

弹性云服务器

用户指南

文档版本 01
发布日期 2025-06-13



版权所有 © 华为云计算技术有限公司 2025。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目 录

1 通过 IAM 授予使用 ECS 的权限..... 1

1.1 创建用户并授权使用 ECS..... 1

1.2 ECS 自定义策略..... 2

2 实例.....5

2.1 ECS 实例概述..... 5

2.2 选择 ECS 计费模式.....7

2.2.1 包年/包月计费.....7

2.2.2 按需计费..... 7

2.2.3 竞价计费..... 8

2.2.3.1 竞价计费模式概述..... 8

2.2.3.2 竞价计费型实例..... 10

2.2.3.3 竞享计费型实例..... 13

2.2.4 按需转包年/包月..... 18

2.2.5 包年/包月转按需..... 20

2.3 购买 ECS.....23

2.3.1 ECS 购买方式导航.....23

2.3.2 快速购买 ECS..... 24

2.3.3 自定义购买 ECS..... 28

2.3.4 购买竞价计费型 ECS..... 57

2.3.5 购买竞享计费型 ECS..... 59

2.3.6 通过私有镜像购买 ECS..... 62

2.3.7 通过智能购买助手购买 ECS..... 64

2.3.8 通过规格选型引导购买 ECS..... 68

2.3.9 通过共享 VPC 购买 ECS..... 71

2.3.10 购买相同配置 ECS..... 72

2.4 登录 Windows ECS..... 73

2.4.1 Windows ECS 登录方式概述..... 73

2.4.2 通过控制台 VNC 登录 Windows ECS..... 74

2.4.3 通过 RDP 文件登录 Windows ECS..... 76

2.4.4 通过本地 Windows 主机登录 Windows ECS..... 78

2.4.5 通过本地 Linux 主机登录 Windows ECS..... 85

2.4.6 通过本地 macOS 主机登录 Windows ECS..... 87

2.4.7 通过移动设备登录 Windows ECS..... 90

文档版本 01 (2025-06-13)

版权所有 © 华为云计算技术有限公司

ii

2.5 登录 Linux ECS.....	95
2.5.1 Linux ECS 登录方式概述.....	95
2.5.2 通过 CloudShell 登录 Linux ECS.....	96
2.5.3 通过 VNC 登录 Linux ECS.....	101
2.5.4 通过 SSH 密钥方式登录 Linux ECS.....	105
2.5.5 通过 SSH 密码方式登录 Linux ECS.....	111
2.5.6 通过 macOS 主机登录 Linux ECS.....	113
2.5.7 通过移动设备登录 Linux ECS.....	114
2.5.8 通过华为云 APP 登录 Linux ECS.....	126
2.6 管理 GPU 加速型 ECS 的 GPU 驱动.....	130
2.6.1 GPU 驱动概述.....	130
2.6.2 Tesla 驱动及 CUDA 工具包获取方式.....	131
2.6.3 （推荐）自动安装 GPU 加速型 ECS 的 GPU 驱动（Linux）.....	133
2.6.4 （推荐）自动安装 GPU 加速型 ECS 的 GPU 驱动（Windows）.....	138
2.6.5 手动安装 GPU 加速型 ECS 的 GRID 驱动.....	143
2.6.6 手动安装 GPU 加速型 ECS 的 Tesla 驱动.....	157
2.6.7 卸载 GPU 加速型 ECS 的 GPU 驱动.....	171
2.7 管理 ECS 配置信息.....	175
2.7.1 更改时区.....	175
2.7.2 开启/关闭 ECS 超线程.....	178
2.7.3 使用实例自定义数据和元数据.....	181
2.7.3.1 通过元数据获取 ECS 基本信息.....	181
2.7.3.2 通过实例自定义数据配置 ECS 实例.....	191
2.7.3.3 验证实例身份文档签名.....	198
2.7.4 修改 ECS 主机名（hostname）.....	200
2.7.5 修改 ECS 名称.....	204
2.7.6 将 ECS 迁移至专属主机.....	204
2.7.7 跨可用区迁移 ECS.....	205
2.7.8 管理云服务器组.....	207
2.7.9 配置同一 VPC 内 ECS 通过主机名进行通信.....	210
2.7.10 启、停弹性云服务器.....	211
2.8 变更 ECS 规格（vCPU 和内存）.....	215
2.8.1 变更单台 ECS 规格.....	215
2.8.2 批量变更多台 ECS 规格.....	219
2.8.3 通过性能助手变更 ECS 规格.....	224
2.8.4 XEN 实例变更为 KVM 实例（Windows）.....	226
2.8.5 XEN 实例变更为 KVM 实例（Linux-自动配置）.....	232
2.8.6 XEN 实例变更为 KVM 实例（Linux-手动配置）.....	237
2.8.7 XEN 实例变更为 KVM 实例（Linux-批量自动配置）.....	242
2.8.8 KVM 实例变更为 QingTian 实例（Windows）.....	248
2.8.9 KVM 实例变更为 QingTian 实例（Linux）.....	252
2.9 变更 ECS 操作系统.....	256

2.9.1 重装操作系统.....	256
2.9.2 切换操作系统.....	257
2.10 查看 ECS 信息.....	262
2.10.1 查看 ECS 创建状态.....	262
2.10.2 查看 ECS 失败任务.....	262
2.10.3 查看 ECS 详细信息（列表视图）.....	263
2.10.4 查看 ECS 详细信息（精简视图）.....	265
2.10.5 导出 ECS 列表信息.....	266
2.10.6 搜索 ECS（旧版）.....	267
2.10.7 搜索 ECS.....	275
3 回收站管理（公测）.....	283
3.1 回收站概述.....	283
3.2 开启回收站.....	289
3.3 关闭回收站.....	290
3.4 配置回收站策略.....	290
3.5 恢复回收站中的云服务器.....	291
3.6 销毁回收站中的云服务器.....	292
3.7 导出回收站列表信息.....	292
4 镜像管理.....	294
4.1 镜像概述.....	294
4.2 创建镜像.....	296
5 磁盘管理.....	298
5.1 ECS 磁盘概述.....	298
5.2 为 ECS 新增磁盘.....	300
5.3 为 ECS 挂载磁盘.....	302
5.4 初始化数据盘.....	304
5.5 添加“包年/包月”磁盘.....	306
5.6 在线卸载磁盘.....	307
5.7 扩容云硬盘.....	309
5.8 扩容本地盘.....	312
6 弹性网卡管理.....	314
6.1 弹性网卡概述.....	314
6.2 绑定弹性网卡.....	315
6.3 解绑弹性网卡.....	317
6.4 切换虚拟私有云.....	318
6.5 修改私有 IP 地址.....	321
6.6 管理虚拟 IP 地址.....	321
6.7 开启网卡多队列功能.....	327
6.8 开启网卡 IPv6 功能.....	332
6.9 动态获取 IPv6 地址.....	334
6.10 委托授权云运维中心访问 ECS.....	352

7 弹性公网 IP 管理	354
7.1 弹性公网 IP 概述	354
7.2 绑定弹性公网 IP	355
7.3 解绑弹性公网 IP	356
7.4 更换弹性公网 IP	357
7.5 修改弹性公网 IP 的带宽	358
7.6 无公网 IP 的弹性云服务器访问 Internet	359
8 安全管理	363
8.1 提升云服务器安全性方法概述	363
8.2 安全组	370
8.2.1 安全组概述	370
8.2.2 默认安全组和规则	378
8.2.3 安全组配置示例	382
8.2.4 创建安全组	387
8.2.5 配置安全组规则	392
8.2.6 更改安全组	403
8.2.7 加入安全组	406
8.2.8 移出安全组	409
8.3 主机安全	411
8.4 云堡垒机	415
8.5 管理项目和企业项目	418
8.6 敏感操作保护	419
9 备份管理	423
9.1 云备份概述	423
9.2 备份弹性云服务器	429
10 密码和密钥对管理	433
10.1 重置 ECS 密码	433
10.1.1 密码使用场景介绍	433
10.1.2 在控制台重置 ECS 密码	434
10.2 管理 ECS 一键式重置密码插件	440
10.2.1 获取 ECS 一键式重置密码插件	440
10.2.2 安装单台 ECS 的一键式重置密码插件（单台操作）	446
10.2.3 更新单台 ECS 的一键式重置密码插件（单台操作）	452
10.2.4 通过 AOM 批量更新 ECS 一键式重置密码插件	456
10.2.5 通过脚本批量更新 ECS 一键式重置密码插件（Linux）	467
10.2.6 通过脚本批量更新 ECS 一键式重置密码插件（Windows）	470
10.3 管理 ECS 密钥对	474
10.3.1 密钥对使用场景介绍	474
10.3.2 （推荐）通过管理控制台创建密钥对	475
10.3.3 通过 PuTTY Key Generator 工具创建密钥对	476
10.3.4 导入密钥对	480

10.3.5 获取和清除云服务器密码（Windows）	482
10.3.5.1 获取 Windows 弹性云服务器的密码	482
10.3.5.2 清除 Windows 弹性云服务器的密码	484
11 启动模板管理	486
11.1 启动模板概述	486
11.2 创建启动模板	486
11.3 管理启动模板	487
12 智能购买组管理	489
12.1 智能购买组概述	489
12.2 创建智能购买组	490
12.3 管理智能购买组	492
13 事件管理	494
13.1 事件概述	494
13.2 查询事件	497
13.3 响应事件	498
13.3.1 响应实例重部署事件	498
13.3.2 响应本地盘换盘事件	503
13.3.3 响应系统维护事件	510
13.4 换盘预处理	513
13.4.1 本地盘换盘预处理（磁盘增强型实例）	513
13.4.2 本地盘换盘预处理（裸金属类型实例）	516
13.5 实例重部署预处理	519
14 操作系统 dump 管理	520
14.1 配置操作系统 dump	520
14.2 查看操作系统 dump	527
15 自助运维管理	529
15.1 配置 ECS 自助运维自定义策略	529
15.2 为 ECS 安装 UniAgent	531
15.3 为 ECS 配置定时运维任务	533
15.4 免登录 ECS 发送远程命令	537
15.5 深度诊断 ECS	542
16 资源与标签	547
16.1 标签管理	547
16.1.1 标签概述	547
16.1.2 添加标签	549
16.1.3 使用标签检索资源	551
16.1.4 删除标签	552
16.2 配额调整	554
17 使用 CES 监控 ECS	556
17.1 监控弹性云服务器	556

17.2 弹性云服务器支持的基础监控指标.....	557
17.3 弹性云服务器支持的操作系统监控指标（安装 Agent）.....	564
17.4 弹性云服务器支持的进程监控指标（安装 Agent）.....	610
17.5 异构类实例安装支持对应监控的 CES Agent（Linux）.....	615
17.6 异构类实例安装支持对应监控的 CES Agent（Windows）.....	622
17.7 设置告警规则.....	625
17.8 查看监控指标.....	626
18 使用 CTS 审计 ECS 操作事件.....	628
18.1 ECS 支持云审计的关键操作.....	628
18.2 查询 ECS 审计事件.....	630
19 QingTian Enclave 管理.....	634
19.1 QingTian Enclave 简介.....	634
19.1.1 什么是 QingTian Enclave.....	634
19.1.2 QingTian Enclave 概念.....	636
19.2 快速入门.....	638
19.3 典型使用案例.....	642
19.3.1 工作流程.....	642
19.3.2 构建 QingTian Enclave 镜像.....	644
19.3.3 启动 QingTian Enclave.....	645
19.4 密码学证明.....	646
19.4.1 PCR 简介.....	646
19.4.2 证明文档.....	648
19.4.3 文档签名验证.....	648
19.4.4 结合华为云 KMS 服务.....	649
19.5 QingTian Enclave 应用开发.....	650
19.5.1 Linux 系统上 QingTian Enclave 应用的开发.....	650
19.5.2 QingTian Enclave 网络代理工具.....	660
19.5.3 QingTian Enclave 日志转发工具.....	665
19.6 QingTian CLI（qt CLI）.....	671
19.6.1 安装 qt CLI.....	671
19.6.2 qt-enclave-env 工具介绍.....	671
19.6.3 qt enclave 子命令介绍.....	671
19.7 错误码.....	676
19.8 常见问题.....	679
19.8.1 通用类.....	679
19.8.2 开发部署类.....	681

1 通过 IAM 授予使用 ECS 的权限

1.1 创建用户并授权使用 ECS

如果您需要对您所拥有的ECS进行精细的权限管理，您可以使用[统一身份认证服务](#)（Identity and Access Management，简称IAM），通过IAM，您可以：

- 根据企业的业务组织，在您的华为账号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用ECS资源。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将ECS资源委托给更专业、高效的其他华为账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

如果华为账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用ECS服务的其他功能。

本章节为您介绍对用户授权的方法，操作流程如[示例流程](#)所示。

前提条件

给用户组授权之前，请您了解用户组可以添加的ECS系统策略，并结合实际需求进行选择。

ECS支持的系统策略及策略间的对比，请参见：[ECS系统策略](#)。若您需要对除ECS之外的其他服务授权，IAM支持服务的所有策略请参见[系统权限](#)。

示例流程

图 1-1 给用户授权 ECS 权限流程



1. 创建用户组并授权

在IAM控制台创建用户组，并授予弹性云服务只读权限“ECS ReadOnlyAccess”。

2. 创建用户并加入用户组

在IAM控制台创建用户，并将其加入1中创建的用户组。

3. 用户登录并验证权限

新创建的用户登录控制台，切换至授权区域，验证弹性云服务的只读权限。

- 在“服务列表”中选择弹性云服务器，进入ECS主界面，单击右上角“购买弹性云服务器”，尝试购买弹性云服务器，如果无法购买弹性云服务器（假设当前权限仅包含ECSReadOnlyAccess），表示“ECSReadOnlyAccess”已生效。
- 在“服务列表”中选择除弹性云服务器外（假设当前策略仅包含ECSReadOnlyAccess）的任一服务，若提示权限不足，表示“ECSReadOnlyAccess”已生效。

1.2 ECS 自定义策略

如果系统预置的ECS权限，不满足您的授权要求，可以创建自定义策略。自定义策略中可以添加的授权项（Action）请参考《ECS API参考》中“策略及授权项说明”章节。

目前华为云支持以下两种方式创建自定义策略：

- 可视化视图创建自定义策略：无需了解策略语法，按可视化视图导航栏选择云服务、操作、资源、条件等策略内容，可自动生成策略。

- JSON视图创建自定义策略：可以在选择策略模板后，根据具体需求编辑策略内容；也可以直接在编辑框内编写JSON格式的策略内容。

具体创建步骤请参见：[创建自定义策略](#)。本章为您介绍常用的ECS自定义策略样例。

ECS 自定义策略样例

- 示例1：授权仅允许用户批量开机、关机、重启云服务器

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ecs:cloudServerFlavors:get",
        "ecs:cloudServers:reboot",
        "ecs:cloudServers:start",
        "ecs:cloudServers:get",
        "ecs:cloudServers:list",
        "ecs:cloudServers:stop"
      ]
    }
  ]
}
```

- 示例2：授权仅允许用户批量关闭云服务器、删除云服务器

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ecs:cloudServers:get",
        "ecs:cloudServers:delete",
        "ecs:cloudServers:list",
        "ecs:cloudServers:stop"
      ]
    }
  ]
}
```

- 示例3：授权仅允许用户通过VNC进行登录

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ecs:cloudServerFlavors:get",
        "ecs:cloudServers:vnc",
        "ecs:cloudServers:get",
        "ecs:cloudServers:list"
      ]
    }
  ]
}
```

- 示例4：授权拒绝用户删除云服务器

拒绝策略需要同时配合其他策略使用，否则没有实际作用。用户被授予的策略中，一个授权项的作用如果同时存在Allow和Deny，则遵循Deny优先。

如果您给用户授予ECSFullAccess的系统策略，但不希望用户拥有ECSFullAccess中定义的删除云服务器权限，您可以创建一条拒绝删除云服务的自定义策略，然后将ECSFullAccess和拒绝策略授予用户，根据Deny优先原则，则用户可以对ECS执行除了删除云服务器外的所有操作。拒绝策略示例如下：

