登录[RDS管理控制台](#)。
 - ii. 在左侧导航栏单击实例列表。

- iii. 在顶部菜单栏左上角处，选择地域。
- iv. 单击目标RDS实例ID。
- v. 查看RDS实例的地域及可用区信息。



- 如果可用区和上一步骤中虚拟交换机的可用区一致，则执行下一步。
- 如果可用区和上一步骤中虚拟交换机的可用区不一致，则需要先创建同一可用区的虚拟交换机，再执行下一步。关于如何创建虚拟交换机，请参见[创建和管理交换机](#)。

说明 本示例中，虚拟交换机和RDS都在华南1（深圳）可用区B，无需新建虚拟交换机。

- 3. 在左侧导航栏单击数据库连接。
- 4. 单击切换专有网络。
- 5. 在弹出的对话框中，选择VPC和交换机，并保留经典网络地址。



配置项	说明
选择VPC	选择步骤1中查询的VPC ID（例如vpc-wz9avqy2c3fw8w4*****）。
选择虚拟交换机	选择同可用区的虚拟交换机ID（例如vsw-wz98loggfq88msu*****）。 说明 如果是新建的虚拟交换机，请选择新的虚拟交换机ID。

配置项	说明
保留原经典网络	<p>选中保留原经典网络，并设置过期时间（例如120天以后）。</p> <p>说明 在经典网络地址到期前，请将经典网络的ECS迁移到VPC中，以实现业务平滑迁移到VPC。更多信息，请参见临时混访方案（同时保留经典网络和专有网络地址）。</p>

6. 单击确定。

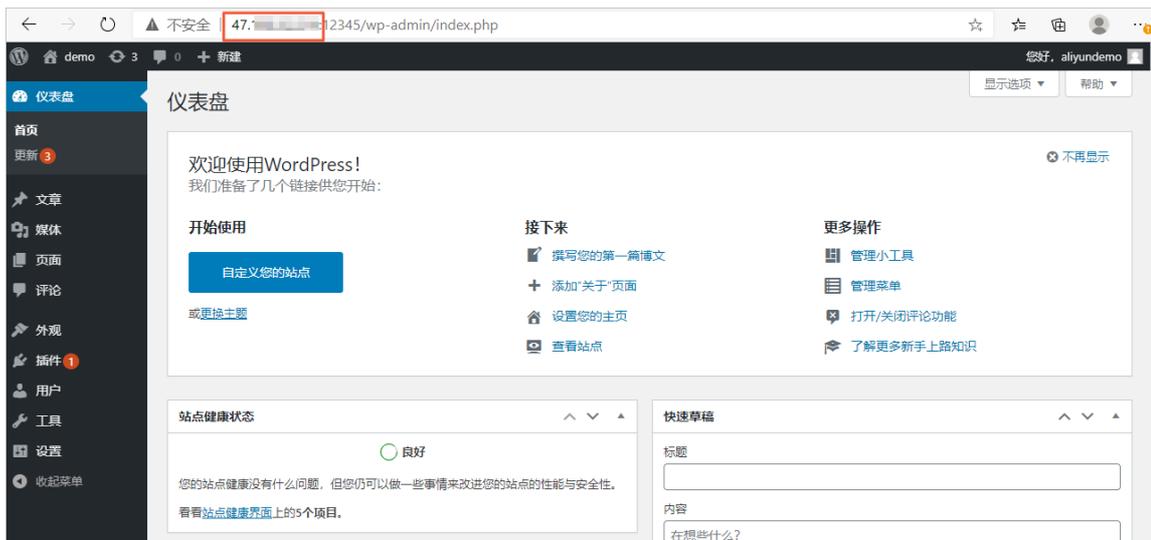
迁移完成后，您可以在左侧导航栏单击数据库连接。此时，RDS的网络类型已经变成专有网络，其中经典网络的内网连接串地址保持不变，VPC的内网连接串地址已变动。