```
{
  "Version": "1.1",
```

```
"Statement": [  
  {  
    "Effect": "Deny",  
    "Action": [  
      "ecs:cloudServers:delete"  
    ]  
  }  
]
```


2 实例

2.1 ECS 实例概述

实例概述

实例即弹性云服务器，是由CPU、内存、操作系统、云硬盘组成的基础计算组件。

弹性云服务器创建成功后，您就可以像使用自己的本地PC或物理服务器一样，在云上使用弹性云服务器，打造一个高效、可靠、安全的计算环境。弹性云服务器的开通是自助完成的，您只需要指定CPU、内存、操作系统、规格、登录鉴权方式即可，同时也可以根据您的需求随时调整您的弹性云服务器规格。

云平台提供了多种实例类型供您选择，不同类型的实例可以提供不同的计算能力和存储能力。同一实例类型下可以根据CPU和内存的配置选择不同的实例规格。

- 关于实例类型的信息，请参考[实例类型](#)。
- 更多实例规格清单请参考[规格清单（x86）](#)和[规格清单（鲲鹏）](#)。

实例配置

ECS的配置信息包含CPU、内存、操作系统、存储容量、网络等基础资源。

表 2-1 实例配置

配置信息	说明	相关参考
规格	弹性云服务器提供x86和鲲鹏架构的多种类型的实例规格。 通过规格定义实例的vCPU个数、内存大小、内网基准/最大带宽、可达到的最大收发包能力、是否支持IPv6等配置。	• 规格清单（x86） • 规格清单（鲲鹏）

配置信息	说明	相关参考
镜像	镜像包含了ECS运行所必需的操作系统、应用软件、初始化应用程序等。 镜像分为公共镜像、私有镜像、共享镜像、市场镜像。	镜像概述
存储	ECS通过挂载的云盘和本地盘提供存储能力： - 云盘：通过专属分布式存储池或云硬盘创建，支持作为系统盘和数据盘。 - 本地盘：部分规格自带本地盘，仅支持作为数据盘。	ECS磁盘概述
网络	虚拟私有云为ECS构建隔离的、用户自主配置和管理的虚拟网络环境，可以在VPC中定义网卡、私网IP地址段、安全组等网络特性。 不同VPC中的ECS网络默认不互通。	弹性网卡概述

实例选型

表 2-2 实例选型

选型方式	说明	相关参考
规格类型选型	提供按CPU架构类型、vCPUs个数和内存大小、规格名称模糊搜索以及实例类型的选型方式。 适用于实例类型，想要根据具体配置要求进行规格选型的用户。	自定义购买ECS
业务场景选型	提供按Web应用、网站应用/电商、游戏、数据库等业务场景以及不同场景业务量的推荐规格。 适用于有明确业务场景需求，想要根据业务场景、业务量等参考指标进行规格选型的用户。	

实例变更

ECS创建成功后，您可以根据业务需要变更ECS的vCPUs和内存、操作系统、存储和带宽。

- 变更vCPUs和内存：[变更单台ECS规格](#)。
- 变更操作系统：[切换操作系统](#)。

- 变更存储：[为ECS新增磁盘、扩容云硬盘](#)。
- 变更带宽：[修改弹性公网IP的带宽](#)。

2.2 选择 ECS 计费模式

2.2.1 包年/包月计费

什么是包年/包月

包年/包月的计费模式是一种预付费方式，按订单的购买周期计费，适用于可预估资源使用周期的场景，价格比按需计费模式更优惠。

更多计费相关信息，请参见[包年/包月](#)。

包年/包月计费模式弹性云服务器使用说明

1. “包年/包月”的弹性云服务器创建后不能删除，如需停止使用，请在弹性云服务器列表页，单击“操作”列下的“更多 > 退订”，执行退订操作。
2. 在创建弹性云服务器时购买的系统盘，卸载后，如果继续作为系统盘使用，则只能挂载给原弹性云服务器，不能挂载其他弹性云服务器的系统盘作为自己的系统盘；如果作为数据盘使用，则可以挂载给任意弹性云服务器。
3. 在创建弹性云服务器时购买的数据盘，卸载后，如果需要重新挂载，则只能挂载给原弹性云服务器作为数据盘使用。

适用包年/包月的资源

包年/包月的资源包括：

- ECS实例，包括vCPU和内存。
 - 镜像，包括预付费的市场镜像。
 - 购买云服务器时同时购买的云硬盘价格，包括系统盘和数据盘。
 - 购买云服务器时同时购买的带宽价格。
- IP和固定带宽统一计费，不单独计费，计费标准参考按固定带宽计费。

如果您要创建一个包年/包月的弹性云服务器，配置费用即包括了以上几种资源的费用。

您可以使用ECS[价格计算器](#)快速了解弹性云服务器配置费用。

2.2.2 按需计费

什么是按需计费

按需付费是后付费方式，可以随时开通/删除弹性云服务器，支持秒级计费，系统会根据云服务器的实际使用情况每小时出账单，并从账户余额里扣款。

更多计费相关信息，请参见[按需计费](#)。

说明

按需付费的弹性云服务器关机再次开机时，可能会出现由于资源不足引起的启动失败，请过一段时间再次启动，或更改弹性云服务器规格。

保证金

购买按需计费的GPU加速型、AI加速型、鲲鹏AI加速型等规格的弹性云服务器实例时，华为云根据用户等级和历史使用情况可能会冻结一定的保证金，资源释放时自动解冻保证金。更多信息，请参见[保证金](#)。

计费样例

ECS的“按需计费”是秒级计费，ECS产品价格详情中标出了每小时价格，您可以将每小时价格除以3600，即得到每秒价格。

示例，某一按需实例价格为0.68元/小时，购买一台按需实例根据实际使用时长、按秒计费。

- 使用30分钟，根据实际使用时长按秒计费： $(0.68/3600) \times 30 \times 60 = 0.34$ 元
- 使用1小时30分钟，根据实际使用时长按秒计费： $(0.68/3600) \times 90 \times 60 = 1.02$ 元

适用按需计费的资源

按需计费的ECS资源包括：

- ECS实例，包括vCPU核数和内存容量。
- 镜像，包括市场镜像，以及来源于市场镜像的共享镜像或自定义镜像。
- 购买云服务器时同时购买的云硬盘价格，包括系统盘和数据盘。
- 购买云服务器时同时购买的带宽价格。

您可以使用ECS[价格计算器](#)快速了解弹性云服务器配置费用。

2.2.3 竞价计费

2.2.3.1 竞价计费模式概述

什么是竞价计费模式？

华为云将可用的计算资源，按照一定折扣进行售卖，其价格随市场供需关系实时变化，这种打折销售、价格实时变化的计费模式称为“竞价计费”。

在该计费模式下，您可以以折扣价购买并使用弹性云服务器，性能与常规云服务器无异。但是当库存资源不足，或市场价格上浮超过您的预期价格时（竞价计费型实例），系统会自动释放您的云服务器资源，对这些折扣售卖的弹性云服务器进行中断回收。与“按需计费”和“包年/包月”方式购买的弹性云服务器相比，在提供同等性能的前提下，竞价计费型实例可提供超低折扣，降低用云成本。

- 采用竞价模式购买的弹性云服务器，称之为“竞价计费型实例”，简称“竞价实例”。
- 购买竞价实例需设定“价格上限”。您愿意为云服务器支付的最高价格。该上限值需大于等于当前的市场价格，小于等于按需计费的价格。当库存资源紧张或市

场价格高于您设置的价格上限时，竞价实例将被中断回收，请提前做好数据备份。

- 采用竞享模式购买的弹性云服务器，称之为“竞享计费型实例”，简称“竞享实例”。
购买竞享实例需选择“保障周期”和“保障周期数量”。保障周期是购买竞享实例的最小单位时间，保障周期不同价格不同。在保障周期内由云平台中断竞享实例，当前周期不计费。在保障周期内用户删除竞享实例，当前周期按使用时长计费。

计费规则

请认真阅读竞价计费模式的计费规则，详情请参见“[竞价计费（竞价模式）](#)”和“[竞价计费（竞享模式）](#)”。

竞价实例与竞享实例对比说明

表 2-3 竞价实例与竞享实例对比说明

竞价类型	竞价模式	竞享模式
购买条件	购买竞价实例需设定“价格上限”，即报价。 • 当“报价 ≥ 市场价格”且库存资源充足时，购买竞价计费型实例成功。系统将按当前市场价格进行计费。 • 当“报价 < 市场价格”时，无法购买竞价计费型实例。	购买竞享实例需选择“保障周期”和“保障周期数量”。保障周期是购买竞享实例的最小单位时间，保障周期不同价格不同。
付费方式	后付费 账单起始价格按用户购买时间的市场价格计算，后续按照整点时间的市场价格计费。	后付费 按用户使用时长和选择的保障周期对应价格计费，实例释放后出所有整点账单。 且使用期间进行关机等操作，仍然计费。
计费周期	秒级计费，按小时结算。	秒级计费，按小时结算。

关机计费	- 普通实例（不含本地盘的实例、不含FPGA卡的实例、非裸金属实例）关机后，基础资源（包括vCPU、内存、镜像、GPU）不计费。其他绑定资源（云硬盘、弹性公网IP、带宽）正常计费。 - 特殊实例（含本地盘的实例、含FPGA卡的实例、裸金属实例），关机后仍然正常收费，同时vCPU和内存等资源也会保留。如需停止计费，请删除实例。	关机后仍然计费。如需停止计费，请删除实例。
更改计费模式	不支持转换为“按需计费”和“包年/包月”计费模式。	不支持转换为“按需计费”和“包年/包月”计费模式。
变更规格	不支持变更规格。	不支持变更规格。
卸载系统盘	不支持卸载系统盘。	不支持卸载系统盘。
中断回收	- 市场价格高于您的报价 - 库存资源不足 - 主动释放	- 库存资源不足 - 主动释放
应用场景	竞价计费型实例存在中断机制，实例生命周期不可控，请勿使用竞价计费型实例运行需长时间作业、或稳定性要求极高的服务。 适用场景：图像渲染、无状态Web服务、基因测序、离线分析、函数计算、批量计算、样本分析、CI/CD与测试等。	

2.2.3.2 竞价计费型实例

什么是竞价计费型实例？

华为云将可用的计算资源，按照一定折扣进行售卖，其价格随市场供需关系实时变化，这种打折销售、价格实时变化的计费模式称为“竞价计费”。

采用竞价模式购买的弹性云服务器，称之为“竞价计费型实例”，简称“竞价实例”。

在该计费模式下，您可以以折扣价购买并使用弹性云服务器，性能与常规云服务器无异。但是当库存资源不足，或市场价格上浮、并超过您的预期价格时，系统会自动释放您的云服务器资源，对这些折扣售卖的弹性云服务器进行中断回收。与“按需计费”和“包年/包月”方式购买的弹性云服务器相比，在提供同等性能的前提下，竞价计费型实例可提供超低折扣，降低用云成本。

工作原理

不同时期，市场对某一规格的云服务器供需情况不同，从而引起市场价格的波动。您可以在市场价格较低时，购买并使用竞价计费型实例，降低计算成本。

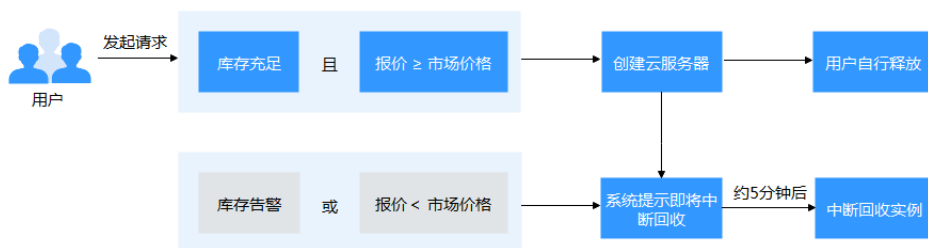
购买竞价计费型实例时，您需要为指定规格的弹性云服务器设定价格上限，即报价。该报价是您愿意为该弹性云服务器支付的最高价格，报价越高，购买成功的机会越大。

- 当“报价 $\geq$ 市场价格”且库存资源充足时，购买竞价计费型实例成功。系统将按当前市场价格进行计费。
- 当“报价 $<$ 市场价格”时，无法购买竞价计费型实例。

竞价计费型实例购买成功后，您可以像使用其他计费模式的云服务器一样，登录并使用弹性云服务器，没有任何差别。但是，系统会定期比价，并检查资源池库存情况：

- 当“报价 $\geq$ 市场价格”且库存资源充足时，您可以继续持有并使用弹性云服务器。
- 当“报价 $<$ 市场价格”或库存资源不足时，系统发出即将释放云服务器资源的通知，并在约5分钟后自动删除弹性云服务器。

图 2-1 竞价计费型实例生命周期



应用场景

- 适用场景

如下业务适合使用竞价计费型实例策略：图像渲染、无状态Web服务、基因测序、离线分析、函数计算、批量计算、样本分析、CI/CD与测试等。

说明

当市场价格高于您的报价或者库存资源不足时，竞价计费型实例会被中断回收，请务必做好数据备份工作。

- 不适用场景

为避免中断回收机制对业务带来影响，对于需要长时间作业、或稳定性要求极高的服务，请勿采用竞价计费型实例策略。

使用须知

- 当前仅支持虚拟化类型为KVM的弹性云服务器使用竞价计费型实例策略。具体的规格支持清单，请以控制台显示的资源为准。
- 在不同可用区，同一规格的云服务器市场价格变化可能不同。
- 使用竞价计费型实例策略的弹性云服务器，不支持切换操作系统功能。
- 使用竞价计费型实例策略的弹性云服务器，不支持自动恢复功能。

- 使用竞价计费型实例策略的弹性云服务器，不支持变更规格。
- 不支持使用市场镜像创建竞价计费型实例。
- 竞价计费型实例不支持转换为“按需计费”和“包年/包月”计费模式。
- 竞价计费型实例不支持卸载系统盘。
- 竞价计费型实例在中断回收时：
 - 不允许使用该竞价计费型实例制作系统盘镜像和整机镜像，但允许使用该云服务器的数据盘制作数据盘镜像。
 - 不允许删除。
- 竞价计费型实例在中断回收时，数据盘和弹性公网IP默认不释放。请设置通知提醒，来决定是否释放关联的数据盘和弹性公网IP。具体方法，请参见“[购买竞价计费型实例](#)”。

计费规则

请认真阅读竞价计费型实例的计费规则，详情请参见“[竞价计费（竞价模式）](#)”。

计费样例

- **样例1：当市场价高于用户出价，竞价计费型实例被释放，根据用户实际使用时长、按秒计费，费用单价为成交时的市场价格。**
8: 30 市场价0.02元/小时，用户出价0.04元/小时，按照市场价格计费0.02元/小时
9: 00 市场价0.03元/小时
10: 00 市场价0.04元/小时
10: 30 市场价0.05元/小时，高于用户的出价，标记释放，提醒用户即将中断
用户共产生3个账单周期，实际扣费明细如下：
8: 30~9: 00 使用30分钟，按秒计费= $0.02/3600 \times 30 \times 60 = 0.01$ 元
9: 00~10: 00 使用1小时，按9:00起始成交价0.03元/小时，计费= $0.03 \text{元/小时} \times 1 \text{小时} = 0.03$ 元
10: 00~10: 30 使用30分钟，按秒计费= $0.04/3600 \times 30 \times 60 = 0.02$ 元
合计0.06元，实际使用时长2小时。
- **样例2：竞价计费型实例资源不足的情况下，竞价计费型实例被释放，根据用户实际使用时长、按秒计费，费用单价为成交时的市场价格。**
8: 30 市场价0.02元/小时，用户出价0.06元/小时，按照市场价格计费0.02元/小时
9: 00 市场价0.03元/小时
10: 00 市场价0.04元/小时
10: 30 市场价0.05元/小时，虽然市场价低于用户出价，但由于竞价计费型实例资源不足，标记释放，提醒用户即将中断
用户共产生3个账单周期，实际扣费明细如下：
8: 30~9: 00 使用30分钟，按秒计费= $0.02/3600 \times 30 \times 60 = 0.01$ 元
9: 00~10: 00 使用1小时，按9:00起始成交价0.03元/小时，计费= $0.03 \text{元/小时} \times 1 \text{小时} = 0.03$ 元
10: 00~10: 30 使用30分钟，按秒计费= $0.04/3600 \times 30 \times 60 = 0.02$ 元
合计0.06元，实际使用时长2小时。

购买竞价计费型实例

您可以通过控制台方式或调用API方式，购买竞价计费型实例。

- 控制台方式，请参见“[购买竞价计费型实例](#)”。
- API方式，请参见《弹性云服务器API参考》的“[创建云服务器](#)”章节。

中断回收

华为云始终可能会中断您的竞价计费型实例，终止实例的使用。竞价计费型实例在中断回收时，不允许使用该竞价计费型实例制作镜像。

中断回收竞价计费型实例的可能原因包括：

- 市场价格高于您的报价
- 库存资源不足

说明

- 由于库存资源不足或者用户出价低于市场价导致的首小时内中断，竞价计费型实例不收费。
- 竞价计费型实例的第一个结算周期内（结算周期为自然小时）均按开机计费。
- 如果竞价计费型实例中断回收的5分钟内跨过了整点，那么整点后该竞价计费型实例按照市场价格计费。
- 开机过程中，竞价计费型实例每小时更新一次价格。重启或关机再开机后，竞价计费型实例以开机时的市场价格计费。

因此，请务必做好数据备份工作。系统会提前发出即将释放云服务器资源的通知，如需设置通知提醒，请参见“[购买竞价计费型实例](#)”。

常见问题

请参见[FAQ](#)。

2.2.3.3 竞享计费型实例

什么是竞享计费型实例？

竞享实例是竞价计费的一种新型售卖模式，其最核心的特点是超低价格和系统抢占机制，即您可以以较低折扣购买实例，但同时在系统资源不足等极端情况下系统可能会自动回收这些实例。其适用于各种无状态、容错或者灵活的应用场景。

采用竞享模式购买的弹性云服务器，称之为“竞享计费型实例”，简称“竞享实例”。

竞享实例目前支持华为云[通用计算增强型](#)，目前已经上线C6机型的多个规格，C6s、C3机型会陆续上线。

在该计费模式下，您可以以折扣价购买并使用弹性云服务器，性能与常规云服务器无异。但是当库存资源不足，系统会自动释放您的云服务器资源，对这些折扣售卖的弹性云服务器进行中断回收。与“按需计费”和“包年/包月”方式购买的弹性云服务器相比，在提供同等性能的前提下，竞享实例可提供超低折扣，降低用云成本。

工作原理

购买竞享实例时，需要选择保障周期（1-6小时），保障周期不同价格不同。保障周期是购买竞享实例的最小单位时间。在保障周期内由云平台中断竞享实例，当前周期不计费。在保障周期内用户删除竞享实例，当前周期按使用时长计费。

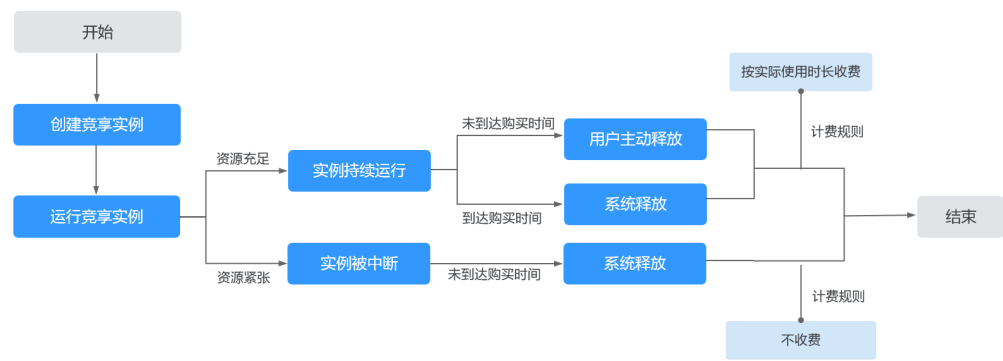
竞享实例购买成功后，当达到用户购买时长或库存资源不足时，实例将会进入“**中断回收中**”状态，随后释放。用户可以根据业务需要随时**主动释放实例**，实例释放后按用户实际使用时长收费。

华为云会尽可能保障竞享实例正常运行，但在极端情况下会中断释放该类实例，实例被中断时会**秒级释放**，请在使用竞享实例时做好备份策略。

在保障周期内由云平台中断竞享实例，当前周期不计费。在保障周期内用户主动释放实例，当前周期按使用时长计费。

一般情况下，竞享实例回收会优先选择使用时长较短的实例中断回收，尽可能降低对用户的业务损伤，但仍然建议您优化应用设计，保证在竞享实例被中断回收的情况下业务也可以正常工作。您可以尝试主动释放竞享实例，检测在竞享实例被中断回收的情况下应用工作是否正常。

图 2-2 竞享实例的生命周期



说明

在保障周期内由云平台中断竞享实例，当前周期不计费。在保障周期内用户主动释放实例，当前周期按使用时长计费。

应用场景

- 适用场景**
如下业务场景适合使用竞享实例：图像渲染、无状态Web服务、基因测序、离线分析、函数计算、批量计算、样本分析、CI/CD与测试等。
- 说明**
当达到用户购买时长或库存资源不足时，竞享实例会被中断回收，请务必做好数据备份工作。
- 不适用场景**
为避免中断回收机制对业务带来影响，对于需要长时间作业、或稳定性要求极高的服务，请勿使用竞享实例。

使用须知

- 竞享计费型实例目前支持通用计算增强型实例规格。
- 华为云尽可能保障竞享实例正常运行，但在系统资源不足等极端情况下会主动释放实例，请务必做好数据备份工作。
- 竞享计费型实例目前只支持部分区域及规格，请以购买页面显示的资源为准。
- 竞享计费型实例保障周期不同价格不同。
- 竞享计费型实例不支持转换为“按需计费”和“包年/包月”计费模式。
- 竞享计费型实例不支持变更实例规格。
- 竞享计费型实例不支持变更操作系统。
- 竞享计费型实例不支持自动恢复功能。
- 竞享计费型实例不支持卸载系统盘。
- 竞享计费型实例在中断回收时：
 - 不允许使用竞享实例制作系统盘镜像和整机镜像，但允许使用该云服务器的数据盘制作数据盘镜像。
 - 不允许删除。
- 竞享计费型实例在中断回收时，数据盘和弹性公网IP默认不释放。请设置通知提醒，来决定是否释放关联的数据盘和弹性公网IP。具体方法，请参见“[购买竞享计费型实例](#)”。

计费规则

请认真阅读竞享计费型实例的计费规则，详情请参见“[竞价计费（竞享模式）](#)”。

- **计费价格：**竞享实例根据购买时长实行分段收费，购买时长小于6小时与等于6小时情况下价格不一致，您可以参考[价格详情](#)。价格计算器上的金额如果遇小数点，则保留小数点后两位，第三位四舍五入。如遇四舍五入后不足¥0.01元，则按¥0.01元展示。