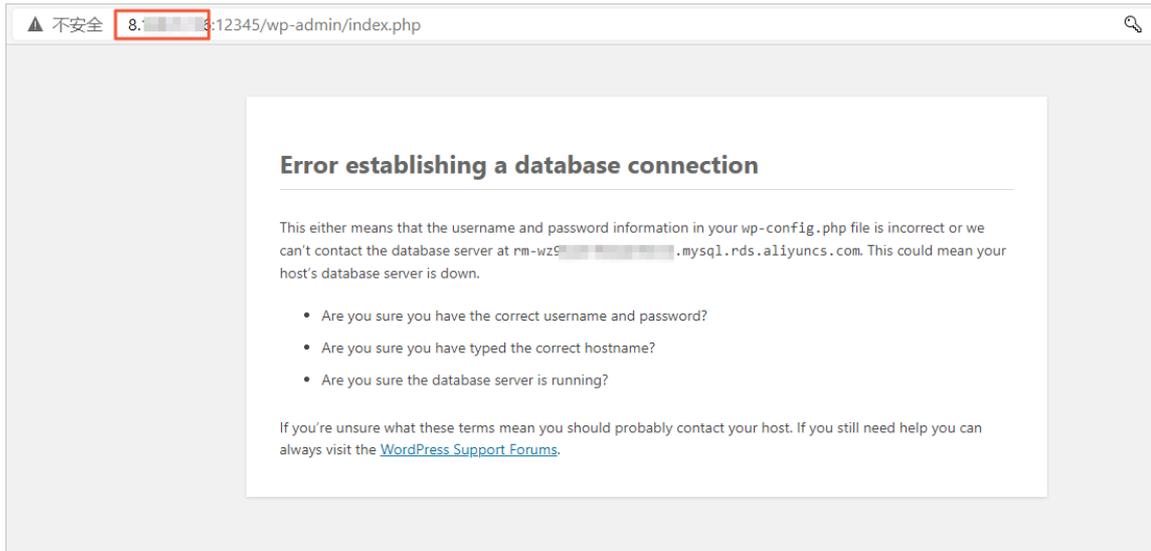
步骤三：检查迁移结果

完成网络迁移后，通过访问业务系统，检查业务系统是否正常运行。

1. 通过浏览器访问Web应用。
2. 查看Web应用是否能够正常访问。
 - o 经典网络的ECS实例（ECS_A），能够正常访问。



- o VPC的ECS实例（ECS_B），不能访问。



如上图所示，留在经典网络的实例（ECS_A）的业务系统能够正常运行；迁移到VPC的ECS实例（ECS_B）的业务系统访问异常。

3. 修改迁移到VPC的ECS实例（ECS_B）的配置信息。

由于RDS实例中VPC的内网连接串地址变动，您需要修改ECS_B的配置信息，以保证ECS_B和RDS实例能够正常连接。根据业务系统不同，需要修改的方式不一样，具体操作请联系您业务系统的开发和运维人员。

例如，在WordPress中，您需要在`wp-config.php`中修改数据库的连接地址，具体操作如下所示。

- i. 远程登录ECS实例（ECS_B）。具体操作，请参见[通过密码认证登录Linux实例](#)。
- ii. 运行以下命令，进入`wp-config.php`文件所在目录（例如路径为`/var/www/html`）。

```
cd /var/www/html
```

- iii. 使用vi编辑器编辑`wp-config.php`。

```
define( 'DB_NAME', 'wordpress02' );

/** MySQL database username */
define( 'DB_USER', 'wordpress' );

/** MySQL database password */
define( 'DB_PASSWORD', '1234567890' );

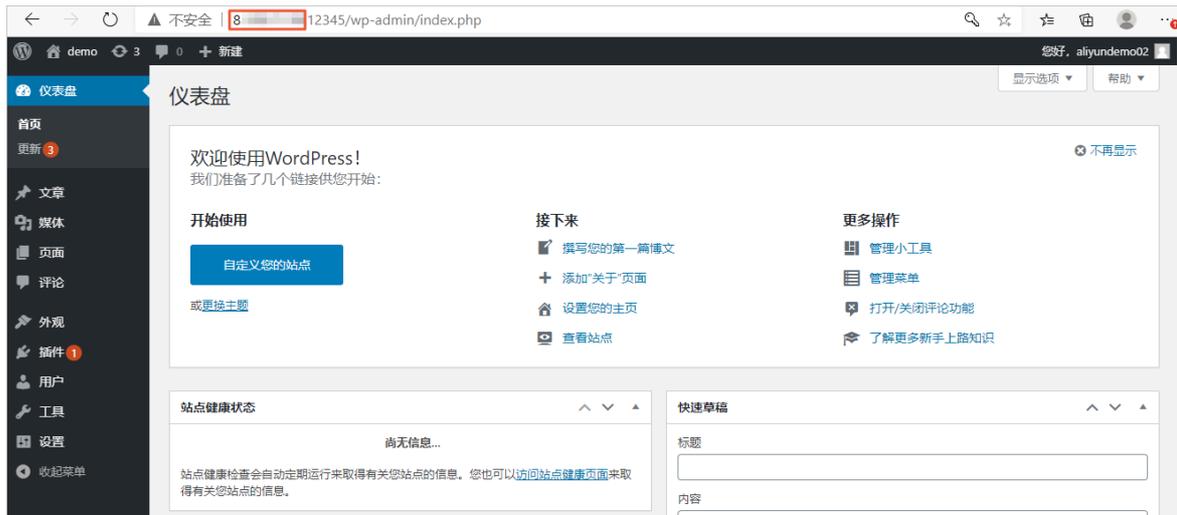
/** MySQL hostname */
define( 'DB_HOST', 'rm-wz5b1234567890.mysql.rds.aliyuncs.com' );

/** Database Charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8mb4' );

/** The Database Collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );
```

将上图原RDS内网连接串地址，替换为VPC中RDS的内网连接串地址。

4. 重新检查ECS_B的Web应用是否能够正常访问。



如上图所示，修改ECS实例的配置文件后，业务系统能够正常运行。

13. 经典网络和专有网络互通

您可以通过建立ClassicLink连接，使经典网络类型的ECS实例可以和专有网络VPC中的云资源通过内网互通。

背景信息

在使用ClassicLink功能前，请注意如下限制：

- 最多允许1000台经典网络ECS实例连接到同一个VPC。
- 同账号且同地域下，一台经典网络ECS实例只能连接到一个VPC。

如果要进行跨账号连接，例如将账号A的ECS实例连接到账号B的VPC，可以将ECS实例从账号A过户到账号B。

您可以[提交工单](#)申请ECS实例过户。过户前，确保您已了解[ECS实例过户须知](#)。

- 经典网络ECS实例只支持与VPC主网段下的ECS实例通信，而不支持与VPC附加网段下的ECS实例通信。
- VPC要开启ClassicLink功能，需要满足以下条件。

VPC网段	限制
172.16.0.0/12	该VPC中不存在目标网段为10.0.0.0/8的自定义路由条目。
10.0.0.0/8	<ul style="list-style-type: none"> ◦ 该VPC中不存在目标网段为10.0.0.0/8的自定义路由条目。 ◦ 确保和经典网络ECS实例通信的交换机的网段在10.111.0.0/16内。
192.168.0.0/16	<ul style="list-style-type: none"> ◦ 该VPC中不存在目标网段为10.0.0.0/8的自定义路由条目。 ◦ 需要在经典网络ECS实例中增加192.168.0.0/16指向私网网卡的路由。您可以使用提供的脚本添加路由，下载路由脚本。 <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 10px;"> <p> 说明 在运行脚本前，请仔细阅读脚本中包含的readme.txt文件。</p> </div>

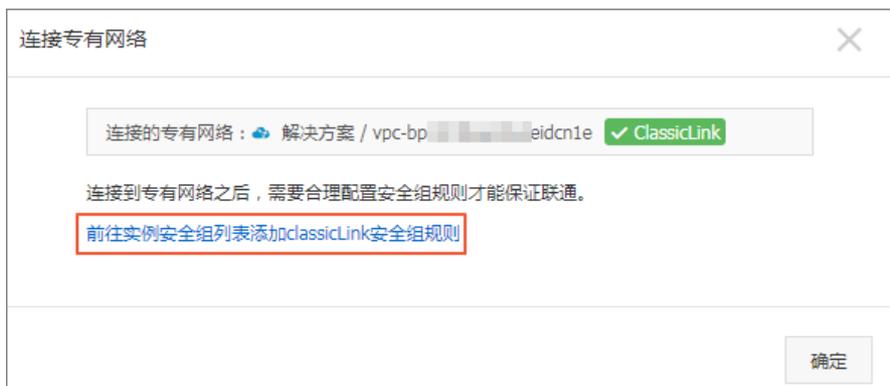
更多信息，请参见[ClassicLink概述](#)。

以下实例演示了如何互通经典网络和专有网络。



操作步骤

1. 登录**专有网络管理控制台**。
2. 在顶部菜单栏左上角处，选择地域。
3. 在目标专有网络开启ClassicLink功能。
 - i. 在专有网络列表，单击目标专有网络的ID。
 - ii. 在基本信息页面，单击右上角的开启ClassicLink。
 - iii. 在确认提示框中，单击**确定**。
4. 登录**ECS管理控制台**。
5. 在左侧导航栏，选择**实例与镜像 > 实例**。
6. 在顶部菜单栏左上角处，选择地域。
7. 在经典网络ECS实例的安全组，设置ClassicLink安全组规则。
 - i. 找到目标经典网络类型ECS实例，在操作列中，选择**更多 > 网络和安全组 > 设置专有网络连接状态**。
 - ii. 在弹出的对话框中选择目标专有网络VPC，单击**确定**。
 - iii. 单击前往实例安全组列表添加classicLink安全组规则。