- **计费周期：**实例创建成功后开始计费，精确到秒级计费，按用户使用时长计费，实例释放后出所有整点账单。**且使用期间进行关机等操作，仍然计费。**
- **关联服务：**竞享实例模式仅适用于vCPU和内存价格，不适用于OS、系统盘、数据盘、网络带宽的价格。OS、系统盘、数据盘、网络带宽、IP按各自计费规则计费（与按需保持一致）。系统盘与实例一起创建，一起释放，但数据盘系统不会删除，需要用户自行删除。
- **代金券：**除现金券、储值卡适用之外，其他折扣券、代金券等均不适用。

计费样例

竞享实例精确到秒级计费，购买界面显示小时单价，将小时单价除以3600即可得到每秒的价格。

- **样例1：**以C6.large.2规格为例，用户购买时长3小时，08:58:30开通实例
 - 使用3小时后正常到期，11:58:30终止实例，终止实例后出整点话单

表 2-4 话单样例 1

账单周期	周期内使用时长（秒）	计费（元）
08:58:30-09:00:00	90	$90/3600 \times 0.07$
09:00:00-10:00:00	3600	0.07
10:00:00-11:00:00	3600	0.07
11:00:00-11:58:30	3510	$3510/3600 \times 0.07$

- 用户主动提前释放实例，10:28:30终止实例，终止实例后出整点话单

表 2-5 话单样例 2

账单周期	周期内使用时长（秒）	计费（元）
08:58:30-09:00:00	90	$90/3600 \times 0.07$
09:00:00-10:00:00	3600	0.07
10:00:00-10:28:30	1710	$1710/3600 \times 0.07$

- 系统提前释放实例，10:28:30终止实例，终止实例后出整点话单（免除）

表 2-6 话单样例 3

账单周期	周期内使用时长（秒）	计费（元）
08:58:30-09:00:00	90	0
09:00:00-10:00:00	3600	0
10:00:00-10:28:30	1710	0

- 样例2：以C6.large.2规格为例，用户购买时长6小时，08:58:30开通实例
 - 使用6小时后正常到期，14:58:30终止实例，终止实例后出整点话单

表 2-7 话单样例 4

账单周期	周期内使用时长（秒）	计费（元）
08:58:30-09:00:00	90	$90/3600 \times 0.12$
09:00:00-10:00:00	3600	0.12
10:00:00-11:00:00	3600	0.12
11:00:00-12:00:00	3600	0.12
12:00:00-13:00:00	3600	0.12
13:00:00-14:00:00	3600	0.12

账单周期	周期内使用时长（秒）	计费（元）
14:00:00-14:58:30	3510	3510/3600*0.12

- 用户主动提前释放实例，13:28:30终止实例，终止实例后出整点话单

表 2-8 话单样例 5

账单周期	周期内使用时长（秒）	计费（元）
08:58:30-09:00:00	90	90/3600*0.12
09:00:00-10:00:00	3600	0.12
10:00:00-11:00:00	3600	0.12
11:00:00-12:00:00	3600	0.12
12:00:00-13:00:00	3600	0.12
13:00:00-13:28:30	1710	1710/3600*0.12

- 系统提前释放实例，13:28:30终止实例，终止实例后出整点话单（免除）

表 2-9 话单样例 6

账单周期	周期内使用时长（秒）	计费（元）
08:58:30-09:00:00	90	0
09:00:00-10:00:00	3600	0
10:00:00-11:00:00	3600	0
11:00:00-12:00:00	3600	0
12:00:00-13:00:00	3600	0
13:00:00-13:28:30	1710	0

购买竞享计费型实例

您可以通过控制台方式或调用API方式，购买竞享计费型实例。

- 控制台方式，请参见“[购买竞享计费型ECS](#)”。
- API方式，请参见《弹性云服务器API参考》的“[创建云服务器](#)”章节。

中断回收

在系统资源不足等极端情况下，华为云会自动回收竞享实例，并免除实例的使用费用（该免除条件规则仅针对购买时长为1-6小时的竞享实例）。

您可以参考[计费样例](#)了解详细样例。

● 用户主动释放实例

当您已完成竞享实例的使用，您可以主动释放实例，以节约您的使用成本。释放步骤如下：

- a. 登录管理控制台。
- b. 选择“计算 > 弹性云服务器”。
- c. 勾选待删除的竞享实例弹性云服务器。
- d. 单击弹性云服务器列表页上方的“删除”或操作中的“删除”按钮。

系统盘与实例一起创建，一起释放，但云平台不会主动删除数据盘、网络带宽、弹性公网IP，需要用户自行删除。请在删除弹框选择是否同时删除弹性公网IP和数据盘。否则，数据盘、网络带宽、弹性公网IP继续计费。

● 系统回收实例

当使用时间到达您的购买时长或在系统资源不足等极端情况下，系统会自动回收实例，请您及时做好数据备份。系统回收实例时会主动删除您的竞享实例及系统盘，但不会主动删除您购买的数据盘、网络带宽、弹性公网IP、SFS Turbo文件系统等其他服务，您可以自行决定是否对其进行删除操作。

📖 说明

- 在系统资源不足等极端情况下，华为云会自动回收竞享实例，并免除实例的使用费用（该免除条件规则仅针对购买时长为1-6小时的竞享实例）。您可以参考[计费样例](#)了解详情。
- 当竞享实例出话单后，系统会进行结算与扣费，如因余额不足而产生欠费，您的资源将被冻结。欠费后，可以查看欠费详情。为防止相关资源不被停止或者释放，请及时进行充值。账号进入欠费状态，需要在约定时间内支付欠款。

因此，请务必做好数据备份工作。系统会提前发出即将释放云服务器资源的通知，如需设置通知提醒，请参见“[购买竞享计费型ECS](#)”。

常见问题

请参见[FAQ](#)。

2.2.4 按需转包年/包月

操作场景

- 按需计费：按需计费是后付费模式，按弹性云服务器的实际使用时长计费，可以随时开通/删除弹性云服务器。
- 包年/包月：包年/包月是预付费模式，按订单的购买周期计费，适用于可预估资源使用周期的场景，价格比按需计费模式更优惠。

如果您需要长期使用当前弹性云服务器，可以将按需购买的云服务器转为包年/包月计费模式，节省开支。按需转包年/包月的具体操作，请参见本节内容。

📖 说明

- 如果弹性云服务器的绑定资源（云硬盘等磁盘、弹性公网IP）支持转包年/包月，则随弹性云服务器同步转换计费模式。
- 如果弹性云服务器的绑定资源（云硬盘等磁盘、弹性公网IP）不支持转包年/包月，则保留原计费模式，详细内容，请参见[绑定资源计费模式转换规则](#)。
- ISO镜像创建的弹性云服务器不支持按需转包年/包月。

绑定资源计费模式转换规则

弹性云服务器的绑定资源主要包括各类磁盘和弹性公网IP，当按需计费的弹性云服务器转包年/包月时，绑定资源的计费模式转换规格如表2-10和表2-11所示。

表 2-10 磁盘计费模式转换规则

磁盘类型	计费模式	是否共享	是否支持随ECS按需转包年/包月	处理措施
本地盘	不涉及	否	不涉及	无。
DSS/DESS下磁盘	包年/包月（存储池计费模式）	否	不涉及	无。
云硬盘	按需计费	否	是（极速型SSD V2类型磁盘不支持）	无。
云硬盘	按需计费	是	否	在控制台的云硬盘页面进行按需转包年/包月操作。 详细内容，请参见 云硬盘计费说明 。
云硬盘	包年/包月	否	否	已经是包年/包月计费模式，无需处理。
云硬盘	包年/包月	是	否	已经是包年/包月计费模式，无需处理。

表 2-11 弹性公网 IP 计费模式转换规则

资源	计费模式	计费方式	带宽类型	是否支持随ECS按需转包年/包月	处理措施
弹性公网IP	按需计费	按带宽计费	独享带宽	是	无。
弹性公网IP	按需计费	按流量计费	独享带宽	否	在控制台的弹性公网IP页面，先将按需按流量计费转换为按需按带宽计费，再将按需计费转换为包年/包月。 详细内容，请参见 变更弹性公网IP计费方式 。

资源	计费模式	计费方式	带宽类型	是否支持随ECS按需转包年/包月	处理措施
弹性公网IP	按需计费	按带宽计费	共享带宽	否	在控制台的弹性公网IP页面进行按需转包年/包月操作。 详细内容，请参见 变更弹性公网IP计费方式 。
弹性公网IP	包年/包月	按带宽计费	独享带宽/共享带宽	否	已经是包年/包月计费模式，无需处理。

前提条件

- 弹性云服务器的计费模式是“按需计费”。
- 弹性云服务器状态为“运行中”或“关机”。

操作步骤

- 登录管理控制台。
- 单击管理控制台左上角的，选择区域和项目。
- 单击“”，选择“计算 > 弹性云服务器”。
- 在弹性云服务器列表页，选中目标云服务器。
- 单击“操作”列下的“更多 > 转包年/包月”。

说明

- 系统支持批量转包年/包月操作，即一次将多台按需计费的弹性云服务器变更为包年/包月计费模式的。操作如下：
- 勾选待转包年/包月的多台弹性云服务器。
 - 单击云服务器列表上方常用操作栏的“更多 > 转包年/包月”。
- 根据界面提示，确认转包年/包月的弹性云服务器信息后，选择弹性云服务器的购买时长，并支付订单。

2.2.5 包年/包月转按需

操作场景

包年/包月是预付费模式，按订单的购买周期计费，适用于可预估资源使用周期的场景。

如果您需要更灵活的计费方式，按照弹性云服务器的实际使用时长计费，您可以将实例的计费方式转为按需付费。

说明

- 包年/包月转按需，支持两种方式：
- 即时转按需：按需的资费模式立即生效。
 - 到期转按需：包年/包月资费模式到期后，按需的资费模式才会生效。

约束与限制

- 只有通过实名认证的客户，才可以执行包年/包月转按需操作。
- 在续费管理页面，订单状态是“使用中”的云服务器资源才能执行包年/包月转按需。
- 解决方案组合产品不支持包年/包月转按需。
- 已开票资源不支持包年/包月转按需。

即时转按需

1. 登录管理控制台。
2. 单击管理控制台左上角的，选择区域和项目。
3. 选择“计算 > 弹性云服务器”。
4. 在弹性云服务器列表中，勾选需要进行操作的弹性云服务器。
5. 单击弹性云服务器列表左上角的“更多 > 即时转按需”。
6. 单击“是”，跳转至费用中心的“包年/包月转按需”页面。

图 2-3 包年/包月转按需



7. 根据界面提示，勾选需要转按需的资源。
8. 确认退款信息后，单击“转按需”。
9. 再次根据界面信息确认要转按需的资源后，单击“确定”。

到期转按需（云服务器控制台）

1. 登录管理控制台。
2. 单击管理控制台左上角的，选择区域和项目。
3. 选择“计算 > 弹性云服务器”。
4. 在弹性云服务器列表中，勾选需要进行操作的弹性云服务器。
5. 单击弹性云服务器列表左上角的“更多 > 到期转按需”。
6. 单击“是”，跳转至费用中心的“到期转按需”页面。

图 2-4 到期转按需



7. 根据界面提示，勾选需要转按需的资源。
8. 单击“到期转按需”。

到期转按需（费用中心）

1. 登录管理控制台。
2. 单击“控制台”页面上方“费用”，在下拉菜单中选择“续费管理”。
系统进入“续费管理”页面。
3. 自定义查询条件。
 - 可在“到期转按需项”页签查询已经设置到期转按需的资源。
 - 可对“手动续费项”、“自动续费项”、“到期不续费项”页签的资源设置到期转按需的操作。

图 2-5 续费管理



4. 设置包年/包月资源到期后转按需。
 - 单个资源到期转按需：选择需要更改计费方式的弹性云服务器，单击操作列“更多 > 到期转按需”。
 - 批量资源到期转按需：选择需要更改计费方式的弹性云服务器，单击列表左上角的“到期转按需”。
5. 查看资费变更的相关信息后，单击“转按需”。

2.3 购买 ECS

2.3.1 ECS 购买方式导航

云平台提供了多种购买ECS的方式，满足您在不同业务场景的需求。

表 2-12 实例购买方式

购买方式	适用场景
快速购买ECS	快速购买ECS的操作指导，您可以根据业务需求选择规格，在指定计费模式、区域、镜像、公网访问和购买量等参数后，快速完成弹性云服务器的购买。
自定义购买ECS	购买ECS的通用操作指导，您可以根据业务场景灵活设置ECS的计费模式、规格类型、镜像类型、存储、网络、安全组、公网访问等配置信息。
购买竞价计费型ECS	购买竞价计费竞价模式ECS的操作指导，相当于以一定折扣购买按需计费ECS。 适用于对成本控制要求比较高，期望以较低折扣使用同等性能应用或服务的场景。
购买竞享计费型ECS	购买竞价计费竞享模式ECS的操作指导，相当于以一定折扣购买按需计费ECS。 适用于对成本控制要求比较高，期望以较低折扣使用同等性能应用或服务的场景。
通过私有镜像购买ECS	私有镜像包含操作系统、预装的公共应用以及用户的私有应用，通过私有镜像购买ECS可以节省重复配置的时间。 适用于有习惯使用的操作系统和应用程序的用户。
通过智能购买助手购买ECS	智能购买助手包含启动模板和智能购买组。 - 启动模板：包含了用于创建ECS的除密码之外的任意配置信息，可以批量购买相同配置的ECS。 - 智能购买组：通过自定义配置可以批量购买不同可用区、不同实例类型以及不同计费模式的ECS。
通过共享VPC购买ECS	通过其他账号共享的VPC和子网购买ECS，实现网络资源的共享和统一管理，提升资源管控效率、降低运维成本。
购买相同配置ECS	通过“购买相同配置”功能可以快速购买与当前配置相同的ECS，节省配置时间。

2.3.2 快速购买 ECS

操作场景

弹性云服务器（Elastic Cloud Server，ECS）是由CPU、内存、操作系统、云硬盘组成的一种可随时获取、弹性可扩展的云服务器。弹性云服务器购买成功后，您就可以像使用自己的本地PC或物理服务器一样，在云上使用弹性云服务器。

弹性云服务器的快速购买功能，支持经济型、高性价比型以及高性能型实例规格的推荐，方便您根据业务需求选择规格，在指定计费模式、区域、镜像、公网访问和购买量等参数后，可快速完成弹性云服务器的购买。

下面介绍如何在管理控制台通过快速购买方式创建一台弹性云服务器的操作指导。如果您想要了解购买ECS的更详细介绍，请参见[自定义购买ECS](#)。

约束与限制

- 仅支持“包年/包月”和“按需计费”模式。
- 仅支持随机分配可用区。
- 仅支持选择推荐规格范围内的实例规格。
- 仅支持选择公共镜像类型的操作系统。

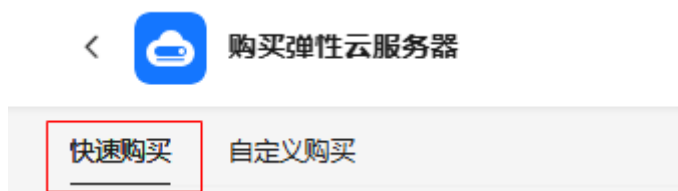
前提条件

1. 注册账号并实名认证。
在购买ECS之前，请先[注册华为账号并开通华为云、实名认证](#)。
如果您已开通华为云并进行实名认证，请忽略此步骤。
2. 为账户充值。
请保证账户有足够的资金，以免购买ECS失败。具体操作，请参见[账户充值](#)。

操作步骤

1. 登录控制台，进入ECS的[快速购买](#)页面。

图 2-6 快速购买



2. 设置“基本配置”信息。
 - a. 选择“计费模式”。
计费模式与ECS的付费方式、计费周期、资源状态变化等有关，请根据实际业务场景进行选择。

表 2-13 计费模式参数配置说明

选项	说明	场景及约束	更多参考
包年/包月	预付费模式，先付费再使用。 根据订单的购买周期计费。	适用于可预估资源使用周期的场景，价格比按需计费模式更优惠。对于长期使用者，推荐该方式。 购买后如果不再使用，不能直接删除，需进行资源退订。	包年/包月
按需计费	后付费模式，先使用再付费。 根据实际使用时长秒级计费，按小时结算。	适用于计算资源需求波动的场景，可以随时开通，随时删除。	按需计费

- b. 选择“区域”。
- 区域指ECS的物理数据中心所在的位置，建议您就近选择靠近您业务的区域，可减少网络时延，提高访问速度。

说明

- 不同区域的云服务产品之间内网互不相通。
 - ECS购买成功后，不支持直接切换区域，请谨慎选择。
3. 设置“实例”。
- 快速购买功能提供经济型、高性价比型和高性能型场景下的推荐规格，您可以根据业务需求快速选择规格。
- 若当前推荐规格不满意您的也无需要，请切换至自定义购买方式，详细内容，请参见[自定义购买ECS](#)。

图 2-7 选择规格

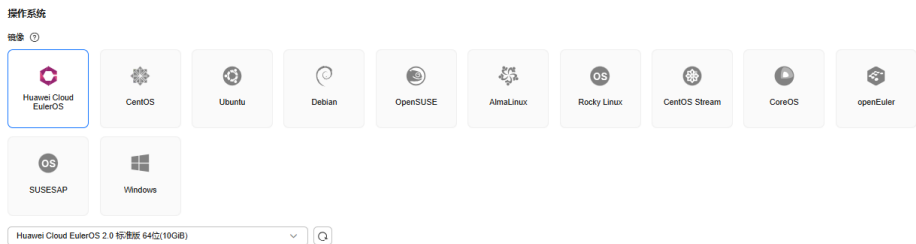


表 2-14 实例适用场景选项

场景	特点	推荐规格（以界面实际显示为准）
经济型	价格经济实惠，适用于中轻载企业应用及个人用户。	T6：t6.small.1、t6.large.1 S7：s7.large.2、s7.large.4
高性价比型	提供较高网络带宽及收发包能力，适用于对计算和网络性能有较高要求的中轻载企业应用。	S7：s7.small.1、s7.large.2、s7.xlarge.2、s7.2xlarge.2
高性能型	提供更高性能、安全及稳定性能力，适用于对计算和网络有高性能要求的中重载企业应用。	C7：c7.large.2、c7.xlarge.2、c7.2xlarge.2、c7.3xlarge.2

4. 设置“操作系统”。
- a. 为ECS设置操作系统。
快速购买功能仅支持为ECS设置公共镜像类型的操作系统，您可以根据需要选择对应的操作系统和版本。
更多信息，请参见[公共镜像概述](#)。

图 2-8 设置操作系统



- b. （可选）设置“开启安全防护”。
- 选择部分操作系统的公共镜像时，系统默认开启主机安全服务（Host Security Service, HSS）的安全防护功能，开启后，默认提供一个免费的基础防护并自动安装主机安全Agent，支持口令检测、漏洞检测等防护功能。
主机安全服务可以为云服务器提供风险预防、入侵检测、高级防御、安全运营、网页防篡改等安全防护功能，帮助构建云服务器安全防护体系，降低云服务器面临的主要安全风险。

说明

一个月的基础防护免费使用期限结束后，该防护配额将自动释放，停止相应的实时防护能力。
如您需要保留或升级原有安全防护能力，建议您重新购买主机安全服务。详细情况，请参见主机安全的[免费试用HSS基础版到期后怎么办？](#)。
购买后您可以在主机安全服务控制台切换不同版本。各版本之间的差异请参考[服务版本差异](#)。

5. 设置“公网访问”。
- a. 勾选“公网访问”，为ECS购买并绑定弹性公网IP。
若去勾选，则表示暂不购买弹性公网IP。

说明

- 若弹性公网IP的默认线路售罄，则不支持勾选“公网访问”。
- b. （可选）设置“公网带宽”。
- 仅当勾选“公网访问”时，会显示该参数。一个带宽只能被一个弹性公网IP使用。
- 按带宽计费：独享带宽，按照购买的带宽大小计费。
 - 按流量计费：独享带宽，按照实际使用的流量来计费。
- c. （可选）设置“带宽大小”。
- 仅当勾选“公网访问”时，会显示该参数。根据业务需要，选择所需的带宽大小，单位Mbit/s。
6. 设置“其他配置”。
- 其他配置由系统默认设置，如需进行自定义配置请通过自定义购买方式进行配置。
- 详细内容，请参见[自定义购买ECS](#)。

表 2-15 其他配置说明

配置项	示例	默认配置说明	相关参考
可用区	随机分配	默认随机分配可用区。	区域和可用区
虚拟私有云	vpc-default	默认设置为最新创建的ECS使用的VPC和子网。	虚拟私有云和子网规划建议
主网卡	subnet-default	- 若当前账号无ECS，则默认使用最新创建的VPC及VPC下的最新可用子网。 - 若当前账号无可用VPC，则使用系统默认创建的VPC和子网。 - 若当前账号的可用VPC下无可用子网，则跳转至自定义购买ECS方式。 - 主网卡默认设置为自动分配IPv4和IPv6地址。 说明 若所选子网未开启IPv6，则不分配IPv6地址。	
安全组	default/Sys-WebServer	系统自动设置为默认安全组。	安全组概述
云服务器名称	ecs-xxxx	系统随机生成。	NA
云监控	已开启详细监控(免费)	选择部分操作系统的公共镜像时，系统默认开启详细监控。	监控弹性云服务器

配置项	示例	默认配置说明	相关参考