- iv. 单击配置规则。
- v. 单击右上角的添加ClassicLink安全组规则，根据以下信息配置ClassicLink安全组规则。

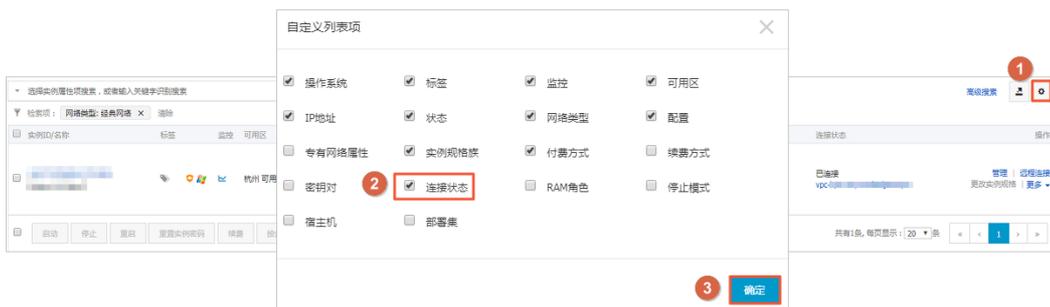
配置	说明
经典网络安全组	显示经典网络安全组的名称。
选择专有网络	选择目标专有网络。
选择专有网络安全组	选择专有网络中需要互通的安全组。
授权方式	选择一种授权方式： <ul style="list-style-type: none"> ■ (推荐) 经典网络 <=> 专有网络: 相互授权访问。 ■ 经典网络 => 专有网络: 授权经典网络类型ECS实例访问专有网络VPC内的云资源。 ■ 专有网络 => 经典网络: 授权专有网络VPC内的云资源访问经典网络类型ECS实例。
协议类型	选择授权通信的协议，例如自定义TCP。
端口范围	端口的输入格式为xx/xx，比如授权80端口，则输入80/80。
优先级	设置该规则的优先级。数字越小，优先级越高。例如：1。
描述	输入安全组规则的描述信息。

- vi. 单击确定。

执行结果

通过以下步骤查看是否已经设置成功。

1. 返回ECS管理控制台的实例列表。
2. 单击右侧的  图标，在弹出的对话框中选中连接状态复选框。
3. 单击确定，查看ECS实例的连接状态。



当连接状态显示为已连接，表示经典网络类型ECS实例成功连接到专有网络VPC。

14. 网络FAQ

本文汇总了使用云服务器ECS网络时的常见问题。

- 网络性能问题
 - 不同地域内的ECS实例通过公网通信，通信丢包概率如何？
 - 如果相同地域下的ECS实例通过内网通信，网络延迟性能如何？
 - 没有明确标注连接数规格的实例，如何保障连接数性能？
 - 在ECS实例上UDP PPS测试或者TCP带宽测试时性能不稳定，如何解决？
- 公网带宽问题
 - 什么是云服务器ECS的入网带宽和出网带宽？
 - 我购买的公网带宽为5 Mbit/s，相应的出入网带宽有什么区别？
 - 云服务器ECS的公网带宽是独享还是共享？
 - 云服务器ECS的公网带宽怎么收费？
 - 为何新建的ECS实例就有200 Kbps左右入网流量？
 - 如何查看云服务器ECS公网流量的费用账单？
 - 为什么云监控显示的云服务器ECS带宽和ECS控制台显示带宽不一致？
 - ECS实例为已停止状态，为什么按流量计费公网带宽仍产生出网流量？
 - 按使用流量计费时出网带宽最大是100Mbit/s，如何升级更高带宽？
- IP地址问题
 - ECS实例从经典网络迁移到专有网络VPC，内网IP会变化吗？
 - 如何查询ECS实例的IP地址？
 - 如何禁用ECS实例的公网网卡？
 - 如何查看弹性公网IP的流量和带宽监控信息？
- 网络访问和流量定向问题
 - 登录Windows的ECS实例后，使用IE浏览器无法打开网站，怎么办？
 - 为什么访问云服务器ECS上的网站时提示“很抱歉，由于您访问的URL可能对网站造成安全威胁，您的访问被阻断”？
 - 为什么我的Windows实例设置辅助私网IP后，无法访问公网环境？
 - 云盾是否有屏蔽IP地址的功能？
 - 云服务器ECS出现了异地登录怎么办？
 - 什么是流量清洗？
 - 云服务器ECS怎么取消流量清洗？
 - 怎么申请云服务器ECS反向解析？
 - 一个IP地址是否允许指向多个反向解析域名？
- 更换公网IP地址问题
 - 创建实例后，我可以更换公网IP（IPv4）地址吗？
 - 为什么在ECS管理控制台上，我看不到更换公网IP选项？
 - 除了更换公网IP地址，我还可以更换私网IP地址吗？
 - 如果在创建实例时未分配公网IP（IPv4）地址，实例创建成功后怎么获得公网IP地址？
- 网络基础问题
 - 什么是BGP机房？

- 什么是广域网和局域网?
- 什么是CIDR?
- 如何表示子网掩码?
- 如何划分子网?
- 限额问题
 - 如何查看资源的限额?

不同地域内的ECS实例通过公网通信，通信丢包概率如何？

当ECS实例间通过云企业网进行跨地域通信时，使用阿里云骨干网络进行传输。阿里云传输网络的服务目标是使跨地域的数据传输每小时数据包丢失率的P99分位统计值低于0.0001%。

如果相同地域下的ECS实例通过内网通信，网络延迟性能如何？

ECS实例在同地域同可用区内通过内网通信可以获得最低延迟，同可用区内实例间通信单向延迟P99分位小于180us。

没有明确标注连接数规格的实例，如何保障连接数性能？

如果某个实例规格族的指标数据中未明确标示连接数，则该实例规格族不提供连接数保障。建议您先进行业务压测了解实例的性能表现，以选择合适的实例规格。

 **说明** 建立连接后存在老化时间，在老化时间结束前连接会一直占用连接数，因此占用的连接数可能大于实际业务中使用的连接数。

在ECS实例上UDP PPS测试或者TCP带宽测试时性能不稳定，如何解决？

在ECS实例上进行网络性能测试时，有较多因素会影响测试结果，例如常见的性能调优手段NUMA拓扑适配、为任务绑定vCPU、为中断绑定vCPU等。

例如，在进行单流TCP带宽测试时，如果接收任务（例如net server进程）和网卡接收队列中断绑定在同一个vCPU上，网卡收到数据帧后会触发中断打断接收任务，频繁打断接收任务会导致测试结果不符合预期。针对这种情况，您可以将接收任务和网卡接收队列中断绑定在不同的vCPU上，利用多vCPU的性能优势获得较好的测试结果。

什么是云服务器ECS的入网带宽和出网带宽？

带宽类别	说明
入网带宽	流入云服务器ECS的带宽，例如： <ul style="list-style-type: none"> ● 云服务器ECS下载外部网络资源。 ● FTP客户端上传资源到云服务器ECS。
出网带宽	流出云服务器ECS的带宽，例如： <ul style="list-style-type: none"> ● 云服务器ECS对外提供访问。 ● FTP客户端下载云服务器ECS内部资源。

我购买的公网带宽为5 Mbit/s，相应的出入网带宽有什么区别？

5 Mbit/s表示带宽总出口是5 Mbit/s，出网带宽为5 Mbit/s，入网带宽不超过10 Mbit/s。

- 出网带宽，即从ECS实例流出的带宽。无论经典网络还是专有网络VPC，出网带宽最高为100 Mbit/s或200 Mbit/s（不同的计费方式，有不同的最高值）。
- 入网带宽，即流入ECS实例的带宽。入网带宽的最大值受出网带宽的影响。
 - 当出网带宽小于10 Mbit/s时，入网带宽最大为10 Mbit/s。

- 当出网带宽大于10 Mbit/s时，入网带宽与您购买的出网带宽一致。

 **注意** 按使用流量计费模式下的出入带宽峰值都是带宽上限，不作为业务承诺指标。当出现资源争抢时，带宽峰值可能会受到限制。如果您的业务需要有带宽的保障，请使用按固定带宽计费模式。

云服务器ECS的公网带宽是独享还是共享？

独享。

云服务器ECS的公网带宽怎么收费？

详情请参见[公网带宽计费](#)。

为何新建的ECS实例就有200 Kbps左右入网流量？

该流量是由ARP（Address Resolution Protocol）广播包产生的。因为每台ECS实例都被分配到一个较大的网段中，在同一网段里，每当有ECS实例与网关之间进行ARP广播时，您新建的ECS实例都会收到请求报文。但是，只要请求的不是您ECS实例的IP地址，您的ECS实例就不需要发送响应报文。

如何查看云服务器ECS公网流量的费用账单？

完成以下操作，查看云服务器ECS公网流量的费用账单。

1. 登录[ECS管理控制台](#)。
2. 选择**费用 > 用户中心**。
3. 在左侧导航栏中，选择**费用账单 > 费用账单**。
4. 单击**账单**页签，选择您需要查询的使用期间，设置产品为**云服务器ECS**，设置产品明细为**云服务器ECS-按量付费**，设置消费类型为**后付费**。
5. 单击**导出账单CSV**，输入验证码，单击**确认**。
6. 在打开的**导出记录**页面中，等待导出文件的状态变更为**导出成功**后，单击操作列的**下载**。
7. 打开下载的CSV文件，查看云服务器ECS公网流量的费用账单。

为什么云监控显示的云服务器ECS带宽和ECS控制台显示带宽不一致？

云服务器ECS作为SLB负载均衡实例的后端服务器，并且使用七层HTTP转发模型。使用这种转发模型，SLB负载均衡将客户端请求转发到云服务器ECS，ECS服务器通过外网带宽响应给用户，这个响应占用的带宽，在ECS控制台中不显示，它是计入到SLB负载均衡使用的出流量中，因此云监控显示的云服务器ECS带宽和ECS控制台显示带宽不一致。