企业项目	default	该参数针对企业用户使用。默认设置为最新创建的ECS使用的企业项目。 - 若当前账号无ECS或ECS无可用于企业项目，则默认使用最新创建的企业项目。 - 若当前账号无可用于企业项目，则创建并使用默认的企业项目。	进入企业中心

7. 设置“购买量”。
- a. （可选）设置“购买时长”。

仅当“计费模式”选择“包年/包月”时，会显示该参数。用于设置ECS的购买时长，最短为1个月，最长为3年。
- b. （可选）设置“自动续费”。

仅当“计费模式”选择“包年/包月”时，会显示该参数。

勾选“自动续费”，在“包年/包月”资源到期后，可以自动进行续费。

按月购买的资源：每次续费1个月，次数不限。

按年购买的资源：每次续费1年，次数不限。

关于自动续费的更多说明，请参考[自动续费规则说明](#)。
- c. 设置“购买数量”。

如需批量购买ECS，可以设置购买ECS的数量。设置后，会批量创建多台相同配置的ECS。

系统会显示您当前还可以购买的ECS数量。为了保证所有资源的合理分配，如果您需要的ECS数量超过当前可以购买的最大数值，可以[申请扩大配额](#)。
8. 确认配置并购买ECS。
- a. 在页面右侧的“配置概要”中，查看ECS配置详情。

未设置的必选字段会通过红色字体进行提示，需在参数配置区域进行设置。
- b. 勾选协议并单击“立即购买”。

ECS创建成功后会默认开机。

后续操作

快速购买未设置登录凭证，如需远程登录，可创建后通过“重置密码”操作设置密码。详细内容，请参见[在控制台重置ECS密码](#)。

2.3.3 自定义购买 ECS

操作场景

弹性云服务器（Elastic Cloud Server，ECS）是由CPU、内存、操作系统、云硬盘组成的一种可随时获取、弹性可扩展的云服务器。弹性云服务器购买成功后，您就可以像使用自己的本地PC或物理服务器一样，在云上使用弹性云服务器。

您只需要指定CPU、内存、操作系统、规格、登录凭证方式即可获得一台弹性云服务器。

下面介绍如何在管理控制台自定义购买弹性云服务器。

操作流程

操作步骤	说明
准备工作	- 注册华为账号并开通华为云，为账户充值。 - 创建VPC、子网、安全组、密钥对、专属计算集群、CloudPond等相关资源。
步骤一：进入ECS购买页	进入“购买弹性云服务器”页面，开始设置购买参数。
步骤二：设置购买参数	根据业务需要，设置购买ECS的参数。
步骤三：确认配置并购买ECS	根据配置概要确认配置详情，完成ECS的购买。

准备工作

- 注册账号并实名认证。
在购买ECS之前，请先[注册华为账号并开通华为云、实名认证](#)。
如果您已开通华为云并进行实名认证，请忽略此步骤。
- 为账户充值。
请保证账户有足够的资金，以免购买ECS失败。具体操作，请参见[账户充值](#)。
- 规划VPC和子网等网络资源。
当您开始购买ECS时，系统会创建默认的VPC（vpc-default）和子网（subnet-default）。
如果您不想使用默认的VPC和子网，建议您提前在对应区域创建新的VPC和子网。
更多信息，请参见[虚拟私有云和子网规划建议](#)。
- 创建安全组并配置安全组规则。
当您开始购买ECS时，系统会创建默认的安全组（default、Sys-WebServer和Sys-FullAccess）。默认安全组的更多信息，请参见[默认安全组和规则](#)。
如果默认安全组和规则不能满足您的业务需要，建议您提前修改安全组规则。具体操作，请参见[配置安全组规则](#)。
- 创建密钥对。
如果采用密钥对方式登录ECS，建议您提前创建密钥对。具体操作，请参见[（推荐）通过管理控制台创建密钥对](#)。
- 创建专属物理资源。
如果您想要将ECS运行在隔离的物理硬件中，请先申请专属计算集群，再购买ECS。
具体操作，请参见[申请专属计算集群](#)。
- 注册边缘小站。
如果您想要将ECS部署在CloudPond上，需提前注册边缘小站。
具体操作，请参见[线上注册边缘小站](#)。

步骤一：进入 ECS 购买页

登录控制台，进入ECS的[自定义购买](#)页面。

图 2-9 自定义购买



说明

- 华为云不定期推出优惠活动，购买前请您先前往[官网活动](#)查询。活动规则以届时官网活动页面展示为准。
- 如果您的云服务器上部署了SAP HANA，则可以选择购买HANA类型的弹性云服务器。HANA云服务器是指专门为SAP HANA提供的一种云服务器类型。
SAP HANA(High-Performance Analytic Appliance)是基于内存计算技术的高性能实时数据计算平台。云平台提供了高性能的IaaS层服务，能够满足SAP HANA需求，帮助用户在云平台上快速申请SAP HANA所需的资源（HANA云服务器、公网IP地址等），并安装和配置SAP HANA，从而提升用户的效率，降低用户的成本，提升用户的体验。
关于更多HANA云服务器的应用场景与购买方法，请参见《[SAP HANA用户指南](#)》。

步骤二：设置购买参数

以下模块包含了自定义购买ECS过程中涉及的所有参数，请您根据业务需求完成计费模式、区域和可用区、规格的vCPU和内存、存储、网络等各类参数的设置。

基础配置

- 选择“计费模式”。
计费模式与ECS的付费方式、计费周期、资源状态变化等有关，请根据实际业务场景进行选择。

表 2-16 计费模式参数配置说明

选项	说明	场景及约束	更多参考
包年/包月	预付费模式，先付费再使用。 根据订单的购买周期计费。	适用于可预估资源使用周期的场景，价格比按需计费模式更优惠。对于长期使用用户，推荐该方式。 购买后如果不再使用，不能直接删除，需进行资源退订。	包年/包月

选项	说明	场景及约束	更多参考
按需计费	后付费模式，先使用再付费。 根据实际使用时长秒级计费，按小时结算。	适用于计算资源需求波动的场景，可以随时开通，随时删除。	按需计费
竞价计费	后付费模式，先使用再付费，相对于按需计费有一定的折扣。 包含竞价模式和竞享模式，根据实际使用时长秒级计费，按小时结算。	适用于对成本控制要求比较高，期望以较低折扣使用同等性能应用或服务的场景。 存在中断机制，实例生命周期不可控，不适用需长时间作业、或稳定性要求极高的服务。	• 竞价计费（竞价模式） • 竞价计费（竞享模式）

📖 说明

- 当您为CloudPond购买云服务器时，仅支持选择“按需计费”。
 - “竞价计费”仅在部分区域上线，详细内容，请参见[功能总览](#)。
2. （可选）设置“竞价类型”。
- 仅当“计费模式”选择“竞价计费”时显示该参数。支持设置为“竞价模式”或“竞享模式”。

图 2-10 设置“竞价类型”



- 竞价模式：价格随市场价格波动，更多信息，请参见[购买竞价计费型ECS](#)。
 - 竞享模式：价格取决于保障周期，更多信息，请参见[购买竞享计费型ECS](#)。
3. 选择“区域”。
- 区域指ECS的物理数据中心所在的位置，建议您就近选择靠近您业务的区域，可减少网络时延，提高访问速度。

📖 说明

- 不同区域的云服务产品之间内网互不相通。
 - ECS购买成功后，不支持直接切换区域，请谨慎选择。
 - 当您为CloudPond购买云服务器时，默认区域为当前小站所在的区域，且不支持更换为其他区域。
4. 选择“可用区”。

可用区指在同一区域下，电力、网络隔离的物理区域，可用区之间内网互通，不同可用区之间物理隔离。

表 2-17 可用区参数配置说明

选项	说明	场景及约束	更多参考
随机分配	不同可用区上线的云服务器类型和规格不同。系统使用哈希算法基于用户的UUID（Universally Unique Identifier）以及选择的规格，分配ECS所在的可用区。	如果需要查看当前平台支持的全部云服务器类型和规格，请选择“随机分配”。 说明 当您批量购买多台ECS时，如果需要将ECS分布到不同可用区，可以勾选“多可用区部署”。	区域和可用区
可用区n	当前区域支持的具体可用区，“n”表示可用区序号。	如果需要将ECS创建在指定可用区，请选择具体的可用区。 - 如果您需要提高应用的高可用性，建议您将弹性云服务器创建在不同的可用区。 - 如果您需要较低的网络时延，建议您将弹性云服务器创建在相同的可用区。	
边缘可用区	边缘可用区部署在用户数据中心，为CloudPond用户专属。	当您为CloudPond购买云服务器时，默认可用区为“边缘可用区”，且不支持更换为其他可用区。	边缘小站与区域和可用区是什么关系？

实例

1. 选择实例选型方式。

表 2-18 实例参数配置说明

选项	说明	场景及约束	更多参考
规格类型选型	提供按不同规格属性的选型： • CPU架构：x86计算、鲲鹏计算。 • 实例筛选：支持按指定vCPU、内存或规格名称搜索规格。 • 规格类型：支持按实例类型和代系名称筛选规格。	适用于熟悉CPU架构、vCPU、内存、实例类型和规格代系名称等属性，想要根据具体配置要求进行规格选型的用户。	ECS实例概述
业务场景选型	提供按业务场景、子场景及子场景业务量的推荐规格。	适用于有明确业务场景需求，想要根据业务场景、业务量等参考指标进行规格选型的用户。	

2. （可选）选择“CPU架构”。
- 当实例选择“规格类型选型”方式时，该参数可见。

表 2-19 CPU 架构参数配置说明

选项	说明	场景及约束	更多参考
x86计算	采用复杂指令集CISC（Complex Instruction Set Computer），支持几乎所有常用软件。 由于指令执行较为复杂所以每条指令花费的时间较长。	适用于Windows系列、仅x86兼容的商业软件等强平台相关场景。	规格清单（x86）
鲲鹏计算	采用精简指令集RISC（Reduced Instruction Set Computer），自研芯片，性价比更高。 因指令类型较少，所以能够以更高的速度执行操作，使计算机的结构更加简单、合理地提高运行速度。	适用于如下场景： • 电商、大数据、科学计算等弱平台相关场景。 • 手机仿真等ARM原生场景。	规格清单（鲲鹏）

3. （可选）选择“业务场景”和“子场景”。
- 当实例选择“业务场景选型”方式时，该参数可见。

 说明

不同区域、不同可用区上线的规格不同，推荐规格请以控制台显示为准。

表 2-20 业务场景选项

业务场景	子场景	说明	推荐规格（示例）
Web应用	传统办公	高安全及高可靠性，预期并发访问量小于200，适用于OA、ERP、CRM等传统办公场景。	C7、C6
	企业展示型网站	高性价比，基本水平的vCPU性能、平衡的计算、内存和网络资源。	● C7、C6 ● S7、S6
	个人应用搭建	高性价比，基本水平的vCPU性能、平衡的计算、内存和网络资源。	● S7、S6 ● T6
	开发测试环境	基本水平的vCPU性能、平衡的计算、内存和网络资源，同时可根据工作负载的需要实现性能的突增，具有短期发挥更高性能的能力。	S7、S6
	前端服务器	基本水平的vCPU性能、平衡的计算、内存和网络资源，适合Apache、Nginx、IIS等前端服务场景。	S7、S6
	后端服务器	CPU/内存配比高，具备高性能、低时延、高性价比的特点。适用于Tomcat、JBoss等后端服务场景。	C7、C6、C6s
网站应用/电商	10万pv，1000活跃用户	高性价比，弹性可用的ECS可随取随用，避免资源浪费。	● S7、S6 ● T6
	20万pv，2000活跃用户	在促销、秒杀、爆款、直播等场景下，满足电商网站对云服务器的高性能、快速弹性、高稳定的业务诉求。	● C7、C6、C6s ● S7、S6
	50万pv，5000活跃用户	在促销、秒杀、爆款、直播等场景下，满足电商网站对云服务器的高性能、快速弹性、高稳定的业务诉求。	C7、C6、C6s
游戏	游戏	具有高性能、高稳定性、低时延、高性价比的特点，满足游戏业务对服务器性能、可靠性、网络、弹性伸缩的高要求。	C7、C6、C6s
数据库	计算	提供稳定的高性能计算能力。	C7、C6、C6s

业务场景	子场景	说明	推荐规格（示例）
	存储	自带高存储带宽和IOPS的本地盘，具有高存储IOPS以及读写带宽的优势，在海量数据存储场景下，具备更高的性价比。	• M7、M6 • D7、D6
	网络	数据访问量大，要求快速的数据交换和处理。依赖于较高的PPS和低网络时延，提供较高的TPS吞吐量。	• E7、E6 • M7、M6 • C7、C6、C6s
数据分析	管理节点	高网络性能要求，调动大量的计算资源，提升数据处理速度。	C7、C6、C6s
	计算节点	高计算性能、高稳定性要求，各个节点的计算能力要保持均衡。	• M7、M6 • C7、C6、C6s • I7、I7、I3、I3 • S7、S6
	存储节点	大量的数据读写，对存储带宽有很高诉求，在海量数据存储场景下，具备更高的性价比。	D7、D6、D3
高性能计算	高性能计算	计算资源使用量大。利用高性能云服务器的高性价比计算资源构建计算集群，可大幅降低成本。	H3
图形渲染	动画渲染	精细度要求高的渲染场景，基于CPU的渲染计算，计算稳定性高。	aC7、C6、C3
	网络影视渲染	基于GPU渲染器的渲染计算，运算速度快。	G6
AI/机器学习	AI训练	搭配NVIDIA智能网卡，适用于深度学习训练、科学计算、计算流体动力学、计算金融、地震分析、分子建模、基因组学等领域。	P2vs、P2v、P2s
	AI推理	搭配NVIDIA智能网卡，适用于图像分类识别、语音识别、自然语言处理、视频编解码、机器学习、轻量级训练。	Pi2

4. 设置“实例筛选”。
- a. 选择规格。

- 搜索规格：输入vCPUs、内存或规格名称直接搜索规格。
当实例选择“规格类型选型”方式时，支持搜索规格。
- 通过列表选择规格：通过实例类型和规格代系名称在列表中选择已上线的规格。
如果您有特定的规格配置需求，选择规格前，请先查看规格的特点、适用场景、指标数据等信息，具体内容请参见[实例类型](#)。

说明

- CloudPond支持的规格清单，请参考[规格清单（IES）](#)。
- 购买弹性云服务器时，用户不能选择已售罄的CPU和内存资源。用户可通过勾选“隐藏售罄的规格”将列表中已售罄的规格隐藏。
- 若“计费模式”为“按需计费”，规格选择GPU加速型、AI加速型或鲲鹏AI加速型，则可能需要冻结一定的保证金。详细内容，请参见[按需计费](#)。
- 本地盘：指弹性云服务器所在物理机的本地存储，当前仅支持HDD（Hard Disk Driver）盘。当您选择的云服务器类型使用本地盘时（如磁盘增强型），系统会自动给云服务器挂载本地盘，并显示对应规格的本地盘信息。
以“本地盘”的值为“3×1800GiB(hdd)”为例，表示一个弹性云服务器挂载3个HDD盘，每个盘的容量为1800GiB。

b. 设置规格显示范围。

- 仅展示最新系列：勾选后，仅显示新上线的云服务器类型与规格，若不勾选，则显示云服务平台当前提供的所有云服务器类型与规格。

说明

该参数仅在部分区域上线，使用时请以控制台实际显示为准。

- 隐藏售罄的规格：勾选后，不显示当前已售罄的规格。

5. （可选）设置“价格上限”。

仅当“计费模式”选择“竞价计费”，“竞价类型”选择“竞价模式”时，该参数可见。

- 自动设置：推荐使用，指将按需计费的价格设置为价格上限。即您愿意为弹性云服务器支付的最高价格是按需计费的价格。
- 手动设置：需要您自己设定竞价计费型实例的价格上限。该上限值需大于等于当前的市场价格，小于等于按需计费的价格。

更多信息，请参见[购买竞价计费型ECS](#)。

6. （可选）设置“保障周期”。

仅当“计费模式”选择“竞价计费”，“竞价类型”选择“竞享模式”时，该参数可见。

- 保障周期：购买竞享实例的最小单位时间，保障周期不同价格不同。
在保障周期内由云平台中断竞享实例，当前周期不计费。在保障周期内用户删除竞享实例，当前周期按使用时长计费。
- 配置单价：无需设置。
- （可选）保障周期数量：仅当“保障周期”设置为“6小时”时显示该参数。
更多信息，请参见[购买竞享计费型ECS](#)。

操作系统

1. 选择“镜像”。
- 镜像是一个包含了操作系统及必要配置的弹性云服务器模板，使用镜像可以创建弹性云服务器。

表 2-21 镜像参数配置说明

选项	说明	更多参考
公共镜像	常见的标准操作系统镜像，具有高度稳定性，皆为正版授权，所有用户可见，包括操作系统以及预装的公共应用。 您可以根据实际需求自助配置应用环境或相关软件。	公共镜像概述
私有镜像	由用户创建或导入的个人镜像，仅用户自己可见。包含操作系统、预装的公共应用以及用户的私有应用，可以节省重复配置ECS的时间。	创建私有镜像 通过私有镜像购买ECS
共享镜像	由其他账号共享的私有镜像，提供跨账号使用同一镜像创建ECS的能力。	共享镜像概述
市场镜像	由云商店提供的预装操作系统、应用环境和各类软件的优质第三方镜像。无需配置，可一键部署，满足建站、应用开发、可视化管理等个性化需求。	云商店

说明

华为云不再提供Windows操作系统类型的公共镜像，Windows操作系统镜像变更为市场镜像类型。

为方便您操作，系统在“公共镜像”页签下展示了Windows操作系统镜像的选项，您可以通过该选项直接选购第三方服务商提供的“第三方镜像”。您也可以在“市场镜像”页签下选购相关Windows操作系统镜像。

Windows操作系统镜像所有使用的约束与限制遵循第三方，计费标准以镜像供应商提供的信息为准。

2. （可选）设置“自动安装GPU驱动”。
- 当规格选择“GPU加速型”，且选择的镜像后缀带“NO Driver”时，会显示该参数。
- 勾选“自动安装GPU驱动”并选择对应版本后，可以为您的云服务器自动安装GPU驱动。

📖 说明

- 系统会对规格与GPU驱动版本进行校验，您可以直接从下拉框中进行选择。更多关于GPU驱动版本的介绍，请参见[Tesla驱动及CUDA工具包获取方式](#)。
- 安装过程大约需要5~10分钟，在安装完成前，请勿关机或重启云服务器，避免安装失败。
- 安装完成后，云服务器会自动重启。
- 如果云服务器切换操作系统，则已自动安装的GPU驱动会失效。
- 如果GPU驱动安装失败或失效，请手动安装GPU驱动，详细内容，请参见[（推荐）自动安装GPU加速型ECS的GPU驱动（Linux）](#)或[（推荐）自动安装GPU加速型ECS的GPU驱动（Windows）](#)。

3. （可选）设置“开启安全防护”。

选择部分操作系统的公共镜像时，系统默认开启主机安全服务（Host Security Service, HSS）的安全防护功能，开启后，默认提供一个月免费的基础防护并自动安装主机安全Agent，支持口令检测、漏洞检测等防护功能。

主机安全服务可以为云服务器提供风险预防、入侵检测、高级防御、安全运营、网页防篡改等安全防护功能，帮助构建云服务器安全防护体系，降低云服务器面临的主要安全风险。

📖 说明

一个月的基础防护免费使用期限结束后，该防护配额将自动释放，停止相应的实时防护能力。

如您需要保留或升级原有安全防护能力，建议您重新购买主机安全服务。详细情况，请参见主机安全的[免费试用HSS基础版到期后怎么办？](#)。

购买后您可以在主机安全服务控制台切换不同版本。各版本之间的差异请参考[服务版本差异](#)。

4. （可选）设置“应用加速”。

仅当“规格”选择“KC2”、“镜像”选择“Huawei Cloud EulerOS 2.0 标准版 64位 ARM版”时，会显示该参数。

设置应用加速后，系统会根据所选Nginx、Redis或MySQL应用，在CPU、内存、网络、存储、内核等领域以及应用本身针对性调优，达到最优状态。

- 不加速：不开启应用加速，默认设置该选项。
- Nginx加速：开启针对Nginx应用的调优。
- Redis加速：开启针对Redis应用的调优。
- MySQL加速：开启针对MySQL应用的调优。

存储与备份

1. （可选）设置“磁盘类型”。

仅当已在[专属分布式存储](#)页面申请了存储池时，会显示该参数。

根据磁盘使用的存储资源是否独享，磁盘划分为“云硬盘”和“专属分布式存储”两类，其中，专属分布式存储是为您提供的独享存储资源。

- 专属分布式存储：用于在已申请的存储池中创建磁盘。
- 云硬盘：用于使用公共存储资源创建磁盘。

 说明

- 使用专属分布式存储资源创建磁盘时，待创建磁盘的磁盘类型需和申请的存储池资源类型保持一致，如都是“高IO”类型。