ECS实例为已停止状态，为什么按流量计费公网带宽仍产生出网流量？

- 问题现象：DDoS基础防护中显示ECS实例为**清洗中**，ECS实例状态为**已停止**，但是按量付费的带宽每小时仍会产生费用。
- 原因分析：ECS实例开启了CC安全防护。开启CC安全防护后，安全机制会主动发送探测包对攻击源进行探测，可能会产生较大的出网流量。
- 解决方法：关闭CC安全防护。

按使用流量计费时出网带宽最大是100Mbit/s，如何升级更高带宽？

公网带宽限制由ECS实例和公网带宽的计费方式决定，详情请参见[使用限制](#)中的公网带宽部分。

如果您的ECS实例是包年包月实例，可以将公网带宽计费方式转为按固定带宽，出网带宽限制可提升至200Mbit/s。按固定带宽和按使用流量计费的区别，请参见[公网带宽计费](#)。

其它情况下，出网带宽的不能超过100Mbit/s。

ECS实例从经典网络迁移到专有网络VPC，内网IP会变化吗？

支持保留内网IP。如果您在实例迁移计划中，设置保留实例内网IP，则实例在迁移到VPC后内网IP不会变动。更多信息，请参见[ECS实例从经典网络迁移到专有网络](#)。

如何查询ECS实例的IP地址？

• Linux实例

通过 `ifconfig` 查看网卡信息。您可以查看IP地址、子网掩码、网关、DNS、MAC地址等信息。

• Windows实例

在命令窗口，通过 `ipconfig /all` 查看网卡信息。您可以查看IP地址、子网掩码、网关、DNS、MAC地址等信息。

 **说明** 如果您想要定位ECS实例IP地址对应的地理位置，可以访问[IP位置查询工具](#)进行查询。

如何禁用ECS实例的公网网卡？

• Linux实例

i. 通过 `ifconfig` 查看ECS实例网卡名称。

ii. 通过 `ifdown` 禁用网卡。假设网卡名称为 `eth1`，则输入 `ifdown eth1`。

 **说明** 您也可以通过`ifup`命令重新启动网卡。假设网卡名称为 `eth1`，则输入 `ifup eth1`。

• Windows实例

i. 在命令窗口，通过 `ipconfig` 查看网卡信息。

ii. 打开控制面板 > 网络和共享中心 > 更改适配器设置，禁用网卡。

如何查看弹性公网IP的流量和带宽监控信息？

详情请参见 [弹性公网IP文档高精度秒级监控](#)。

登录Windows的ECS实例后，使用IE浏览器无法打开网站，怎么办？

对于Windows实例，如果登录后使用IE浏览器无法打开网站，常见原因及解决方法如下：

• 检查ECS实例是否有公网IP

如果没有公网IP，您可以选择以下一种方式获取：

- 申请弹性公网IP并绑定到ECS实例，具体操作请参见 [申请EIP](#)和[绑定ECS实例](#)。
- 通过升级公网带宽配置来获取固定公网IP，具体操作请参见[包年包月实例修改带宽](#)或[按量付费实例修改带宽](#)。

• 关闭IE浏览器的增强安全配置

具体操作请参见[关闭Windows Server 2012的IE增强安全配置](#)。

为什么访问云服务器ECS上的网站时提示“很抱歉，由于您访问的URL可能对网站造成安全威胁，您的访问被阻断”？

- 问题现象：访问云服务器ECS搭建上的网站时，提示“很抱歉，由于您访问的URL可能对网站造成安全威胁，您的访问被阻断”。
- 原因分析：云盾的应用防火墙对您的URL访问判定存在攻击行为，进行安全拦截。
- 解决方法：将本地公网IP，添加到云盾应用防火墙的白名单中。详情请参见[通过设置白名单解决因误判IP被拦截问题](#)。

为什么我的Windows实例设置辅助私网IP后，无法访问公网环境？

- 问题现象：Windows实例设置辅助私网IP后，无法访问公网环境。
- 原因分析：Windows 2008之后出网IP策略调整为选择与下一跳IP的前缀匹配最短的IP，可能会导致网络不通的情况。
- 解决方案：通过Net sh命令设置辅助私网IP，将skipassource设置为true。

具体命令如下所示：

```
Netsh int ipv4 add address <Interface> <IP Addr> [<Netmask>] [skipassource=true]
```

参数说明如下所示。

辅助私网IP信息	说明	举例
<Interface>	辅助私网IP的网络接口	'以太网'
<IP Addr>	辅助私网IP地址	192.168.0.100
<Netmask>	辅助私网IP的掩码	255.255.255.0

通过Net sh设置辅助私网IP的示例如下：

```
Netsh int ipv4 add address '以太网' 192.168.0.100 255.255.255.0 skipassource=true
```