- 更多关于专属分布式存储的内容，请参见《[专属分布式存储服务用户指南](#)》。

2. 设置“系统盘”。

系统盘用于存储云服务器的操作系统，创建云服务器时自带系统盘，且系统盘自动初始化。

 说明

购买“包年/包月”云服务器时购买的系统盘，卸载后，如果继续作为系统盘使用，则只能挂载给原云服务器；如果作为数据盘使用，则可以挂载给任意云服务器。

表 2-22 系统盘参数配置说明

选项	说明	场景及约束	更多参考
磁盘类型	根据磁盘的IO性能划分磁盘类型。	根据性能，磁盘可分为极速型SSD V2、极速型SSD、通用型SSD V2、超高IO、通用型SSD、高IO、普通IO。 不同类型云硬盘的性能和价格有所不同，您可根据应用程序要求选择您所需的云硬盘。	磁盘类型及性能介绍
系统盘大小	系统盘容量大小，单位为GiB。	云硬盘根据磁盘容量计费，请根据业务需要选择合适的容量大小。 说明 对于P1型、P2型弹性云服务器，系统盘大小需大于等于15GB，建议大于40GB。	
IOPS	云硬盘每秒进行读写的操作次数。 仅当“磁盘类型”选择“通用型SSD V2”时，支持设置该参数。	建议您参考取值范围并根据业务需要，设置IOPS。	
吞吐量	云硬盘每秒成功传送的数据量，即读取和写入的数据量。 仅当“磁盘类型”选择“通用型SSD V2”时，支持设置该参数。	建议您参考取值范围并根据业务需要，设置吞吐量。	

3. （可选）设置系统盘的“高级设置”。

“高级设置”用于设置系统盘的“SCSI”和“加密”属性。

表 2-23 系统盘高级设置参数配置说明

选项	说明	场景及约束	更多参考
SCSI	用于设置系统盘为SCSI磁盘模式。 该参数无需设置，默认勾选。	磁盘模式包含： • VBD（虚拟块存储设备，Virtual Block Device）模式 • SCSI（小型计算机系统接口, Small Computer System Interface）模式 系统默认的磁盘模式为VBD，如果选择了SCSI，能支持SCSI指令透传，可应用于需要支持SCSI指令的场景。 说明 磁盘模式在购买磁盘时配置，购买完成后无法修改。	磁盘模式介绍
加密	用于加密系统盘。 • 如果选择了加密镜像，系统盘会自动加密，无需再次设置。 • 如果未选择加密镜像，可通过勾选“加密”进行系统盘加密操作。	加密系统盘，可以为您的数据提供强大的安全防护。加密磁盘生成的快照及通过这些快照创建的磁盘将自动继承加密功能。 系统盘加密的具体参数，请参见 4 。 说明 CloudPond用户不支持磁盘加密。	云硬盘加密

4. （可选）设置磁盘加密参数。
- 仅当磁盘的“高级设置”勾选了“加密”时，会显示该参数。

 说明

为了使用加密特性，需单击“创建委托”授权EVS获取KMS密钥用来加解密云硬盘。

如果您有授权资格，则可直接授权，如果权限不足，需先联系拥有Security Administrator权限的用户授权，然后再重新操作。更多信息，请参见[哪些用户有权限使用加密特性？](#)。

加密参数包括：

- 委托名称：用于授权EVS获取KMS密钥来加解密云硬盘。当“委托名称”为“EVSAccessKMS”时，表示已授权成功。

 说明

为了使用加密特性，需单击“创建委托”授权EVS获取KMS密钥用来加解密云硬盘。

如果您有授权资格，则可直接授权，如果权限不足，需先联系拥有Security Administrator权限的用户授权，然后再重新操作。更多信息，请参见[哪些用户有权限使用加密特性？](#)。

- KMS加密：用于设置获取KMS密钥的方式。
 - 从KMS密钥中选择：通过密钥名称选择KMS密钥。

- 输入KMS密钥ID：通过密钥ID选择KMS密钥。
- （可选）密钥名称：加密云硬盘使用的密钥名称。仅当“KMS加密”选择“从KMS密钥中选择”时，会显示该参数。
您可以选择使用已有的密钥，或者单击“查看密钥列表”，在KMS控制台创建新的密钥。默认为evs/default。
- 密钥ID：该加密数据盘使用的密钥的ID。

5. 设置“数据盘”

数据盘用于存储用户数据。数据盘可以在购买ECS的时候购买，由系统自动挂载给云服务器。也可以在购买了云服务器之后，单独购买云硬盘并挂载给云服务器。

说明

- 数据盘挂载至云服务器后，需要[初始化云硬盘](#)才可以正常使用。
- 购买“包年/包月”云服务器时购买的非共享数据盘，卸载后，如果重新挂载，则只能挂载给原云服务器作数据盘使用。
- 购买“包年/包月”云服务器时购买的数据盘，不支持单独续订、退订、开通自动续费、转按需付费方式、以及释放功能。

表 2-24 数据盘参数配置说明

选项	说明	场景及约束	更多参考
磁盘类型	根据磁盘的IO性能划分磁盘类型。	根据性能，磁盘可分为极速型SSD V2、极速型SSD、通用型SSD V2、超高IO、通用型SSD、高IO、普通IO。 不同类型云硬盘的性能和价格有所不同，您可根据应用程序要求选择您所需的云硬盘。	磁盘类型及性能介绍
数据盘大小	数据盘容量大小，单位为GiB。	云硬盘根据磁盘容量计费，请根据业务需要选择合适的容量大小。	
IOPS	云硬盘每秒进行读写的操作次数。 仅当“磁盘类型”选择“通用型SSD V2”时，支持设置该参数。	建议您参考取值范围并根据业务需要，设置IOPS。	
吞吐量	云硬盘每秒成功传送的数据量，即读取和写入的数据量。 仅当“磁盘类型”选择“通用型SSD V2”时，支持设置该参数。	建议您参考取值范围并根据业务需要，设置吞吐量。	

选项	说明	场景及约束	更多参考
数量	数据盘的数量。	请根据业务需要选择需要增加的数据盘数量。 购买ECS时，您最多可以为ECS添加23块数据盘。	

6. （可选）设置数据盘的“高级设置”。
- “高级设置”用于设置系统盘的“SCSI”、“共享盘”和“加密”属性。

表 2-25 系统盘高级设置参数配置说明

选项	说明	场景及约束	更多参考
SCSI	用于设置数据盘为SCSI磁盘模式。 该参数无需设置，默认勾选。	磁盘模式包含： • VBD（虚拟块存储设备，Virtual Block Device）模式 • SCSI（小型计算机系统接口, Small Computer System Interface）模式 系统默认的磁盘模式为VBD，如果选择了SCSI，能支持SCSI指令透传，可应用于需要支持SCSI指令的场景。 说明 磁盘模式在购买磁盘时配置，购买完成后无法修改。	磁盘模式介绍
共享盘	用于设置数据盘为共享盘。	设置数据盘为共享盘后，该共享盘可以挂载挂载至多个ECS。	共享云硬盘
加密	用于加密数据盘。	加密数据盘，可以为您的数据提供强大的安全防护。 数据盘加密的具体参数，请参见 4 。 说明 CloudPond用户不支持磁盘加密。	云硬盘加密

选项	说明	场景及约束	更多参考
用数据盘镜像创建磁盘	用于设置用数据盘镜像创建数据盘。	当选择Windows或Linux的镜像创建ECS时，系统支持使用数据盘镜像创建数据盘。 勾选“用数据盘镜像创建磁盘”，在弹窗中选择您制作的数据盘镜像。 说明 同一个数据盘镜像，只能给一个数据盘使用，不能重复选择。 使用整机镜像创建云服务器，或数据盘使用SCSI、共享盘、加密功能时，均不支持与数据盘镜像创建磁盘同时使用。	创建私有镜像

7. （可选）设置“开启备份”。
- 仅当需要备份ECS或云硬盘时，设置该参数。
- 备份可以帮助您在服务器故障时恢复数据，为了您的数据安全，建议您开启备份。

 说明

- 使用云备份功能需要进行单独计费，计费详情请参见[云备份是如何计费的？](#)
- CloudPond不支持设置“云备份”。

8. （可选）设置“云备份”。
- 仅当勾选“开启备份”时，会显示该参数。
- 您可以根据实际情况选择设置云备份的方式。
- 现在购买：设置云备份相关参数。

i. 设置“云备份存储库名称”：只能由中文字符、英文字母、数字、下划线、中划线组成，且长度小于等于64个字符。例如：vault-f61e。默认的命名规则为“vault_xxxx”。

ii. 设置“云备份存储库容量”：此容量为备份云服务器所需的容量。存储库的空间不能小于云服务器的空间。取值范围为[云服务器总容量，10485760]GB。

iii. 设置“备份策略”：在下拉列表中选择备份策略，或进入云备份控制台查看或编辑备份策略。

- 使用已有：选择已有云备份存储库并设置备份策略。

i. 选择“云备份存储库”：在下拉列表中选择已有的云备份存储库。

ii. 设置“备份策略”：在下拉列表中选择备份策略，或进入云备份控制台查看或编辑备份策略。

网络

1. 设置“虚拟私有云”和“主网卡”。
- 虚拟私有云（VPC）为弹性云服务器构建隔离的、用户自主配置和管理的虚拟网络环境，可以在VPC中定义安全组、VPN、IP地址段、带宽等网络特性。不同虚拟私有云里面的弹性云服务器网络默认不通。

图 2-11 “网络” 参数设置



您可以在下拉列表中选择已有的虚拟私有云，或者根据业务需要创建新的虚拟私有云。系统会默认关联主网卡并设置私有IP地址的分配方式。
更多信息，请参见[虚拟私有云和子网规划建议](#)。

说明

- 弹性云服务器使用的VPC网络DHCP不能禁用。
- 如果想要使用其他账号的共享VPC和子网，请先接受共享邀请，详细操作，请参见[接受/拒绝共享邀请](#)。
有关VPC子网共享的更多信息，请参见《虚拟私有云用户指南》的“[共享VPC](#)”相关内容。

2. 设置“主网卡”。

主网卡用于系统的默认路由，不允许删除，随ECS自动创建。当设置了“虚拟私有云”后，系统会默认关联主网卡并设置私有IP地址的分配方式。

- a. 选择“主网卡”：当虚拟私有云下有多个子网时，可以在下拉列表选择其他子网作为主网卡。
- b. 设置IPv4地址分配方式：默认选择“自动分配IP地址”。
 - 自动分配IP地址：系统自动为主网卡分配私有IPv4地址。
 - 手动分配IP地址：为主网卡设置指定私有IPv4地址。设置前，可单击“查看已使用IP地址”进行查看，避免冲突。

说明

为主网卡设置指定私有IPv4地址时，如果是批量创建多台弹性云服务器：

- 此时，该IP地址为起始IP地址。
- 请确保IP地址在子网范围内且连续可用。
- 其他子网不能与指定IP的子网相同。
- 使用已有弹性网卡：若当前VPC有可用弹性网卡时，显示该选项。设置指定弹性网卡作为主网卡，可以通过下拉列表选择指定的弹性网卡。
- c. （可选）设置IPv6地址分配方式：默认选择“暂不分配IPv6地址”。
仅当选择的规格的“IPv6”列为“是”、且子网开启了IPv6功能时，该参数可见。
 - 暂不分配IPv6地址：暂不为网卡分配私有IPv6地址。
 - 自动分配IPv6地址：系统自动为网卡分配私有IPv6地址。

当选择“自动分配IPv6地址”后，网卡的IP地址为IPv6类型。在同一VPC内，ECS通过IPv6地址在双栈ECS之间进行内网访问。

如需访问公网，需要创建EIP共享带宽，并将实例的IPv6地址添加至共享带宽即可。

详细内容，请参见[添加弹性公网IP到共享带宽](#)。

说明

- 子网开启IPv6功能的详细内容，请参见[IPv6网络](#)。
- ECS创建成功后，需检查是否获取IPv6地址，如果未获取需配置ECS动态获取IPv6地址，具体操作请参见[动态获取IPv6地址](#)。

3. （可选）设置“新增扩展网卡”。

扩展网卡是可以单独创建的网卡。当您需要为ECS配置多个网卡时，可以新增多张扩展网卡，并指定扩展网卡的IP地址。

扩展网卡无法和外部正常通信，需要配置策略路由，详细信息，请参见[为多网卡ECS配置策略路由](#)。

说明

云服务器可绑定的扩展弹性网卡数量由云服务器实例规格决定，具体请参见[规格清单（x86）](#)和[规格清单（鲲鹏）](#)。

- 选择“扩展网卡1”：当虚拟私有云下有多个子网时，可以在下拉列表选择其他子网作为扩展网卡。
- 设置IPv4地址分配方式：默认选择“自动分配IP地址”。

- 自动分配IP地址：系统自动为扩展网卡分配私有IPv4地址。
- 手动分配IP地址：为扩展网卡设置指定私有IPv4地址。设置前，可单击“查看已使用IP地址”进行查看，避免冲突。
- 使用已有弹性网卡：设置指定弹性网卡作为扩展网卡，可以通过下拉列表选择指定的弹性网卡。

- （可选）设置IPv6地址分配方式：默认选择“暂不分配IPv6地址”。

仅当选择的规格的“IPv6”列为“是”、且子网开启了IPv6功能时，该参数可见。

- 暂不分配IPv6地址：暂不为网卡分配私有IPv6地址。
- 自动分配IPv6地址：系统自动为网卡分配私有IPv6地址。
当选择“自动分配IPv6地址”后，网卡的IP地址为IPv6类型。在同一VPC内，ECS通过IPv6地址在双栈ECS之间进行内网访问。
如需访问公网，需要创建EIP共享带宽，并将实例的IPv6地址添加至共享带宽即可。
详细内容，请参见[添加弹性公网IP到共享带宽](#)。

说明

- 子网开启IPv6功能的详细内容，请参见[IPv6网络](#)。
- ECS创建成功后，需检查是否获取IPv6地址，如果未获取需配置ECS动态获取IPv6地址，具体操作请参见[动态获取IPv6地址](#)。

4. 设置“源/目的检查”。

开启“源/目的检查”，系统会检查弹性云服务器发送的报文中源IP地址是否正确，如果不正确，则不允许发送该报文。通过该功能，有助于防止伪装报文攻击，提升安全性。默认情况下“源/目的检查”的状态为“ON”，无需设置。

说明

源/目的检查设置对使用已有弹性网卡无效，仅对同云服务器一起创建的网卡生效。

安全组

1. 设置“安全组”。

在下拉列表中选择可用的安全组。支持为ECS选择多个安全组（建议不超过5个），此时，ECS的访问规则遵循几个安全组规则的并集。

首次创建ECS时，系统会自动创建默认安全组default、Sys-WebServer和Sys-FullAccess，详细信息，请参见[默认安全组和规则](#)。

您可以单击“展开安全组规则”查看具体的“入方向规则”和“出方向规则”。安全组规则的配置会影响ECS的正常访问与使用，配置方法请参见[为安全组添加安全组规则](#)。常用端口与协议的用途如下，请按需开启：

- 80端口：浏览网页的默认端口，主要用于HTTP服务。
- 443端口：网页浏览端口，主要用于HTTPS服务。
- ICMP协议：用于ping云服务器之间的通信情况。
- 22端口：用于Linux云服务器的SSH方式登录。
- 3389端口：用于Windows云服务器的远程桌面登录。

2. （可选）使用预设规则创建安全组。

当下拉列表中可选择的安全组不满足业务需求时，可单击“新建安全组”，使用预设规则创建安全组。

安全组预设规则中预先配置了入方向规则和出方向规则，您可以选择所需的预设规则，快速完成安全组的创建。

a. 配置安全组基本信息

图 2-12 配置安全组基本信息

使用预设规则创建安全组

基本信息

名称

sg-

企业项目 ?

default

新建企业项目

标签(可选)

如果您需要使用同一标签标识多种云资源，即所有服务均可在标签输入框下拉选择同一标签，建议在TMS中[创建预定义标签](#)

test

01

删除

+ 添加标签

您还可以添加19个标签。

描述(可选)

请输入

0/255

表 2-26 安全组基本信息参数说明

参数	参数说明	取值样例
名称	必选参数。 安全组的名称。要求如下： - 长度范围为1~64位。 - 名称由中文、英文字母、数字、下划线（_）、中划线（-）、点（.）组成。 说明 安全组名称创建后可以修改，建议不要重名。	sg-AB
企业项目	必选参数。 创建安全组时，可以将安全组加入已启用的企业项目。 企业项目管理提供了一种按企业项目管理云资源的方式，帮助您实现以企业项目为基本单元的资源及人员的统一管理，默认项目为default。 关于创建和管理企业项目的详情，请参见《 企业管理用户指南 》。	default

参数	参数说明	取值样例
标签	可选参数。 您可以在创建安全组的时候为安全组绑定标签，标签用于标识安全组资源，可通过标签实现对安全组资源的分类和搜索。 关于标签更详细的说明，请参见 标签概述 。	“标签键”：test “标签值”：01
描述	可选参数。 安全组的描述信息。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-

b. 配置预设规则

图 2-13 配置预设规则

使用预设规则创建安全组

配置规则 ?

预设规则

开放常用端口

您可以勾选常见协议端口，在入方向快速添加规则放行对应的协议及端口。若您未勾选任何协议端口，则不会放行任何端口。您可在安全组创建后，根据实际访问需求添加或修改安全组规则。

入方向规则

☐ 远程登录和ping

☐ SSH (22) ☐ RDP (3389) ☐ FTP (20-21) ☐ Telnet (23) ☐ ICMP (全部)

☐ Web服务

☐ HTTP (80) ☐ HTTPS (443) ☐ HTTP_ALT (8080)

☐ 数据库

☐ MySQL (3306) ☐ MS SQL (1433) ☐ PostgreSQL (5432) ☐ Oracle (1521)

☐ Redis (6379)

^ 预设规则

入方向规则 出方向规则

⚠

- 入方向规则的源地址设置为0.0.0.0/0或::/0，表示允许或拒绝所有外部IP地址访问您的实例。
- 如果将“22、3389、8848”等 [高危端口](#) 暴露到公网，可能导致网络入侵，造成业务中断、数据泄露或数据勒索等严重后果。建议您将安全组规则设置为仅允许已知的IP地址访问。

优先级	策略	类型	协议端口	源地址
1	允许	IPv4	全部	sg-AB
1	允许	IPv6	全部	sg-AB

取消

确定

表 2-27 安全组预设规则参数说明

参数	参数说明	取值样例
预设规则	必选参数。 支持三种预设规则，预先配置了不同的入方向和出方向规则，方便您快速完成安全组的创建。 - 通用Web服务器：默认配置放通SSH（22）、RDP（3389）、HTTP（80）、HTTPS（443）端口和ICMP（全部）协议。 - 开放全部端口：开放全部端口有一定安全风险，请谨慎选择。 - 开放常用端口：通过勾选常见协议端口，在入方向快速添加规则放通对应的协议及端口。	开放常用端口
入方向规则	可选参数。仅当“预设规则”选择“开放常用端口”时，会显示该参数。 当前支持快速添加的协议和端口如下，请根据业务场景进行选择： - 远程登录和ping：SSH（22）、RDP（3389）、FTP（20-21）、Telnet（23）、ICMP（全部） - Web服务：HTTP（80）、HTTPS（443）、HTTP_ALT（8080） - 数据库：MySQL（3306）、MS SQL（1433）、PostgreSQL（5432）、Oracle（1521）、Redis（6379） 端口详细说明，请参见 ECS常用端口 。	-

- c. 单击“确定”完成安全组创建。
3. （可选）配置安全组规则。
如需修改当前安全组的规则，可单击“配置安全组规则”进行修改。
更多详细信息，请参见[配置安全组规则](#)。
4. （可选）展开/隐藏安全组规则。
您可以展开或隐藏安全组规则区域，在此区域包含：
 - 已选安全组：展示当前已选的安全组。如果选择多个安全组，支持通过单击“上移”或“下移”调整安全组的优先级。
 - 安全组规则：支持查看“入方向规则”和“出方向规则”。

公网访问

1. 设置“弹性公网IP”。
- 弹性公网IP是指将公网IP地址和路由网络中关联的弹性云服务器绑定，以实现虚拟私有云内的弹性云服务器通过固定的公网IP地址对外提供访问服务。
- 您可以根据实际情况选择以下三种方式：

- 现在购买：自动为每台弹性云服务器分配独享带宽的弹性公网IP，带宽值可以由您设定。
 - 使用已有：为弹性云服务器分配已有弹性公网IP。使用已有弹性公网IP时，不能批量创建弹性云服务器。
 - 暂不购买：弹性云服务器不能与互联网互通，仅可作为私有网络中部署业务或者集群所需弹性云服务器进行使用。
2. 设置弹性公网IP的“线路”。
- 全动态BGP：可根据设定的寻路协议第一时间自动优化网络结构，以保持客户使用的网络持续稳定、高效。
 - 静态BGP：网络结构发生变化，运营商无法在第一时间自动调整网络设置以保障用户的体验度。
3. （可选）设置“公网带宽”。