云盾是否有屏蔽IP地址的功能？

目前，云盾没有单独屏蔽IP的功能。

- 如果您使用的ECS实例是Windows系统，您可以在IIS中屏蔽单独IP地址的访问。
- 如果您使用的ECS实例是Linux系统，您可以参见[ECS Linux 系统屏蔽某个IP的访问](#)。

云服务器ECS出现了异地登录怎么办？

如果出现异地登录，解决办法如下。

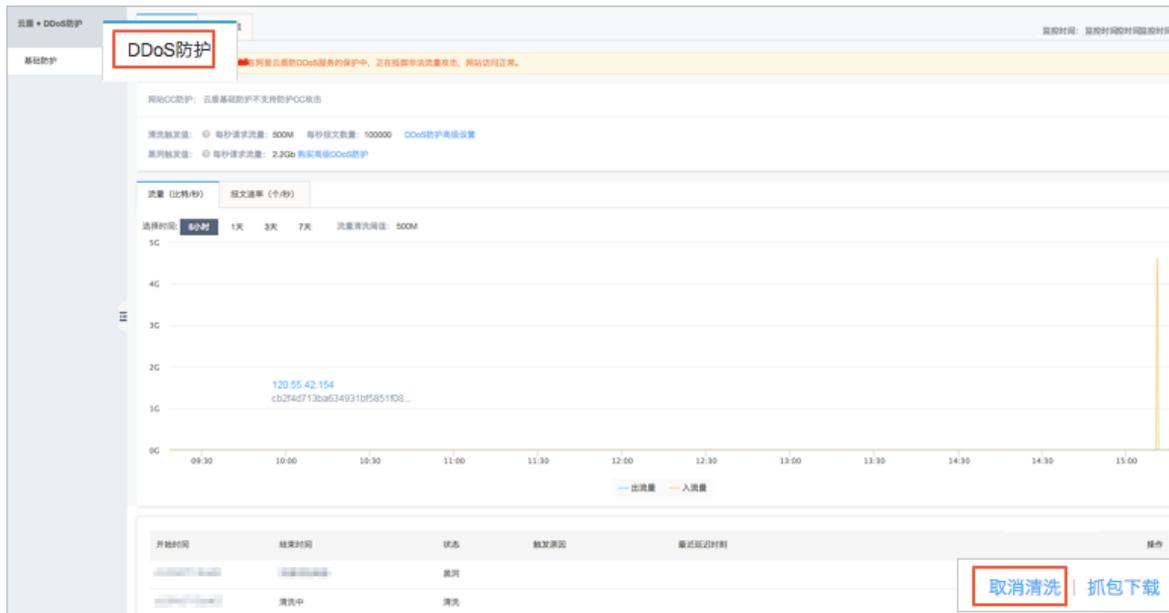
1. 确认异地登录的时间点，是否是自己或者其他管理员登录。
2. 如果不是合法管理员登录的，可执行以下操作。
 - i. 立即[重置密码](#)。
 - ii. 排查是否被病毒攻击，请参见[云服务器ECS中病毒/木马了怎么办](#)。
 - iii. 使用安全组功能设置[只允许特定的IP登录](#)。

什么是流量清洗？

清洗是指实时监控进入云服务器ECS的数据流量，及时发现包括DDoS攻击在内的异常流量。云服务器ECS默认提供DDoS攻击防御功能。当出现网络攻击时，系统自动检测到网络攻击，并为ECS实例清洗异常流量。在不影响正常业务的前提下，清洗掉异常流量，可以将可疑流量从原始网络路径中重定向到净化产品上，识别和剥离恶意流量，转发合法流量到原网络中以及目标系统。

云服务器ECS怎么取消流量清洗？

1. 登录[云盾DDoS基础防护管理控制台](#)
2. 选择云产品，找到您想要取消的正在清洗中的IP，单击[查看详情](#)。
3. 单击[取消清洗](#)。



怎么申请云服务器ECS反向解析？

反向解析常用于邮件服务。启动该功能后，可以拒绝接收所有没有注册域名的地址发来的信息。多数垃圾邮件发送者使用动态分配或者没有注册域名的IP地址发送垃圾邮件，逃避追踪。您可以在邮件服务器上拒绝接收来自没有域名的站点发来的信息，降低垃圾邮件的数量。

您可以[提交工单](#)申请反向解析。建议您在工单中注明ECS实例所在的地域、公网IP地址和注册域名，提高流程效率。申请成功后，您可以使用dig命令查看是否生效。例如。

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

返回以下类似信息说明配置已生效。

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

一个IP地址是否允许指向多个反向解析域名？

不允许，只支持一个反向解析域名。例如，121.196.255.**不可以同时设置mail.abc.com、mail.ospf.com、mail.zebra.com等多个反向解析域名。