- 仅当“弹性公网IP”选择“现在购买”时，会显示该参数。一个带宽只能被一个弹性公网IP使用。
- 按带宽计费：独享带宽，按照购买的带宽大小计费。
 - 按流量计费：独享带宽，按照实际使用的流量来计费。
 - 加入共享带宽：一个带宽中可以加入多个弹性公网IP，多个弹性公网IP共用一个带宽。

说明

- 一个共享带宽支持添加的弹性公网IP个数有限，如果配额不足，可以选择切换使用其他共享带宽，或者申请扩大共享带宽的EIP配额。
 - 包年/包月方式购买的EIP，不支持使用共享带宽。
 - 包年/包月方式购买的共享带宽，到期后系统自动删除，并给该共享带宽中添加的EIP创建按流量计费的独占带宽。
4. （可选）设置“带宽大小”。
- 仅当“弹性公网IP”选择“现在购买”时，会显示该参数。根据业务需要，选择所需的带宽大小，单位Mbit/s。
5. （可选）设置“释放行为”。
- 仅当“计费模式”为“按需计费”和“竞价计费”时，会显示该参数。
- 如需在删除云服务器时同步删除弹性公网IP，可以勾选“随实例释放”。
6. （可选）选择弹性公网IP。
- 仅当“弹性公网IP”选择“使用已有”时，会显示该参数。可以在下拉列表中选择可用的弹性公网IP。

云服务器管理

1. 设置“云服务器名称”。
- 本步骤中设置的“云服务器名称”，会被设置为云服务器操作系统中初始的主机名（hostname）。
- 云服务器名称需符合命名规则：只能由中文字符、英文字母、数字及“_”、“-”、“.”组成。

说明

- Windows操作系统云服务器的名称建议不超过15个字符，且不要重名，否则部分Windows应用将无法使用。
- 弹性云服务器操作系统中的主机名（hostname）的命名规则遵循 [RFC 952](#)和[RFC 1123](#)规范。
- 在将“云服务器名称”设置为虚拟机操作系统中的主机名时，为避免出现未知问题，建议使用a-z或0-9以及中划线“-”组成的名称命名。
- “_”将在弹性云服务器内部被转换为“-”。
 - 连续使用的“-”和“_”将在弹性云服务器内部被转换为1个“-”。
 - 以“.”、“-”、“_”和中文字符开头将在弹性云服务器内部被忽略，从第一个非以上字符开始。
 - 不作为开头的“.”和中文字符及后面内容将在弹性云服务器内部被忽略。
- 批量购买多台云服务器时，支持自动增加数字后缀命名或者自定义规则命名。
- 自动增加数字后缀命名：多台云服务器的名称自动按序增加4位数字后缀。例如：输入ecs，从ecs-0001开始命名；若已有ecs-0010，则从ecs-0011开始命名。
 - 自定义规则命名：通过name_prefix[begin_number,bits]name_suffix格式可给各个云服务器设置不同的名称。begin_number取值区间为[0,9999]，bits取值区间为[1,4]。例如：ecs[66,3]abc，若创建2台云服务器最终生成的名称分别为ecs066abc、ecs067abc。
- 允许重名：允许创建的云服务器名称相同。如果是批量创建，勾选“允许重名”后，批量创建的多台云服务器名称全部相同，不再按序增加。
2. 设置“登录凭证”。
- 登录凭证用于设置登录ECS的方式。

表 2-28 登录凭证参数配置说明

选项	说明	场景及约束	更多参考
密码	使用设置初始密码方式作为ECS的登录凭证方式，您可以通过用户名密码方式登录ECS。 Linux ECS设置的是root用户的初始密码，Windows ECS设置的是Administrator用户的初始密码。	建议您使用复杂度高的密码，保证密码符合要求，防止恶意攻击。密码设置规则如 表2-29 所示。 说明 系统不会定期自动修改弹性云服务器密码。为安全起见，建议您定期修改密码。	密码使用场景介绍
密钥对	使用密钥对作为ECS的登录凭证方式。 您可以选择使用已有的密钥，或者单击“新建密钥对”创建新的密钥。	密钥对登录凭证方式的安全性更高。 说明 如果选择使用已有的密钥，请确保您已在本地获取该文件，否则，将影响您正常登录弹性云服务器。	（推荐）通过管理控制台创建密钥对

选项	说明	场景及约束	更多参考
使用 镜像 密码	仅当“镜像”选择“私有镜像”，且使用的是已经设置了密码的Linux操作系统私有镜像时，会显示该参数。 支持使用该私有镜像的密码作为ECS的登录密码。	请确保所选择的私有镜像已经设置了密码。	创建加密镜像 《镜像服务用户指南》
创建 后 设置	暂不设置ECS的密码。	待ECS创建成功后，您需要单击“操作”列下的“重置密码”，根据界面提示，为ECS设置密码。	在控制台重置ECS密码

表 2-29 密码设置规则

参数	规则
密码	- 密码长度范围为8到26位。 - 密码至少包含以下4种字符中的3种： - 大写字母 - 小写字母 - 数字 - Windows操作系统云服务器支持的特殊字符：!@\$%^_-=+[{()}];.//?~#* - Linux操作系统云服务器支持的特殊字符：!@\$%^_-=+[{()}];.//?~#* - 密码不能包含用户名或用户名的逆序。 - Windows操作系统的云服务器，不能包含用户名中超过两个连续字符的部分。

3. （可选）设置密码。
仅当“登录凭证”选择“密码”时，会显示该参数。
根据[表2-29](#)完成“密码”和“确认密码”的设置，两次输入需保持一致。
4. （可选）设置“密钥对”。
仅当“登录凭证”选择“密钥对”时，会显示该参数。通过下拉列表选择可用的密钥对，或参考[（推荐）通过管理控制台创建密钥对](#)新建密钥对。

 说明

如果选择使用已有的密钥，请确保您已在本地获取该文件，否则，将影响您正常登录弹性云服务器。

5. （可选）企业项目
该参数针对企业用户使用。如需使用该功能，请联系客服申请开通。

企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理，默认项目为default。

请从下拉列表中选择所在的企业项目。更多关于企业项目的信息，请参见[进入企业中心](#)。

6. （可选）设置“标签”。

如需通过标签管理ECS资源时，可以为ECS添加标签。

标签用于标识弹性云服务器，可以方便识别和管理您拥有的ECS资源。您最多可以给弹性云服务器添加10个标签。

更多信息，请参见[标签概述](#)。

 说明

创建弹性云服务器时添加的标签，将同步添加至一同创建的EIP和云硬盘（包括系统盘、数据盘）上。如果云服务器使用的是已有EIP，则该标签不会在EIP上标识。

如您的组织已经设定弹性云服务器的相关标签策略，则需按照标签策略规则为弹性云服务器添加标签。如果添加的标签不符合标签策略规则，则可能会导致弹性云服务器创建失败，请联系组织管理员了解标签策略详情。

云服务器创建成功后，您可以在弹性云服务器、EIP和云硬盘详情页，查看到对应的标签。

高级配置

1. 设置“云监控”。

选择部分操作系统的公共镜像时，系统推荐您配套使用主机监控。主机监控采集丰富的操作系统层面监控指标，用于监控服务器资源使用情况，也可查询数据用于资源的故障排查。

勾选“开启详细云监控”后，通过在云服务器中安装Agent插件，支持对云服务器的CPU、内存、网络、磁盘、进程等指标的1分钟详细监控。

安装Agent后的监控指标请参考[弹性云服务器支持的操作系统监控指标（安装Agent）](#)。

2. 设置“云服务器组（可选）”

云服务器组内的弹性云服务器将遵循反亲和策略或故障域策略，尽量分散地创建在不同主机上。创建云服务器组的详细操作，请参见[管理云服务器组](#)。

 说明

包含本地盘的弹性云服务器无法在创建后加入弹性云服务器组，如需使用弹性云服务器组功能，请在创建时选择弹性云服务器组。

3. 设置“云服务器描述”信息。

4. 设置“实例自定义数据注入”。

用于在创建ECS时，通过注入自定义数据配置ECS，例如，通过脚本初始化操作系统。配置后，ECS首次启动时会自行注入数据信息。

– 以文本形式：在下方文本框内输入用户数据内容。

– 以文件形式：主要用于创建云服务器时注入的脚本文件或其他文件。

实例自定义数据注入的详细操作，请参见[通过实例自定义数据配置ECS实例](#)。

5. 设置“委托”。

当需要与其他账号共享云服务器资源，或者委托更专业的人或团队来代为管理时，租户管理员可以在IAM创建委托并授予云服务器资源的管理权限。被委托方使用自己的用户登录系统后，切换到您的账号下管理资源，避免您将自己的安全凭证（密码）共享给其他账号，确保了您的账号安全。

如果您在IAM上创建了委托，可以通过单击下拉列表选择委托名称，获取相应权限。更多关于委托的信息，请参见[委托其他账号管理资源](#)。

6. 设置“CPU选项”。
 - 当需要为云服务器实例开启或关闭超线程时，勾选“指定CPU选项”。
关于超线程的详细介绍，请参见[开启/关闭ECS超线程](#)。
 - 每核心线程数
当勾选“指定CPU选项”时，显示该参数。在“每核心线程数”下拉框进行设置。
 - 1: 关闭超线程
 - 2: 开启超线程，默认开启

购买量

1. （可选）设置“购买时长”。
仅当“计费模式”选择“包年/包月”时，会显示该参数。用于设置ECS的购买时长，最短为1个月，最长为3年。
2. （可选）设置“自动续费”。
仅当“计费模式”选择“包年/包月”时，会显示该参数。
勾选“自动续费”，在“包年/包月”资源到期后，可以自动进行续费。
 - 按月购买的资源：每次续费1个月，次数不限。
 - 按年购买的资源：每次续费1年，次数不限。关于自动续费的更多说明，请参考[自动续费规则说明](#)。
3. （可选）设置“使用时长”。
仅当“计费模式”选择“按需计费”或“竞价计费”时，会显示该参数。勾选“设置定时删除时间”后，可以在设定时间自动删除云服务器。

须知

设置定时删除时间后，系统将在设定时间自动删除云服务器，请提前做好数据备份，谨慎操作。

设置的删除时间需晚于当前时间1小时，且不能超过3年。设置后还可以在实例删除前修改定时删除时间。

系统每5分钟执行一次定时删除任务，按照系统删除服务器的时间停止计费。

4. 设置“购买数量”。
如需批量购买ECS，可以设置购买ECS的数量。设置后，会批量创建多台相同配置的ECS。
系统会显示您当前还可以购买的ECS数量。为了保证所有资源的合理分配，如果您需要的ECS数量超过当前可以购买的最大数值，可以[申请扩大配额](#)。

说明

您也可以在购买页底部进行设置：

- 当“计费模式”选择“包年/包月”时，可设置“购买量”和“购买时长”。
- 当“计费模式”选择“按需计费”或“竞价计费”时，可设置“购买量”。

设置完成后，可以通过“配置费用”查看具体收费项。如果您对价格有疑问，可通过[了解计费详情](#)来了解产品价格。

步骤三：确认配置并购买 ECS

1. 在页面右侧的“配置概要”中，查看ECS配置详情。
未设置的必选字段会通过红色字体进行提示，需在参数配置区域进行设置。
2. （可选）单击“生成Open API”。
仅当需要生成Java、Python、Go、.NET、NodeJs、PHP、C++等编程语言的最佳实践脚本时，可执行本步骤。
如下配置信息暂不支持生成：
 - 故障域（云服务器组策略）
 - 弹性公网IP随实例释放
 - 弹性网卡
 - 数据盘随实例释放
 - 系统盘和数据盘加密
 - 云备份
3. （可选）保存为启动模板。
仅当需要通过本配置创建启动模板，用于创建新的ECS时，可执行本步骤。更多信息，请参见[通过智能购买助手购买ECS](#)。
包含以下任一配置项时均不支持保存为启动模板：计费模式为包年/包月、竞价类型为竞享模式、配置了主机安全、登录凭证为密码。
4. 勾选协议并单击“立即购买”。
ECS创建成功后会默认开机。

后续操作

- 连接ECS
支持通过多种方式连接实例，具体操作，请参见[登录Windows ECS](#)和[登录Linux ECS](#)。
- 初始化数据盘
如果您在创建实例时一并创建了数据盘，需要先对数据盘进行初始化才能正常使用。具体操作，请参见[初始化数据盘](#)。
- ECS实践
购买ECS后，可以根据业务需要搭建不同的环境、网站或应用。ECS常见的搭建实践，请参见[ECS最佳实践汇总](#)。

2.3.4 购买竞价计费型 ECS

操作场景

竞价计费型实例采用竞价计费模式，以一定折扣购买并使用弹性云服务器，性能与常规云服务器无异。但是当库存资源不足，或市场价格上浮、并超过您的预期价格时，系统会自动释放您的云服务器资源，对这些折扣售卖的弹性云服务器进行中断回收。

与“按需计费”和“包年/包月”方式购买的弹性云服务器相比，在提供同等性能的前提下，竞价计费型实例可提供超低折扣，降低用云成本。

更多关于竞价计费型实例的介绍，请参见[竞价计费（竞价模式）](#)。

约束与限制

- 当前仅支持虚拟化类型为KVM的弹性云服务器使用竞价计费型实例策略。具体的规格支持清单，请以控制台显示的资源为准。
- 在不同可用区，同一规格的云服务器市场价格变化可能不同。
- 使用竞价计费型实例策略的弹性云服务器，不支持切换操作系统功能。
- 使用竞价计费型实例策略的弹性云服务器，不支持自动恢复功能。
- 使用竞价计费型实例策略的弹性云服务器，不支持变更规格。
- 不支持使用市场镜像创建竞价计费型实例。
- 竞价计费型实例不支持转“包年/包月”方式。
- 竞价计费型实例不支持卸载系统盘。
- 竞价计费型实例在中断回收时：
 - 不允许使用该竞价计费型实例制作系统盘镜像和整机镜像，但允许使用该云服务器的数据盘制作数据盘镜像。
 - 不允许删除。
- 竞价计费型实例在中断回收时，数据盘和弹性公网IP默认不释放。请设置通知提醒，来决定是否释放关联的数据盘和弹性公网IP。

购买云服务器

请按照[自定义购买ECS](#)、[Windows ECS登录方式概述](#)或[Linux ECS登录方式概述](#)的描述，购买并登录竞价计费型实例。但是，如下参数的设置请特别注意：

创建竞价计费型实例时，如下参数的设置请特别注意：

- 计费模式：选择“竞价计费”。
相对于按需计费模式，以更低的折扣按实际使用时长计费。但是，华为云会根据市场价格或供需资源变化随时自动释放竞价计费型实例。
- 出价模式：包括“自动设置”和“手动设置”。
 - 自动设置：推荐使用，指将按需计费的价格设置为价格上限。即您愿意为弹性云服务器支付的最高价格是按需计费的价格。
 - 手动设置：需要您自己设定竞价计费型实例的价格上限。该上限值需大于等于当前的市场价格，小于等于按需计费的价格。
- 单击“立即购买”，确认规格和价格无误后，勾选同意协议，并单击“提交”。

说明

竞价计费型实例购买成功后，始终可能会被系统中断回收。因此，请务必做好数据备份工作。

配置中断回收提醒（可选）

竞价计费型实例购买成功后，您可以像使用云上其他云服务器一样，正常使用竞价计费型实例。但是，华为云会根据市场价格或供需资源变化随时自动释放竞价计费型实例，终止实例的使用。

当“报价 < 市场价格”或库存资源不足时，系统发出即将释放云服务器资源的通知，并在约5分钟后自动中断回收弹性云服务器。您可以通过如下方式配置中断回收提醒：

通过“云审计服务”、“消息通知服务”，查看并设置中断回收提醒。操作步骤类似如下，具体操作请以《云审计服务用户指南》为准：

- 步骤1 开通“云审计服务”，具体操作请参见“[开通云审计服务](#)”。
- 用户开通云审计服务后，系统会自动识别当前云平台上所开通的云服务，自动抓取各云服务的各项关键操作并主动向云审计服务上报各项关键操作的审计日志。
- 步骤2 配置中断回收通知。

云审计服务在记录某些特定关键操作发生时，支持对这些关键操作通过消息通知服务实时向相关订阅者发送通知，该功能由云审计服务触发，消息通知服务（SMN）完成通知发送。

1. 登录控制台。
2. 单击管理控制台左上角的，选择区域和项目。
3. 选择“管理与监管 > 云审计服务”。
4. 单击左侧导航树的“关键操作通知”。
5. 单击页面右上角的“创建关键操作通知”，并按[表2-30](#)填写参数配置。

表 2-30 创建关键操作通知

参数类型	参数	参数配置
基本信息	通知名称	用户自定义，如spottest。
配置操作	操作类型	选择“自定义操作”。
	操作列表	依次选择“ECS > server > interruptServer”，并单击“添加”。
配置用户	指定用户	选择“不指定”，此时，云审计服务默认指定对所有用户发起的关键操作进行通知。
配置SMN主题	发送通知	选择“发送”。

参数类型	参数	参数配置
	SMN主题	在下拉列表中选择SMN发送通知的主题，用于华为云中中断回收竞价计费型实例时，系统发送通知使用。如果没有合适的SMN主题，请新建主题： 1. 单击“消息通知服务”，跳转至消息通知服务页面。 2. 单击“创建主题”，根据界面提示新建一个主题，如“spot”。具体操作请参见“ 创建主题 ”。 3. 主题创建成功后，单击“主题”列表页“操作”列下的“添加订阅”，接收发布至主题的消息。具体操作请参见“ 订阅主题 ”。

配置成功后，当删除实例时，您将提前5分钟收到系统发出的提醒。

步骤3 （可选）查看中断回收实例。

- 1. 选择“管理与监管 > 云审计服务”。
- 2. 单击左侧导航树的“事件列表”。
- 3. 事件列表支持通过筛选来查询对应的操作事件。请展开“筛选”下拉框，按[表 2-31](#)选择查询条件，并单击“查询”。

表 2-31 查询中断回收实例

参数	参数配置
事件来源	ECS
资源类型	server
筛选类型	按事件名称 > interruptServer
操作用户	所有操作用户
事件级别	所有事件级别

- 4. 在需要查看的事件左侧，展开该记录的详细信息。
- 5. 在需要查看的记录右侧，单击“查看事件”，弹窗显示该操作事件结构的详细信息。

----结束

2.3.5 购买竞享计费型 ECS

操作场景

竞享实例采用竞价计费模式，以一定折扣购买并使用弹性云服务器，性能与常规云服务器无异。但是当库存资源不足，系统会自动释放您的云服务器资源，对这些折扣售卖的弹性云服务器进行中断回收。

与“按需计费”和“包年/包月”方式购买的弹性云服务器相比，在提供同等性能的前提下，竞享实例可提供超低折扣，降低用云成本。

更多关于竞享实例的介绍，请参见[竞价计费（竞享模式）](#)。

约束与限制

- 竞享计费型实例目前支持通用计算增强型实例规格。
- 华为云尽可能保障竞享实例正常运行，但在系统资源不足等极端情况下会主动释放实例，请务必做好数据备份工作。
- 竞享计费型实例目前只支持部分区域及规格，请以购买页面显示的资源为准
- 竞享计费型实例保障周期不同价格不同。
- 竞享计费型实例不支持转换为按需和包年/包月实例。
- 竞享计费型实例不支持变更实例规格。
- 竞享计费型实例不支持变更操作系统。
- 竞享计费型实例不支持自动恢复功能。
- 竞享计费型实例不支持卸载系统盘。
- 竞享计费型实例在中断回收时：
 - 不允许使用竞享实例制作系统盘镜像和整机镜像，但允许使用该云服务器的数据盘制作数据盘镜像。
 - 不允许删除。
- 竞享计费型实例在中断回收时，数据盘和弹性公网IP默认不释放。请设置通知提醒，来决定是否释放关联的数据盘和弹性公网IP。

购买云服务器

请按照[自定义购买ECS](#)、[Windows ECS登录方式概述](#)或[Linux ECS登录方式概述](#)的描述，购买并登录竞享计费型实例。但是，如下参数的设置请特别注意：

创建竞享实例时，如下参数的设置请特别注意：

- 计费模式：选择“竞价计费”。
相对于按需计费模式，以更低的折扣按实际使用时长计费。但是当库存资源不足，系统会自动释放您的云服务器资源，请务必做好数据备份。
- 竞价类型：选择“竞享模式”。
- 选择“保障周期”和“保障周期数量”。
保障周期是购买竞享实例的最小单位时间。在保障周期内由云平台中断竞享实例，当前周期不计费。在保障周期内用户删除竞享实例，当前周期按使用时长计费。
- 单击“立即购买”，确认规格和价格无误后，勾选同意协议，并单击“提交”。

说明

竞享实例购买成功后，始终可能会被系统中断回收。因此，请务必做好数据备份工作。

配置中断回收提醒

竞享实例购买成功后，您可以像使用其他云服务器一样，正常使用竞享实例。但是，当使用时间到达您的购买时长或在系统资源不足等极端情况下，系统会自动回收实例。您可以通过如下方式配置中断回收提醒：