创建实例后，我可以更换公网IP（IPv4）地址吗？

实例创建六小时内，您可以更换公网IP地址。详细步骤，请参见[更换公网IP地址](#)。

超过六小时后，根据实例的网络类型有不同区别。

- 专有网络类型ECS实例：支持将公网IP转换成弹性公网EIP。详细步骤请参见[专有网络类型ECS公网IP转为弹性公网IP](#)。
- 经典网络类型ECS实例：不支持。但是您可以在释放实例时，将公网IP转换成弹性公网EIP，详细步骤请参见[经典网络类型ECS公网IP转为弹性公网IP](#)。

为什么在ECS管理控制台上，我看不到更换公网IP选项？

- 实例创建六小时内：如果实例的计费方式为按量付费、网络类型为专有网络，在停止实例时需要启用普通停机模式。如果启用节省停机模式，在控制台操作界面无法看到[更换公网IP](#)选项。
- 实例创建六小时后：不支持直接更换公网IP地址，因此无法看到[更换公网IP](#)选项。

除了更换公网IP地址，我还可以更换私网IP地址吗？

- 专有网络类型ECS实例：可以。详细步骤，请参见[修改私有IP地址](#)。
- 经典网络类型ECS实例：不可以。

如果在创建实例时未分配公网IP（IPv4）地址，实例创建成功后怎么获得公网IP地址？

- 申请和绑定弹性公网IP，具体操作，请参见[弹性公网IP文档申请EIP](#)。
- 变更实例公网带宽，从而分配一个固定公网IP地址。包年包月实例的更多信息，请参见[升降配方式概述](#)，按量付费实例的更多信息，请参见[按量付费实例修改带宽](#)。

什么是BGP机房？

BGP（边界网关协议）主要用于互联网AS（自治系统）之间的互联，主要功能在于控制路由的传播和优选路由。

中国网通、中国电信、中国铁通和一些大的民营IDC运营商都具有AS号，全国各大网络运营商多数均通过BGP协议与自身的AS号实现多线互联。

使用BGP方案实现多线路互联时，需要为IDC在CNNIC（中国互联网信息中心）或APNIC（亚太网络信息中心）申请IP地址段和AS号，然后通过BGP协议将此段IP地址广播到其它网络运营商的网络中。使用BGP协议互联后，网络运营商的所有骨干路由设备将会比较到IDC机房IP段的路由，优选更佳的路由，以保证不同网络运营商用户的高速访问。

什么是广域网和局域网？

- 广域网：又称外网、公网。是连接不同地区局域网或城域网计算机通信的远程网。通常跨越很大的物理范围，所覆盖的范围从几十公里到几千公里，它能连接多个地区、城市和国家，或横跨几个洲并能提供远距离通信，形成国际性的远程网络。广域网并不等同于互联网。
- 局域网：又称内网。是指在某一区域内由多台计算机互联的计算机组。局域网可以实现文件管理、应用软件共享、打印机共享、工作组内的日程安排、电子邮件和传真通信服务等功能。局域网是封闭型的，可以由办公室内的两台计算机组成，也可以由一个公司内的上千台计算机组成。在阿里云，相同地域下的ECS实例可以采用同类型网络配置实现内网互通，不同地域的ECS实例之间的内网隔离。

什么是CIDR？

CIDR（Classless Inter-Domain Routing）是互联网中一种新的寻址方式，与传统的A类、B类和C类寻址模式相比，CIDR在IP地址分配方面更为高效。CIDR采用斜线记法，表示为：IP地址/网络ID的位数。

- 示例一：CIDR格式换算为IP地址网段

例如10.0.0.0/8，换算为32位二进制地址：00001010.00000000.00000000.00000000。其中/8表示8位网络ID，即32位二进制地址中前8位是固定不变的，对应网段为：

00001010.00000000.00000000.00000000~00001010.11111111.11111111.11111111。则换算为十进制后，10.0.0.0/8表示：子网掩码为255.0.0.0，对应网段为10.0.0.0~10.255.255.255。

- 示例二：IP地址网段换算为CIDR格式

例如192.168.0.0~192.168.31.255，后两段IP换算为二进制地址：00000000.00000000~00011111.11111111，可以得出前19位（8*2+3）是固定不变的，则换算为CIDR格式后，表示为：192.168.0.0/19。

如何表示子网掩码？

子网掩码有两种表示方法：

- 点分十进制表示法。

例如，A类网络缺省子网掩码：255.0.0.0

- 在IP地址后加上斜杠（/）以及1~32的掩码范围，其中1~32表示子网掩码中网络标识位的长度。

例如，192.168.0.3/24。

如何划分子网？

子网划分的最佳实践，请参见[网络规划](#)。

如何查看资源的限额？

查看资源的使用限制和限额，请参见[使用限制](#)。