通过“云审计服务”、“消息通知服务”，查看并设置中断回收提醒。操作步骤类似如下，具体操作请以《云审计服务用户指南》为准：

- 步骤1** 开通“云审计服务”，具体操作请参见“[开通云审计服务](#)”。
- 用户开通云审计服务后，系统会自动识别当前云平台上所开通的云服务，自动抓取各云服务的各项关键操作并主动向云审计服务上报各项关键操作的审计日志。
- 步骤2** 配置中断回收通知。

云审计服务在记录某些特定关键操作发生时，支持对这些关键操作通过消息通知服务实时向相关订阅者发送通知，该功能由云审计服务触发，消息通知服务（SMN）完成通知发送。

1. 登录控制台。
2. 单击管理控制台左上角的，选择区域和项目。
3. 选择“管理与监管 > 云审计服务”。
4. 单击左侧导航树的“关键操作通知”。
5. 单击页面右上角的“创建关键操作通知”，并按[表2-32](#)填写参数配置。

表 2-32 创建关键操作通知

参数类型	参数	参数配置
基本信息	通知名称	用户自定义，如spottest。
配置操作	操作类型	选择“自定义操作”。
	操作列表	依次选择“ECS > server > interruptServer”，并单击“添加”。
配置用户	指定用户	选择“不指定”，此时，云审计服务默认指定对所有用户发起的关键操作进行通知。
配置SMN主题	发送通知	选择“发送”。
	SMN主题	在下拉列表中选择SMN发送通知的主题，用于华为云中中断回收竞价计费型实例时，系统发送通知使用。如果没有合适的SMN主题，请新建主题： 1. 单击“消息通知服务”，跳转至消息通知服务页面。 2. 单击“创建主题”，根据界面提示新建一个主题，如“spot”。具体操作请参见“ 创建主题 ”。 3. 主题创建成功后，单击“主题”列表页“操作”列下的“添加订阅”，接收发布至主题的消息。具体操作请参见“ 订阅主题 ”。

配置成功后，当删除实例时，您将提前5分钟收到系统发出的提醒。

步骤3 （可选）查看中断回收实例。

- 1. 选择“管理与监管 > 云审计服务”。
- 2. 单击左侧导航树的“事件列表”。
- 3. 事件列表支持通过筛选来查询对应的操作事件。请展开“筛选”下拉框，按表 2-33选择查询条件，并单击“查询”。

表 2-33 查询中断回收实例

参数	参数配置
事件来源	ECS
资源类型	server
筛选类型	按事件名称 > interruptServer
操作用户	所有操作用户
事件级别	所有事件级别

- 4. 在需要查看的事件左侧，展开该记录的详细信息。
- 5. 在需要查看的记录右侧，单击“查看事件”，弹窗显示该操作事件结构的详细信息。

----结束

2.3.6 通过私有镜像购买 ECS

操作场景

私有镜像是由用户创建或导入的个人镜像，仅用户自己可见。包含操作系统、预装的公共应用以及用户的私有应用，可以节省重复配置ECS的时间。

使用公共镜像和私有镜像创建云服务器云主机的区别是：

- 公共镜像：创建的云服务器云主机包含所需操作系统和预装的公共应用，需要您自行安装应用软件。
- 私有镜像或共享镜像：创建的云服务器云主机包含操作系统、预装的公共应用以及用户的私有应用。

说明

您可以选择使用加密镜像，更多关于镜像加密的信息，请参见[镜像加密](#)。

约束与限制

- 如果选择使用整机镜像创建弹性云服务器，整机镜像关联的云硬盘不支持使用“数据盘镜像创建磁盘”功能。
- 当整机镜像为可用区内可用时（状态栏为“正常”，且提示“AZx可用”），那么该整机镜像只能在该可用区中创建云服务器，且云服务器系统盘和数据盘的加密属性会和原始云服务器的系统盘和数据盘的加密属性保持一致，不支持在创建时修改系统盘和数据盘的SCSI模式、共享属性、加密属性。

- 当整机镜像为区域内可用时（状态栏为“正常”，且未提示“AZx可用”），那么该整机镜像可以在整个区域内创建云服务器，且云服务器系统盘和数据盘的加密属性会和原始云服务器的系统盘和数据盘的加密属性保持一致，支持在创建时修改数据盘的SCSI模式、共享属性、加密属性。
- 不支持选择使用ISO文件注册的ISO镜像创建弹性云服务器，必须完成操作系统及驱动安装将ISO镜像做成系统盘镜像后才能使用。
- ISO镜像创建的云服务器只建议用来装机，部分功能受限。如：不支持挂载磁盘操作。
- 为了确保使用私有镜像创建的弹性云服务器开启网卡多队列功能，建议您在创建私有镜像时完成网卡多队列的配置。弹性云服务器开启网卡多队列功能可以将弹性云服务器中的网卡中断分散给不同的CPU处理，以满足网卡的需求，从而提升网络PPS和带宽性能。

详细操作请参考[如何设置镜像的网卡多队列属性？](#)

操作步骤（通过 ECS 购买页）

1. 登录控制台，进入[购买弹性云服务器](#)页面。
2. 根据业务需要，设置计费模式、区域、可用区等基础配置、选择实例。
3. 在“操作系统”区域，选择“私有镜像”页签。

图 2-14 私有镜像参数设置



4. 通过下拉列表，选择私有镜像。
 5. 继续设置其他购买ECS相关参数，完成ECS的购买。
- 其余参数的设置的详细内容，请参见[自定义购买ECS](#)。

操作步骤（通过 IMS 列表页）

1. 登录控制台，进入[私有镜像](#)页面。
2. 在镜像所在行的“操作”列下，单击“申请服务器”，进入“购买弹性云服务器”页面。

图 2-15 申请云服务器

名称ID	状态	操作系统类型	操作系统	镜像类型	磁盘容量 (GiB)	加密	创建时间	操作
image-example 60ced7a5-551f-4f52-9...	正常	Linux	CentOS 7.5 64bit	ECS系统盘镜像(80)	40	否	2023/08/31 19:33:14...	申请服务器 修改 更多

3. 根据业务需要，在“购买弹性云服务器”页面完成参数的设置。
- 参数设置的详细内容，请参见[自定义购买ECS](#)。

说明

- 使用系统盘私有镜像创建ECS时，ECS的规格可以重新设置，系统盘的类型也可以重新选择，但系统盘的容量只能设置为大于镜像的系统盘。
- 使用整机私有镜像创建ECS时，如果整机镜像中包含了一块或多块数据盘，系统会自动设置好数据盘参数。您可以增加系统盘和数据盘容量，但不能缩小。
- 如果整机镜像中包含多块数据盘，需要加载一段时间才能正常显示系统盘信息，请耐心等待。

后续操作

通过私有镜像购买的ECS，可能因缺少插件而无法重置密码，请检查安装一键式重置密码插件。

详细内容，请参见[安装单台ECS的一键式重置密码插件（单台操作）](#)。

2.3.7 通过智能购买助手购买 ECS

操作场景

智能购买助手支持跨计费模式和可用区部署不同类型实例，包含启动模板和智能购买组。

- 启动模板是一种用于快速购买ECS的工具，包含了用于创建ECS的除密码之外的任意配置信息，可以批量购买相同配置的ECS。
更多信息，请参见[启动模板管理](#)。
- 智能购买组是一种新的算力获取方式，通过启动模板的自定义配置，可以批量购买不同可用区、不同实例类型以及不同计费模式的ECS。
更多信息，请参见[智能购买组管理](#)。

约束与限制

- 支持的区域包括：华北-乌兰察布一、华东-上海一、华东-上海二、华南-广州、西南-贵阳一。
- 仅支持跨可用区部署ECS实例，不支持跨区域部署ECS实例。
- 通过智能购买组部署ECS实例，其目标容量限制：
 - 以实例个数为目标容量：最多创建500台实例。
 - 以vCPUs为目标容量：最大创建40000vCPUs。
- 每个智能购买组最多指定一个启动模板。
- 智能购买组免费，但通过智能购买组创建的实例正常计费。

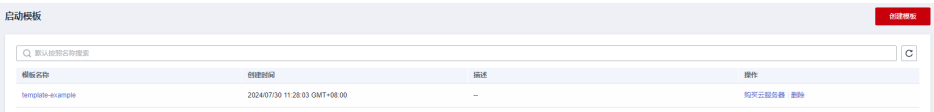
前提条件

已创建实例启动模板。具体操作，请参见[创建启动模板](#)。

通过启动模板快速购买 ECS

1. 在启动模板列表中，单击“操作”列的“购买云服务器”，进入“购买弹性云服务器”页面。

图 2-16 启动模板列表



2. 在“购买弹性云服务器”页面，已根据启动模板的配置信息，预设了购买ECS的参数，您可以根据业务需要进行修改。
例如，修改“登录凭证”方式为“密码”，并设置ECS的密码。
参数设置的详细内容，请参见[自定义购买ECS](#)。
3. 在购买页右侧的“配置概要”中，确认配置信息。
4. 确认无误后，勾选协议并单击“立即购买”。
ECS创建成功后会默认开机。

通过智能购买组跨计费模式和可用区购买 ECS

1. 登录控制台，进入[创建智能购买组](#)页面。
2. 设置智能购买组的名称、目标容量以及按需实例容量。

图 2-17 智能购买组

智能购买组名称

alg-example

目标容量

实例个数

—

5

+

?

☒ 使用按需实例提供部分算力

按需实例容量

—

3

+

实例个数

表 2-34 参数设置说明

参数	示例	说明
智能购买组名称	alg-example	智能购买组的名称。 长度为2~64个字符，只能包含中文、字母、数字、下划线（_）和中划线（-）。
目标容量	实例个数，5	用于设置使用智能购买组购买的实例目标总容量。 您可以通过目标容量指定智能购买组交付的算力总和，支持设置为实例个数或vCPU数量。每个智能购买组的目标容量限制： - 如果以实例个数为目标容量最多创建500台实例。 - 如果以vCPUs为目标容量最大创建40000vCPUs。

参数	示例	说明
按需实例容量	3	仅当勾选“使用按需实例提供部分算力”时，会显示该参数。 用于设置按需实例的容量，取值小于等于“目标容量”。

3. 设置启动模板、实例配置及实例分配策略。

图 2-18 实例配置信息



表 2-35 参数设置说明

参数	示例	说明
启动模板	alg-example	用于设置智能购买组在创建实例时，选择启动模板作为配置信息的来源。 通过“展开启动模板详情”可查看所选启动模板的具体配置信息。
实例配置	可用区1，s7.medium.2	用于在启动模板配置信息基础上自定义“指定可用区”和“规格”。 支持添加多个实例自定义配置，推荐您选择多个不同可用区和实例规格，提升资源交付的成功率。

参数	示例	说明
实例分配策略	最低价格策略	用于设置实例分配遵循的策略。 - 最低价格策略：智能购买组购买的所有实例的价格总和最低。 - 多可用区均衡策略：智能购买组购买的实例在多个可用区之间均匀分配算力。 - 容量优化策略：智能购买组购买的实例按照大规格优先的原则进行购买。即目标容量为实例个数时智能购买组的vCPU容量最大；目标容量为vCPU大小时智能购买组的实例个数最小。

4. 设置智能购买组类型、启动/结束时间等参数。

图 2-19 智能购买组信息

智能购买组类型

一次性交付

持续保持

?

启动时间

立即启动

指定启动时间

?

结束时间

无限期

指定结束时间

?

全局竞价实例的价格上限

☒

 设定价格上限

?

全局竞价实例的价格上限

¥

0.12

/小时

组内释放设置

☒

 智能购买组过期时释放实例

?

☒

 超过容量时释放实例

?

表 2-36 参数设置说明

参数	示例	说明
智能购买组类型	一次性交付	用于设置智能购买组的类型。 - 一次性交付：智能购买组仅在启动时尝试一次性创建目标容量的实例，即使未达到目标容量也不再重试。 - 持续保持：智能购买组实时监控当前集群的容量与目标容量，如未达到目标容量继续创建实例，直至满足目标容量。

参数	示例	说明
启动时间	立即启动	用于设置智能购买组开始创建实例的时间。 - 立即启动：智能购买组创建成功后立即启动。 - 指定启动时间：自定义智能购买组的启动时间。
结束时间	无限期	与启动时间相结合，用于设置智能购买组的有效时间。 - 无限期：智能购买组长期有效。 - 指定结束时间：自定义智能购买组的过期时间。
全局竞价实例的价格上限	0.12	仅当勾选了“设定价格上限”时，会显示该参数。用于设置智能购买组内竞价实例的价格上限。 当智能购买组内某一竞价实例的市场价格高于该价格上限时，该竞价实例将被中断回收。如果同时设置了单个竞价实例的价格上限和全局竞价实例的价格上限，则以单个竞价实例的价格上限为准。
组内释放设置	- 智能购买组过期时释放 - 实例超过容量时释放实例	当设置了智能购买组的结束时间时，该参数有效。 - 智能购买组过期时释放：当智能购买组超过有效时间，即删除组内实例。 - 实例超过容量时释放实例：当智能购买组的实例个数/vCPU之和超过目标容量时，即删除超出容量的实例。

5. 单击“立即创建”，开始创建实例。

2.3.8 通过规格选型引导购买 ECS

操作场景

购买弹性云服务器时，您需要根据业务需求指定CPU、内存、规格、操作系统、登录鉴权方式等具体配置。华为云提供了多种实例类型供您选择，不同类型的实例提供不同的计算能力和存储能力。支持的实例类型，请参见[实例类型](#)。

弹性云服务器的“帮我选”功能，提供规格选型引导，针对不同业务场景和预期业务量，进行规格推荐，帮助您快速选择规格。

购买弹性云服务器的详细内容，请参见[自定义购买ECS](#)。本文介绍如何通过“帮我选”的规格选型引导进行规格筛选的操作指导。

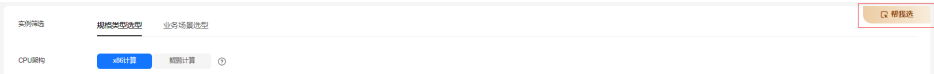
约束与限制

- 支持传统办公、网站应用、电商等场景的规格选型引导，其他业务场景请在购买页自行选择规格。
- 支持规格选型引导的区域，请参见[功能总览](#)。
- 包年/包月和按需计费的弹性云服务器支持规格选型引导。

操作步骤

1. 登录控制台，进入[购买弹性云服务器](#)页面。
2. 根据业务需要，完成区域、计费模式、可用区等基础配置的设置。
3. 在“实例筛选”区域右上角，单击“帮我选”。

图 2-20 帮我选



4. 在“帮我选”页面根据业务场景进行设置。
 - 选择“传统办公”业务场景。

图 2-21 传统办公场景



- i. 设置业务预期用户数：根据登录或使用某软件系统的总用户数量的范围进行设置。
 - ii. 设置业务预期并发量：根据同一时间，每秒同时访问软件系统的用户数量的范围进行设置。

如果业务预期并发量达到200以上，请[联系售前](#)获取专业咨询服务。
 - iii. 单击“下一步”，在推荐规格中进行选择。
 - iv. 单击“确认选择”，完成规格设置。

如果您对推荐规格不满意，还可以在规格列表中直接选择其他规格。
- 选择“网站应用”业务场景。

图 2-22 网站应用场景



- i. 根据业务需要，选择对应的网站类型。
 - ii. （可选）设置业务预期用户数：根据登录或使用小程序的总用户数量的范围进行设置。
当“网站类型”选择“营销类小程序”时，该参数可见。
 - iii. （可选）设置业务预期并发量：根据同一时间，每秒同时访问小程序的用户数量的范围进行设置。
当“网站类型”选择“营销类小程序”时，该参数可见。
如果业务预期并发量达到200以上，请[联系售前](#)获取专业咨询服务。
 - iv. 单击“下一步”，在推荐规格中进行选择。
 - v. 单击“确认选择”，完成规格设置。
如果您对推荐规格不满意，还可以在规格列表中直接选择其他规格。
- 选择“电商”业务场景。

图 2-23 电商场景



- i.

（可选）若有“秒杀/直播带货”需求，则勾选“是”。
- ii.

设置业务预期日活跃用户数：根据日登录或使用电商平台的活跃用户数（去除重复登录的用户）的范围进行设置。
如果业务预期日活跃用户数达到5000以上，请[联系售前](#)获取专业咨询服务。
- iii.

设置业务预期并发量：根据同一时间，每秒同时访问电商平台的用户数量的范围进行设置。
如果业务预期并发量达到200以上，请[联系售前](#)获取专业咨询服务。
- iv.

单击“下一步”，在推荐规格中进行选择。
- v.

单击“确认选择”，完成规格设置。
如果您对推荐规格不满意，还可以在规格列表中直接选择其他规格。

2.3.9 通过共享 VPC 购买 ECS

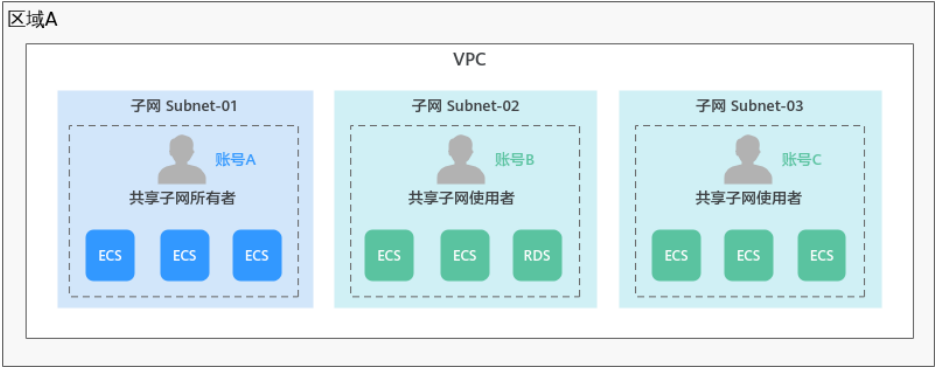
操作场景

购买ECS时，您可以通过共享VPC功能，使用其他账号共享的VPC和子网，以实现网络资源的共享和统一管理，提升资源管控效率、降低运维成本。

例如，为了规范管理网络资源，某企业使用账号A作为IT管理账号，用于管理基础公共资源，包括VPC、子网等。同时，账号A将多个子网共享给其他账号共同使用。

- 账号A：IT管理账号，作为资源所有者，创建VPC及子网，并将多个子网分别共享给其他账号使用。
- 账号B：业务账号，作为资源使用者，使用账号A共享的子网2创建ECS。
- 账号C：业务账号，作为资源使用者，使用账号A共享的子网3创建ECS。

图 2-24 业务规划示意图



本章节介绍通过共享VPC购买ECS的操作指导。有关VPC子网共享的更多信息，请参见《虚拟私有云用户指南》的“[共享VPC](#)”相关内容。

约束与限制

- 单个资源使用者最多可同时接收100个共享子网，当共享子网数量超过100个时，使用者将无法接收到超出数量的共享子网。
- 共享VPC功能不计费，资源使用者只需要为自己所创建的资源付费。

前提条件

作为资源所有者的账号A已创建共享VPC和子网，并指定资源使用者为账号B。创建共享的详细操作，请参见[创建共享](#)。

操作步骤

1.

以账号B登录控制台，进入[资源访问管理](#)页面，接受共享邀请。
详细内容，请参见[接受/拒绝共享邀请](#)。
2.

进入[购买弹性云服务器](#)页面。
3.

根据业务需要，完成购买ECS的基础配置、网络配置以及高级配置等各项参数的设置。
设置“网络”相关参数时，选择由账号A共享的VPC和子网。

图 2-25 设置网络参数



其余配置，请参见[自定义购买ECS](#)。

2.3.10 购买相同配置 ECS

操作场景

对于已购买成功的弹性云服务器，如需再次购买相同配置的，建议您使用“购买相同配置”功能，快速购买同一配置的弹性云服务器，节省时间。

约束与限制

超大内存型弹性云服务器，暂不支持使用“购买相同配置”功能。

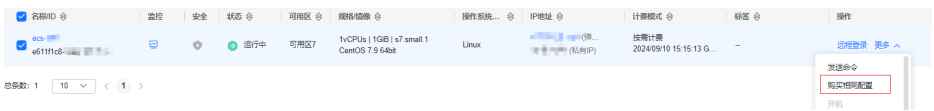
操作步骤

1.

登录控制台，进入[弹性云服务器](#)页面。
2.

选择目标弹性云服务器，并单击“操作”列下的“更多 > 购买相同配置”。

图 2-26 购买相同配置



系统跳转至“购买弹性云服务器”页面，并自动复制已选择云服务器的参数配置。

3.

根据需要调整待购买ECS的参数配置。
参数设置的详细内容，请参见[自定义购买ECS](#)。

4. 确认无误后，勾选协议并单击“立即购买”。

说明

为安全起见，当复制的弹性云服务器存在如下场景时，系统不会自动复制相应的参数配置，需用户手动配置：

- 数据盘个数超过10个时，需手动添加磁盘数量。
- 网卡个数超过5个时，需手动添加其余网卡。
- 安全组个数超过5个时，需手动添加其余安全组。
- 使用数据盘镜像创建的磁盘，需重新选择数据盘镜像。
- 使用整机镜像创建的弹性云服务器，默认只显示整机镜像关联的磁盘，需手动添加新增磁盘。
- 使用磁盘加密功能的云硬盘，需重新勾选“加密”。
- “高级配置”中的相关功能，需重新设置。

2.4 登录 Windows ECS

2.4.1 Windows ECS 登录方式概述

约束与限制

- 只有运行中的云服务器才允许用户登录。
- Windows操作系统用户名“Administrator”。
- 忘记密码，请先通过“重置密码”功能设置登录密码。

重置密码：选中待重置密码的云服务器，并选择“操作”列下的“更多 > 重置密码”。详细操作，请参见[在控制台重置ECS密码](#)。

- 对于密钥方式鉴权的弹性云服务器，需先通过管理控制台提供的获取密码功能，将创建弹性云服务器时使用的私钥文件解析为密码。
- GPU实例中，部分G系列实例不支持云平台提供的远程登录功能，需要自行安装VNC Server进行登录。详细信息请参见[GPU加速型](#)。推荐使用MSTSC方式登录弹性云服务器。
- 使用MSTSC方式访问GPU加速型弹性云服务器时，使用WDDM驱动程序模型的GPU将被替换为一个非加速的远程桌面显示驱动程序，造成GPU加速能力无法实现。因此，如果需要使用GPU加速能力，您必须使用不同的远程访问工具，如VNC工具。如果使用管理控制台提供的“远程登录”功能无法满足您的访问需求，请自行在弹性云服务器上安装符合要求的远程访问工具（如Tight VNC）。

Tight VNC下载地址：<https://www.tightvnc.com/download.php>

登录方式概述

请根据需求选择登录方式，登录云服务器。

表 2-37 Windows 云服务器登录方式一览

云服务器操作系统	本地主机操作系统	连接方法	条件
Windows	Windows	（推荐使用）使用控制台提供的RDP文件登录云服务器。 通过RDP文件登录Windows ECS。	云服务器绑定弹性公网IP （通过内网登录云服务器时可以不绑定弹性公网IP，例如VPN、云专线等内网网络连通场景。）
	Windows	使用mstsc方式登录云服务器。 在本地主机单击“开始”菜单，输入mstsc命令，打开远程桌面对话框。 通过本地Windows主机登录Windows ECS。	
	Linux	安装远程连接工具，例如rdesktop，执行连接命令。 通过本地Linux主机登录Windows ECS。	
	macOS系统	安装远程连接工具，例如Microsoft Remote Desktop for Mac在macOS系统上登录。 通过本地macOS主机登录Windows ECS。	
	移动设备	安装远程连接工具，例如Microsoft Remote Desktop在移动设备上登录。 通过移动设备登录Windows ECS。	
	Windows	使用管理控制台远程登录方式： 通过控制台VNC登录Windows ECS。	不依赖弹性公网IP

相关链接

- [忘记密码怎么办？](#)
- [Windows云服务器如何配置多用户登录？](#)
- [无法登录到Windows云服务器怎么办？](#)

2.4.2 通过控制台 VNC 登录 Windows ECS

操作场景

本节为您介绍如何通过控制台提供的远程登录功能（即VNC方式）登录到弹性云服务器上。

当您无法使用RDP文件、MSTSC或其他远程登录工具连接弹性云服务器时，可以选择通过VNC方式进行登录，该登录方式主要用于紧急运维场景，可查看弹性云服务器状态或进行相关维护操作。

前提条件

如果您的弹性云服务器是采用密钥方式鉴权，请在登录前先使用密钥文件解析登录密码。密钥文件解析密码请参考[获取Windows弹性云服务器的密码](#)。

登录 Windows 弹性云服务器

1. 登录管理控制台。

2. 单击管理控制台左上角的，选择区域和项目。

3. 单击“”，选择“计算 > 弹性云服务器”。

4. 获取弹性云服务器密码。
VNC方式登录弹性云服务器时，需已知其密码，然后再采用VNC方式登录。
 - 当您的弹性云服务器是采用密码方式鉴权时，请直接使用创建云服务器时设置的密码进行登录。
 - 当您的弹性云服务器是采用密钥方式鉴权时，密码获取方式请参见[获取Windows弹性云服务器的密码](#)。

5. 选择要登录的弹性云服务器，单击“操作”列下的“远程登录”。

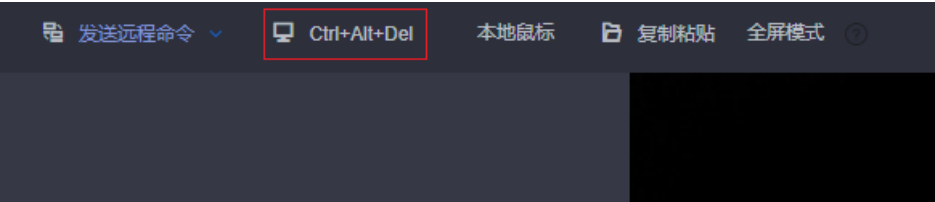
图 2-27 远程登录



6. 在弹出的“登录Windows弹性云服务器”窗口中，选择“其他方式”下的VNC方式，单击“立即登录”。

7. （可选）如果界面提示“Press Ctrl+Alt+Delete to unlock”，请单击远程登录操作面板上方的“Ctrl+Alt+Del”按钮进行登录。

图 2-28 单击“Ctrl+Alt+Del”



8. （可选）如果远程登录界面上无法显示鼠标，查看面板上方是否有“本地鼠标”按钮，单击“本地鼠标”按钮，鼠标就可以正常显示了。

图 2-29 本地鼠标



9. 根据界面提示，输入弹性云服务器密码。

相关链接

- [忘记密码怎么办？](#)
- [Windows云服务器如何配置多用户登录？](#)
- [无法登录到Windows云服务器怎么办？](#)

2.4.3 通过 RDP 文件登录 Windows ECS

操作场景

远程桌面协议（Remote Desktop Protocol，RDP），是微软提供的多通道的远程登录协议。本节为您介绍如何使用RDP文件远程登录Windows弹性云服务器。

说明

从管理控制台下载的RDP文件对应唯一的云服务器，当前RDP文件命名规则为“云服务器名称-弹性IP”。

前提条件

- 弹性云服务器状态为“运行中”。
- 如果弹性云服务器采用密钥方式鉴权，已获取Windows弹性云服务器的密码，获取方式请参见[获取Windows弹性云服务器的密码](#)。
- 弹性云服务器已经绑定弹性公网IP，绑定方式请参见[绑定弹性公网IP](#)。
- 所在安全组入方向已开放3389端口，配置方式请参见[配置安全组规则](#)。
- 使用的登录工具与待登录的弹性云服务器之间网络连通。例如，默认的3389端口没有被防火墙屏蔽。
- 弹性云服务器开启远程桌面协议RDP（Remote Desktop Protocol）。使用公共镜像创建的弹性云服务器默认已打开RDP。打开RDP方法请参考[开启远程桌面协议RDP](#)。

Windows 操作系统使用 RDP 文件登录 Windows 弹性云服务器

本地主机为Windows操作系统，那么您可以使用RDP文件登录Windows弹性云服务器。

1. 登录管理控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”。

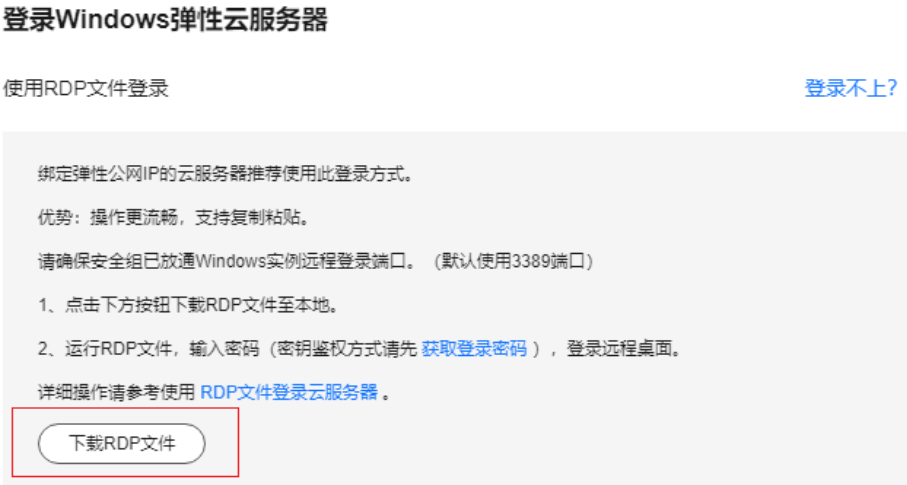
4. 选择要登录的弹性云服务器，单击“操作”列下的“远程登录”。

图 2-30 远程登录



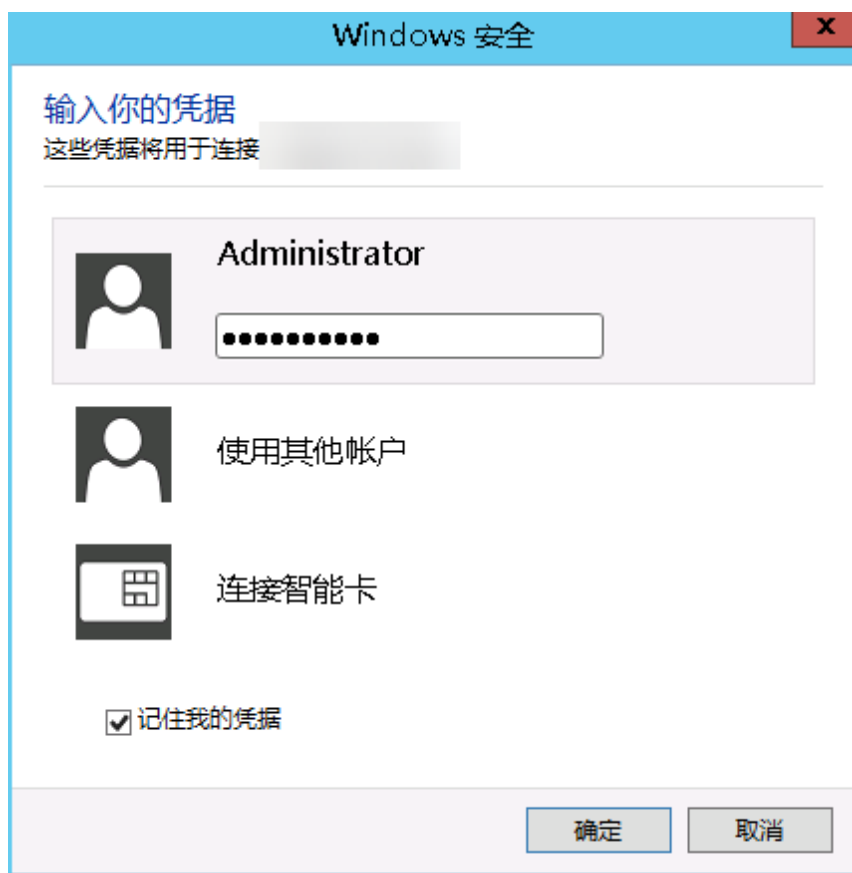
5. 在弹出的“登录Windows弹性云服务器”窗口中，选择“使用 RDP 文件登录”，单击“下载RDP文件”，将 RDP 文件下载到本地。

图 2-31 单击“下载 RDP 文件”



6. 双击已下载到本地的RDP文件，根据提示输入密码，即可远程连接到Windows云服务器。
- 当您的弹性云服务器是采用密码方式鉴权时，请直接使用创建云服务器时设置的密码进行登录。
 - 当您的弹性云服务器是采用密钥方式鉴权时，密码获取方式请参见[获取Windows弹性云服务器的密码](#)。
 - 如果您忘记密码，请参见[在控制台重置ECS密码](#)。

图 2-32 使用 RDP 文件登录 Windows 云服务器



2.4.4 通过本地 Windows 主机登录 Windows ECS

操作场景

本节为您介绍如何在本机使用远程登录工具MSTSC登录Windows弹性云服务器。

前提条件

- 弹性云服务器状态为“运行中”。
- 如果弹性云服务器采用密钥方式鉴权，已获取Windows弹性云服务器的密码，获取方式请参见[获取Windows弹性云服务器的密码](#)。
- 弹性云服务器已经绑定弹性公网IP，绑定方式请参见[绑定弹性公网IP](#)。
使用MSTSC方式通过内网登录云服务器时可以不绑定弹性公网IP，例如VPN、云专线等内网网络连通场景。
- 所在安全组入方向已开放3389端口，配置方式请参见[配置安全组规则](#)。
- 使用的登录工具与待登录的弹性云服务器之间网络连通。例如，默认的3389端口没有被防火墙屏蔽。
- 弹性云服务器开启远程桌面协议RDP（Remote Desktop Protocol）。使用公共镜像创建的弹性云服务器默认已打开RDP。打开RDP方法请参考[开启远程桌面协议RDP](#)。

使用 MSTSC 方式登录 Windows 弹性云服务器

本地主机为Windows操作系统，那么可以使用Windows自带的远程桌面连接工具MSTSC登录Windows云服务器。

以下演示了使用MSTSC方式登录Windows 2012操作系统云服务器的操作步骤。

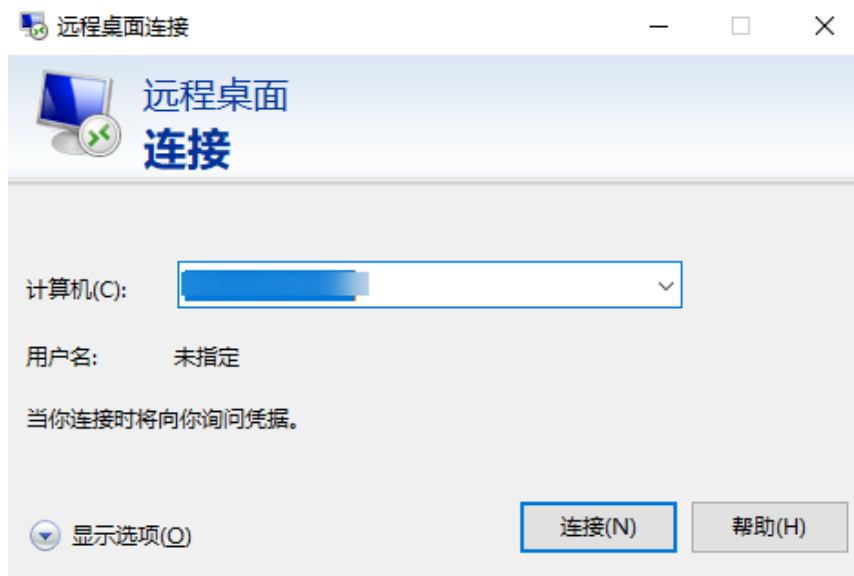
图 2-33 MSTSC 方式登录云服务器



详细操作步骤如下：

1. 在本地主机单击“开始”菜单。
2. 在“搜索程序和文件”中，输入“mstsc”，单击mstsc打开远程桌面连接工具。
3. 在“远程桌面连接”的对话框中，单击“选项”。

图 2-34 显示选项

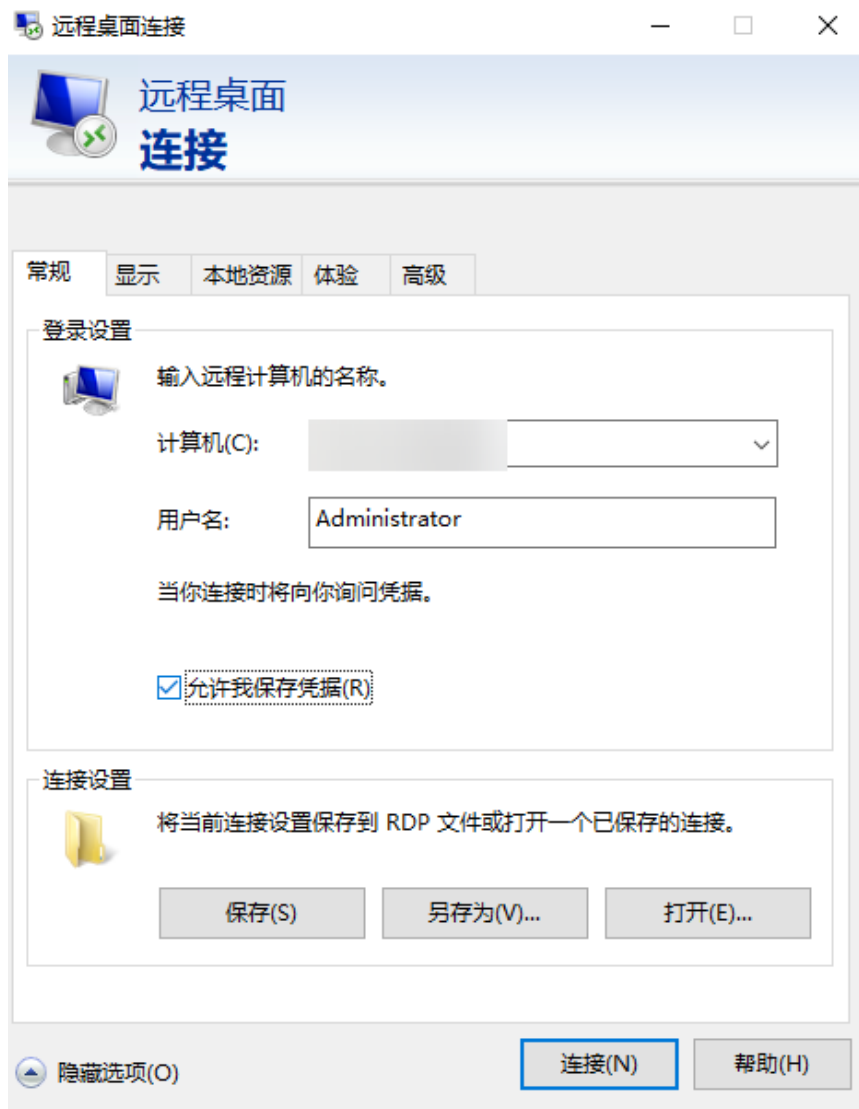


4. 输入待登录的云服务器的弹性公网IP和用户名，默认为Administrator。

说明

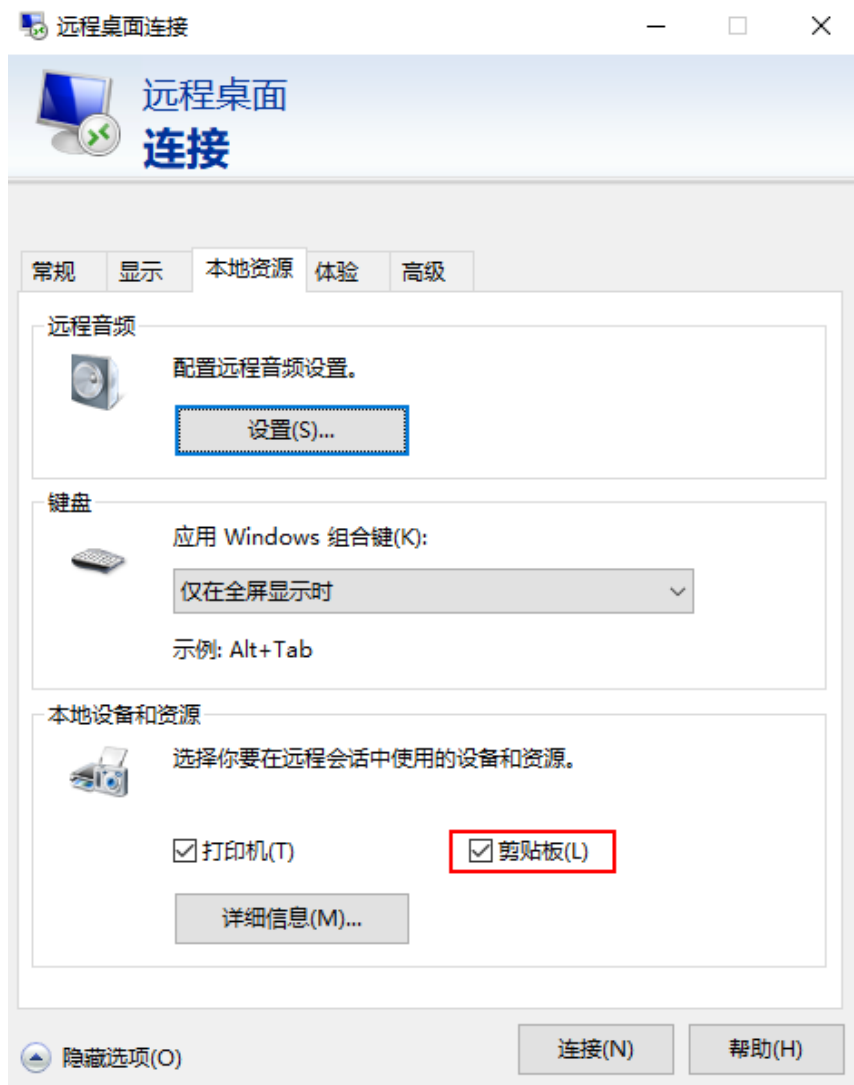
如需再次登录时不再重复输入用户名和密码，可勾选“允许我保存凭据”。

图 2-35 远程桌面链接



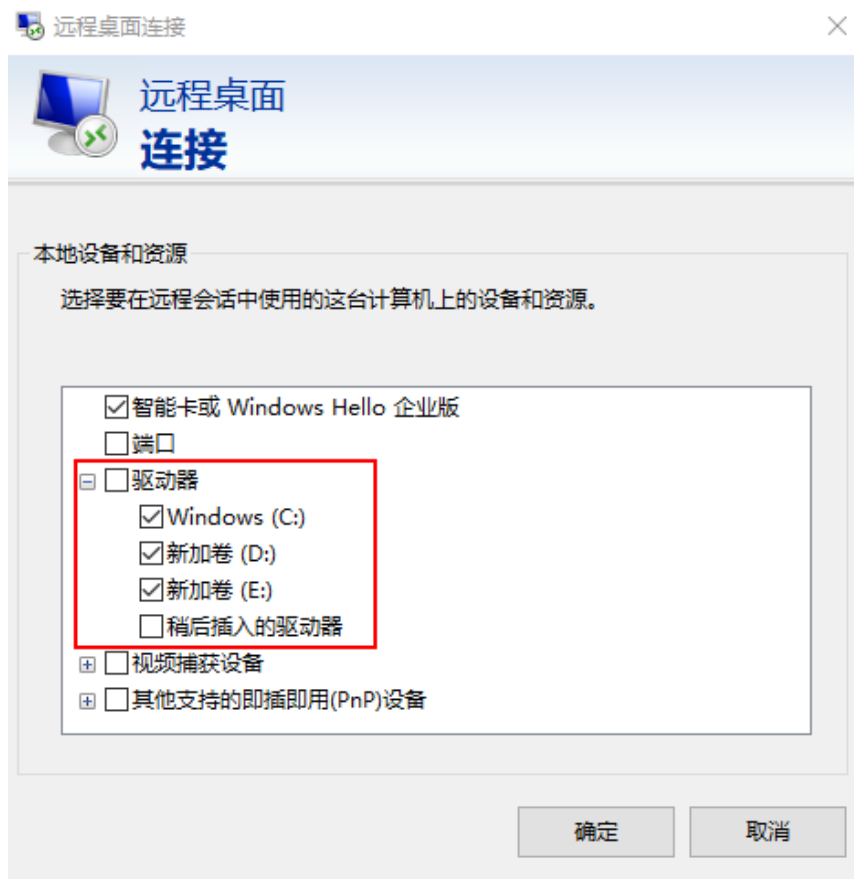
5. （可选）如需在远程会话中使用本地主机的资源，请单击“本地资源”选项卡完成如下配置。
如需从本地主机复制到云服务器中，请勾选“剪贴板”。

图 2-36 勾选剪贴板



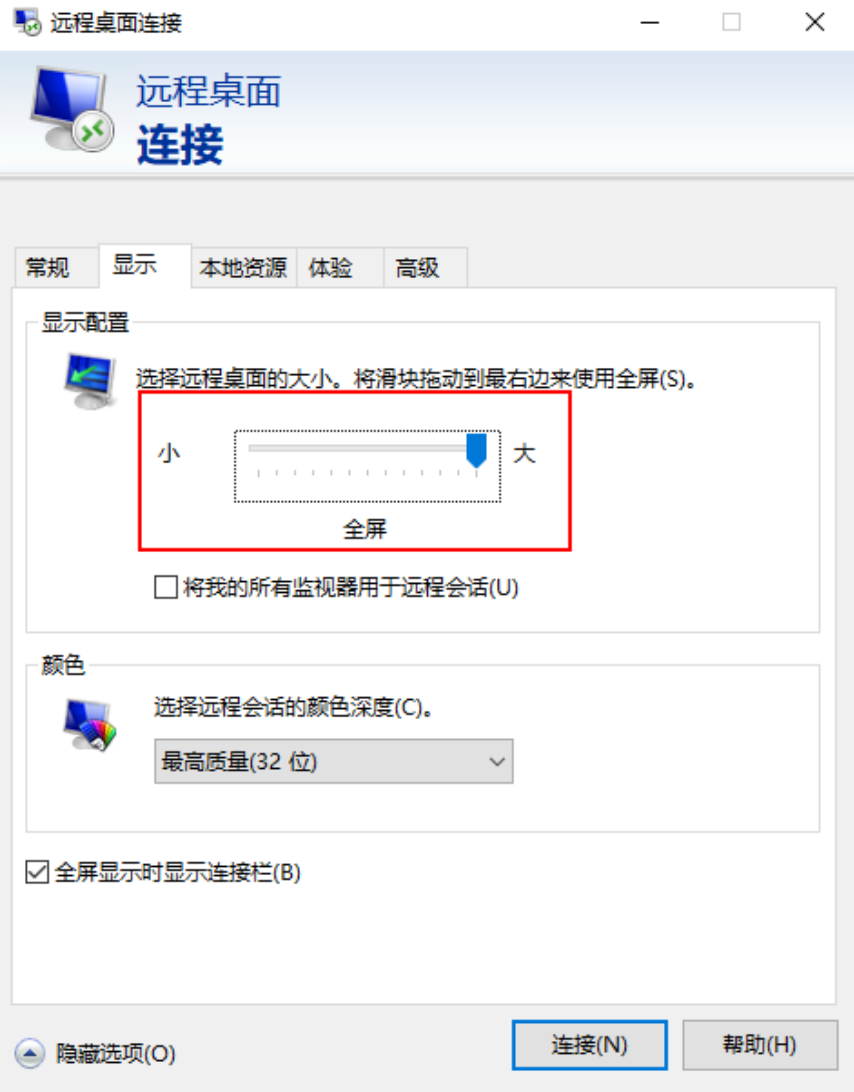
如需从本地主机复制文件到云服务器中，单击“详细信息”，勾选相应的磁盘。

图 2-37 勾选驱动器



6. (可选) 如需调整远程桌面窗口的大小, 可以选择“显示”选项卡, 再调整窗口大小。

图 2-38 调整窗口大小



7. 单击“确定”，根据提示输入密码，登录云服务器。
为安全起见，首次登录云服务器，需更改密码。
8. （可选）通过远程桌面连接（Remote Desktop Protocol，RDP）方式登录云服务器后，如果需要使用RDP提供的“剪切板”功能，将本地的大文件（文件大小超过2GB）复制粘贴至远端的Windows云服务器中，由于Windows系统的限制，会导致操作失败。
具体的解决方法，请参考[使用远程桌面链接方式复制文件](#)。

开启远程桌面协议 RDP

首次登录弹性云服务器时，请先使用VNC方式登录弹性云服务器，打开RDP（Remote Desktop Protocol），然后再使用mstsc方式连接。

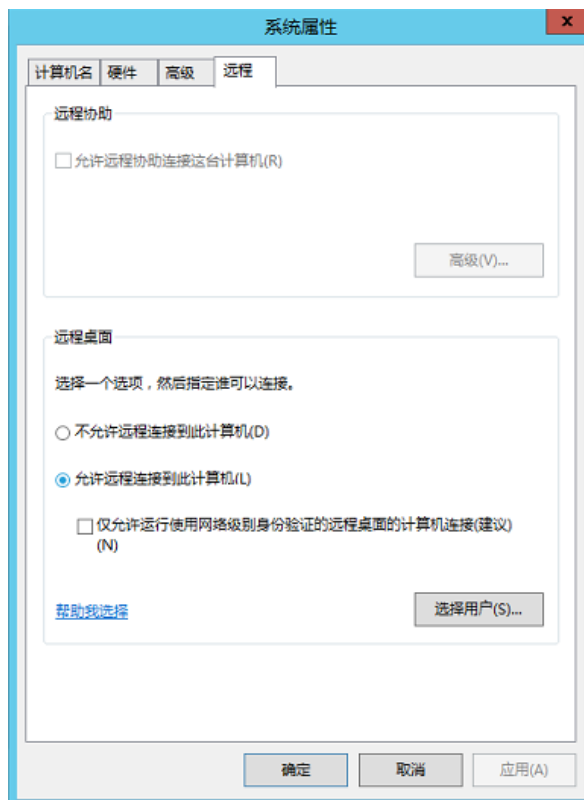
说明

使用公共镜像创建的云服务器，默认已打开RDP。

1. VNC方式登录弹性云服务器。
登录方法请参见[通过控制台VNC登录Windows ECS](#)。

- 单击“开始”菜单，选择“控制面板 > 系统和安全 > 系统 > 远程设置”。系统进入“系统属性”页面。

图 2-39 系统属性



- 选择“远程”页签，在“远程桌面”栏，选择“允许远程连接到此计算机”。
- 单击“确定”。

相关链接

- [忘记密码怎么办？](#)
- [Windows云服务器如何配置多用户登录？](#)
- [无法登录到Windows云服务器怎么办？](#)

2.4.5 通过本地 Linux 主机登录 Windows ECS

操作场景

本节为您介绍如何在Linux操作系统主机上登录Windows云服务器。

前提条件

- 云服务器状态为“运行中”。
- 云服务器已经绑定弹性公网IP。
使用MSTSC方式通过内网登录云服务器时可以不绑定弹性公网IP，例如VPN、云专线等内网网络连通场景。

- 所在安全组入方向已开放3389端口。
- 使用的登录工具与待登录的云服务器之间网络连通。例如，默认的3389端口没有被防火墙屏蔽。
- 云服务器开启远程桌面协议RDP（Remote Desktop Protocol）。使用公共镜像创建的云服务器默认已打开RDP。打开RDP方法请参考[开启远程桌面协议RDP](#)。

操作步骤

如果本地主机为Linux操作系统，您可以使用远程连接工具（例如rdesktop）连接Windows实例。

1. 执行以下命令，检查云服务器是否安装rdesktop。
rdesktop
如果提示“command not found”说明未安装rdesktop。请参考[rdesktop工具官方](#)获取rdesktop安装包安装rdesktop。
2. 输入以下命令登录云服务器。
rdesktop -u 用户名 -p 密码 -g 分辨率 弹性公网IP地址
例如：**rdesktop -u administrator -p password -g 1024*720 121.xx.xx.xxx**

表 2-38 远程登录命令参数

参数	说明
-u	用户名，Windows实例默认用户名是Administrator。
-p	登录Windows实例的密码。
-f	默认全屏，需要用 Ctrl+Alt+Enter 组合键进行全屏模式切换。
-g	分辨率，中间用星号（*）连接，可省略，省略后默认为全屏显示。例如： 1024*720
弹性公网IP地址	需要远程连接的服务器IP地址。需要替换为您的Windows实例的弹性公网IP地址。

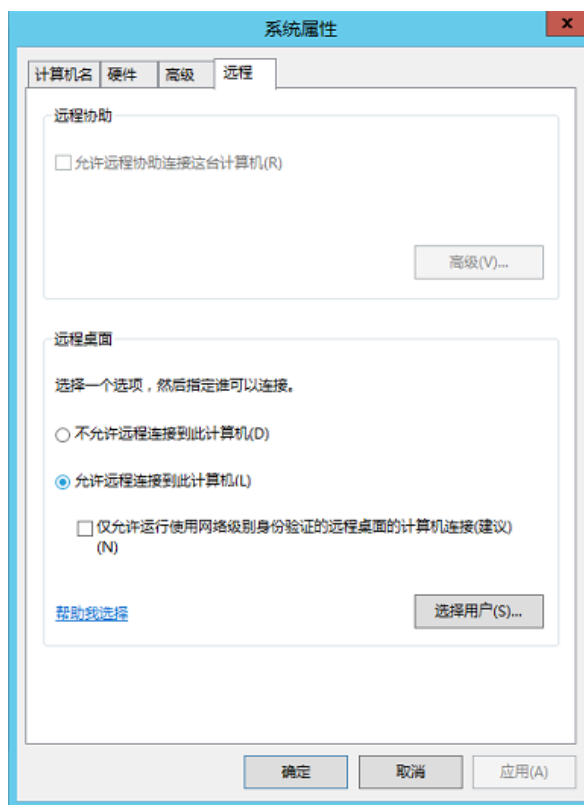
开启远程桌面协议 RDP

首次登录弹性云服务器时，请先使用VNC方式登录弹性云服务器，打开RDP（Remote Desktop Protocol），然后再使用mstsc方式连接。

说明

- 使用公共镜像创建的云服务器，默认已打开RDP。
1. VNC方式登录弹性云服务器。
登录方法请参见[通过控制台VNC登录Windows ECS](#)。
 2. 单击“开始”菜单，选择“控制面板 > 系统和安全 > 系统 > 远程设置”。
系统进入“系统属性”页面。

图 2-40 系统属性



3. 选择“远程”页签，在“远程桌面”栏，选择“允许远程连接到此计算机”。
4. 单击“确定”。

2.4.6 通过本地 macOS 主机登录 Windows ECS

操作场景

本节操作以使用“Microsoft Remote Desktop for Mac”工具远程连接“Windows Server 2012 R2 数据中心版 64位”操作系统云服务器为例，介绍macOS系统登录Windows云服务器的操作步骤。

前提条件

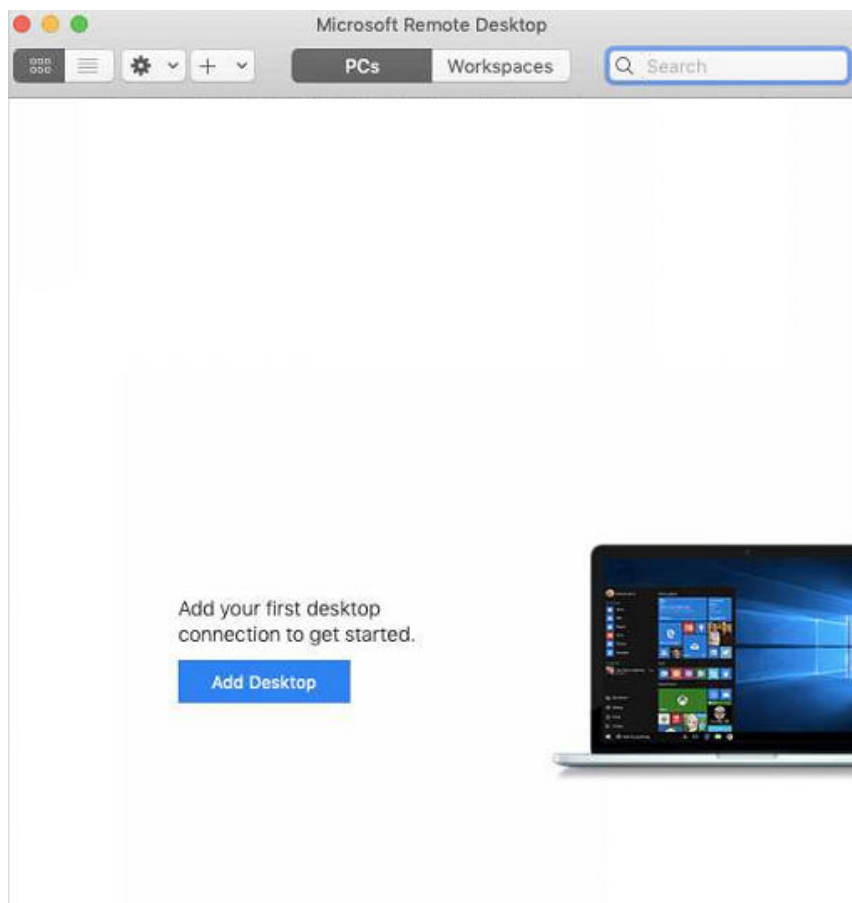
- 云服务器状态为“运行中”。
- 已获取Windows云服务器用户名和密码。忘记密码请参考[在控制台重置ECS密码重置密码](#)。
- 弹性云服务器已经绑定弹性公网IP，绑定方式请参见[绑定弹性公网IP](#)。
- 所在安全组入方向已开放3389端口，配置方式请参见[配置安全组规则](#)。
- 已安装Microsoft Remote Desktop for Mac或其他macOS系统适用的远程连接工具。

微软官方已停止提供Remote Desktop客户端的下载链接，您可单击[Microsoft Remote Desktop Beta](#)下载Beta版本使用。

操作步骤

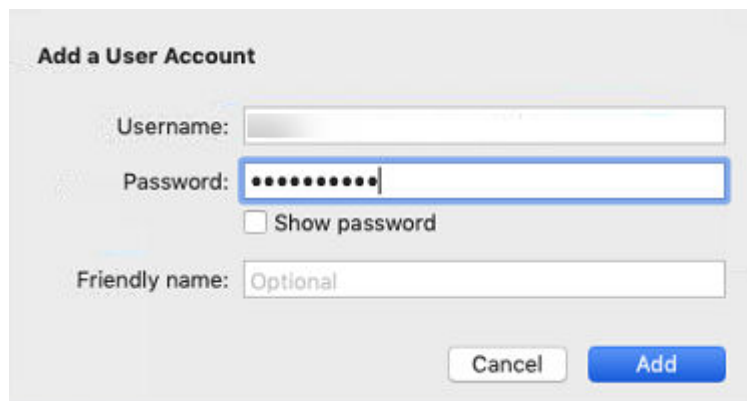
1. 启动Microsoft Remote Desktop。
2. 单击“Add Desktop”。

图 2-41 Add Desktop



3. 在“Add PC”页面，设置登录信息。
 - PC name: 输入需要登录的Windows实例的弹性公网IP地址。
 - User account: 在下拉列表中选择“Add user account”。弹出“Add user account”对话框。
 - i. 输入Windows实例账号“administrator”，并输入实例的登录密码，单击“Add”。

图 2-42 Add user account



Add a User Account

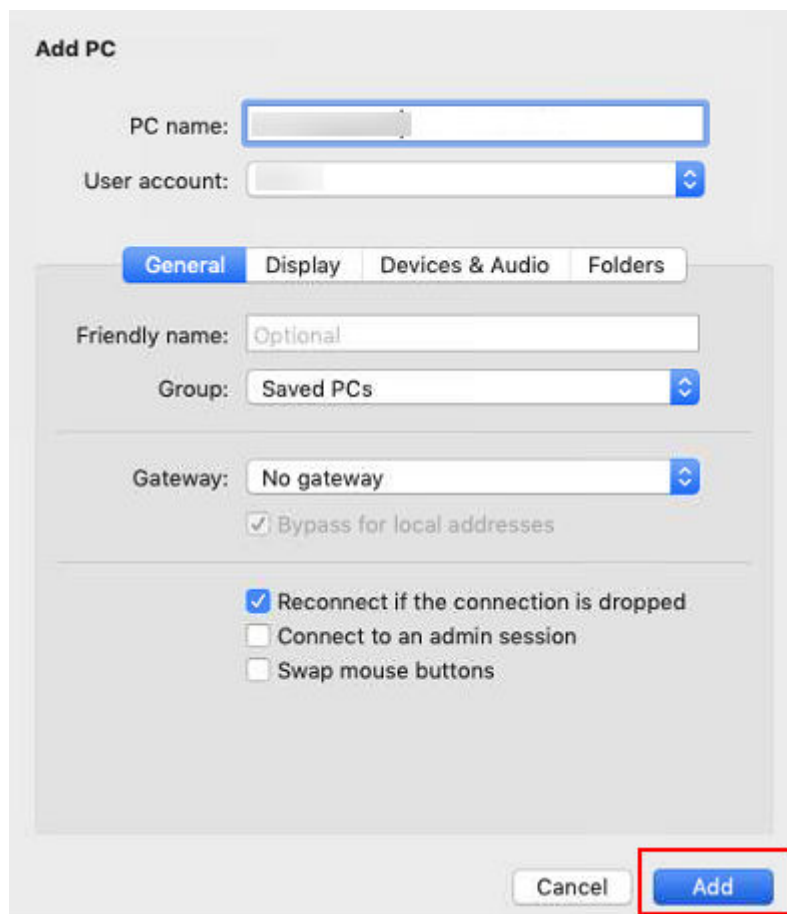
Username:

Password:

☐ Show password

Friendly name:

图 2-43 Add PC



Add PC

PC name:

User account:

General | Display | Devices & Audio | Folders

Friendly name:

Group:

Gateway:

☒ Bypass for local addresses

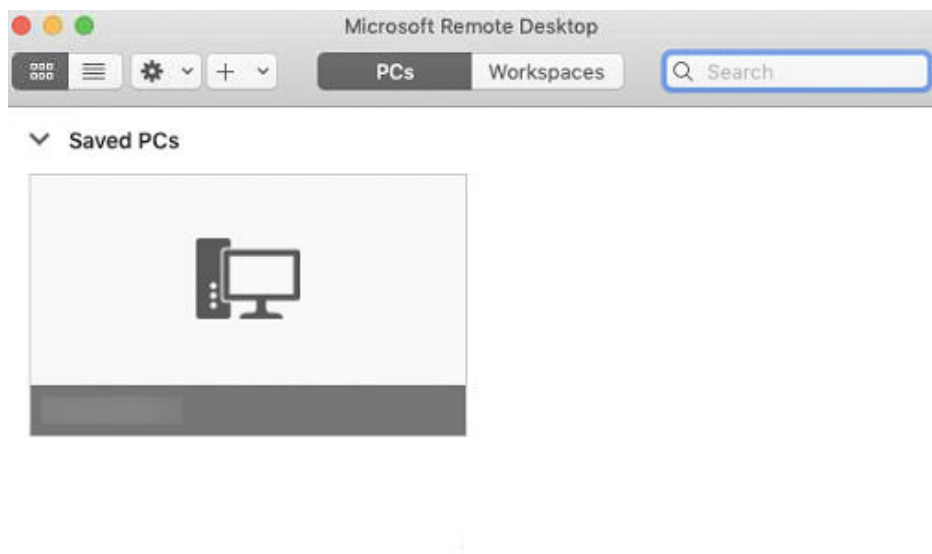
☒ Reconnect if the connection is dropped

☐ Connect to an admin session

☐ Swap mouse buttons

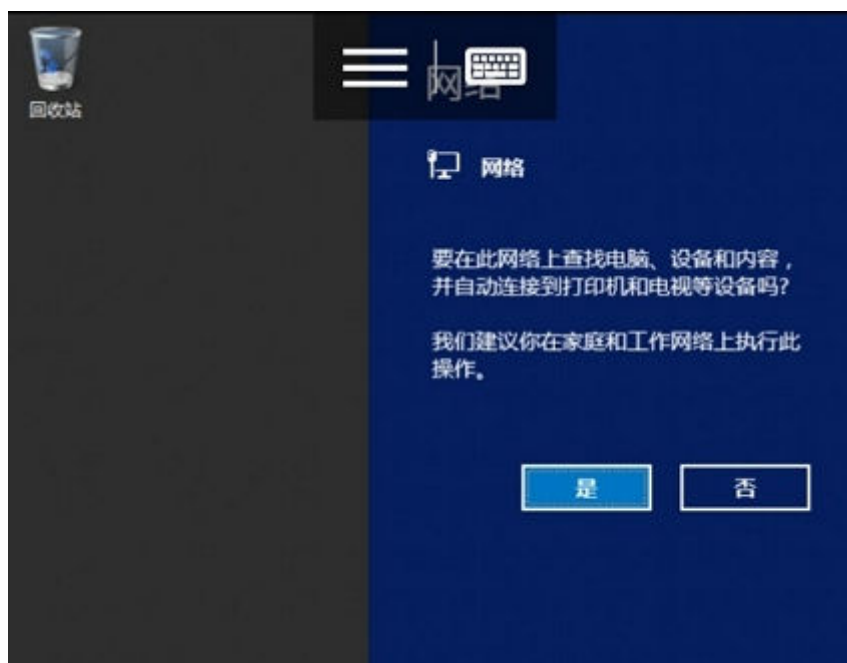
4. 在“Remote Desktop”页面，双击需要登录的Windows实例图标。

图 2-44 双击登录 Windows 实例



5. 确认信息后，单击“Continue”。
至此，您已经登录Windows实例。

图 2-45 登录成功



2.4.7 通过移动设备登录 Windows ECS

操作场景

如果您需要随时随地管理和操作云端的Windows ECS，可以在移动设备上使用远程桌面类应用进行连接。

本文以Microsoft发布的远程桌面（Remote Desktop）应用为例，介绍如何通过Android系统的移动设备登录Windows ECS。

说明

不同移动设备的操作系统类型和支持下载的远程桌面应用可能存在差异，具体操作请参考对应应用的操作指导。

前提条件

- 云服务器状态为“运行中”。
- 已获取Windows云服务器用户名和密码。忘记密码请参考[在控制台重置ECS密码](#)重置密码。
- 云服务器已经绑定弹性公网IP，绑定方式请参见[绑定弹性公网IP](#)。
- 所在安全组入方向已开放3389端口，配置方式请参见[配置安全组规则](#)。
- 移动设备已通过“应用市场”搜索并下载远程连接工具，本文以“Microsoft远程桌面”为例进行介绍。

操作步骤

- 在移动设备上启动远程桌面。
- 在“远程桌面”页面右上角，单击图标，选择“远程桌面”。

图 2-46 远程桌面

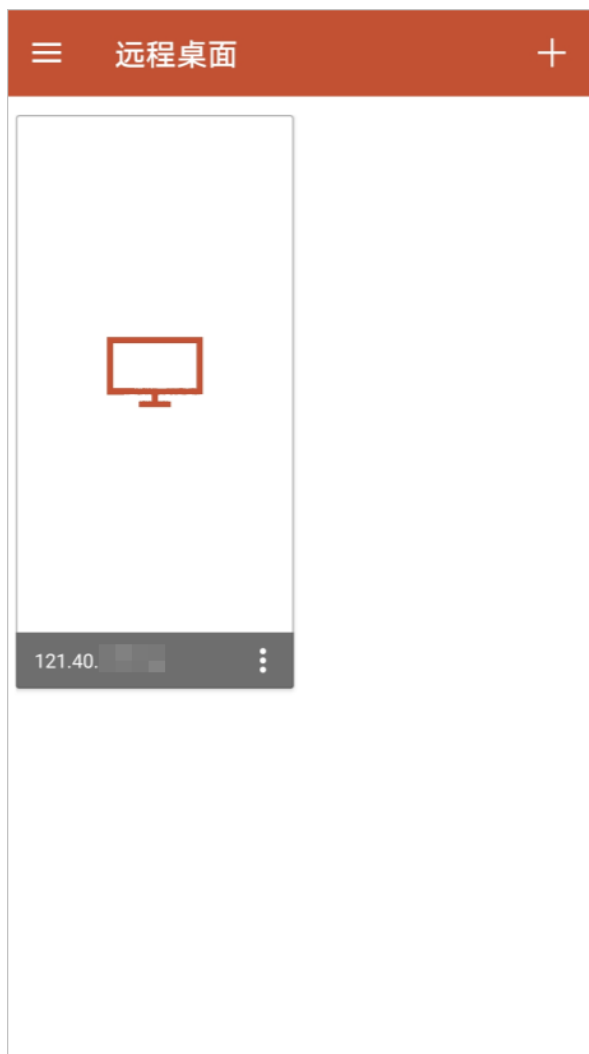


这里什么也没有。

开始前,请先添加你想用此设备连接至的远程桌面.你也可以添加此应用使用的远程资源或者管理员为你设置好的远程PC.

- 在“添加桌面”页面的“主机名称”区域，输入Windows ECS的主机名称或弹性公网IP地址
- 单击“保存”。
- 在“远程桌面”页面，单击需要登录的Windows ECS图标。

图 2-47 登录 Windows 实例



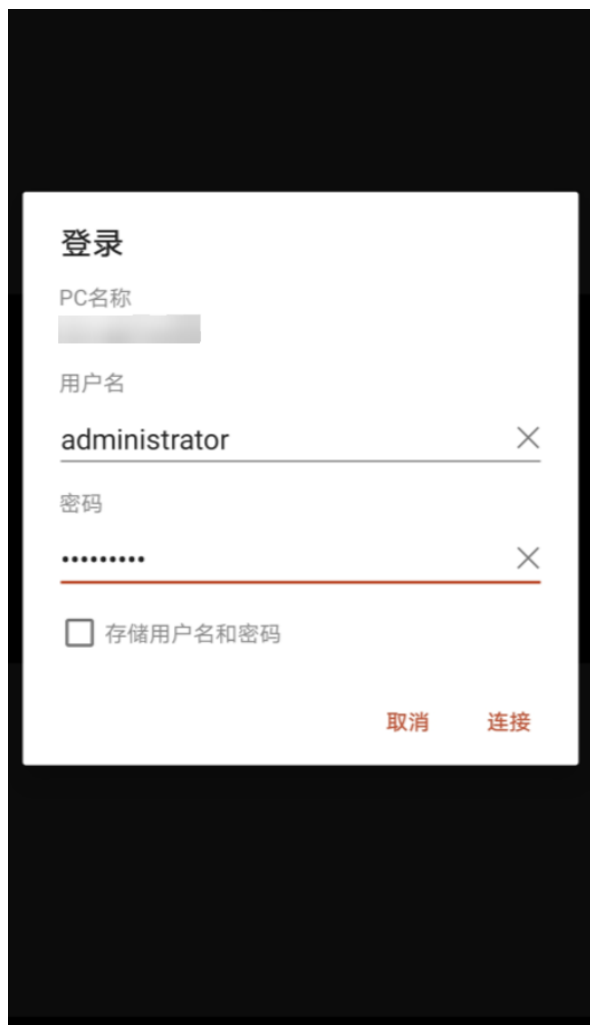
6. 如果弹出“证书无法被验证，无论如何都要连接吗？”，请确认信息后，单击“连接”。

图 2-48 确认信息



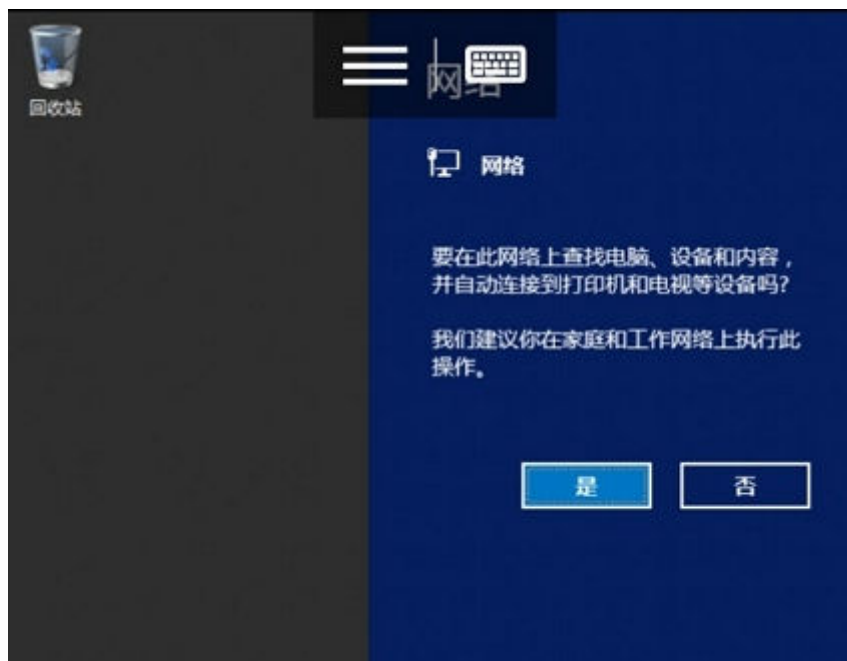
7. 在“登录”页面，填写用户名（例如administrator）和密码，单击“连接”。

图 2-49 登录页面



至此，您已经登录Windows ECS。

图 2-50 登录成功



2.5 登录 Linux ECS

2.5.1 Linux ECS 登录方式概述

约束与限制

- 只有运行中的弹性云服务器才允许用户登录。
- Linux操作系统用户名“root”。
- 忘记密码，请先通过“重置密码”功能设置登录密码。

重置密码：选中待重置密码的云服务器，并选择“操作”列下的“更多 > 重置密码”。详细操作，请参见[在控制台重置ECS密码](#)。

登录方式概述

请根据需要选择登录方式，登录云服务器。

表 2-39 Linux 云服务器登录方式一览

云服务器操作系统	本地主机操作系统	连接方法	条件
Linux	Windows	(推荐使用)使用控制台提供的CloudShell登录云服务器。 通过CloudShell登录Linux ECS。	云服务器绑定弹性公网IP。 (通过内网登录云服务器时可以不绑定弹性公网IP,例如VPN、云专线等内网网络连通场景。)
	Windows	使用PuTTY、Xshell等远程登录工具: - 密码方式鉴权: SSH密码方式登录(本地使用Windows操作系统)。 - 密钥方式鉴权: SSH密钥方式登录(本地使用Windows操作系统)。	
	Linux	使用命令连接: - 密码方式鉴权: SSH密码方式登录(本地使用Linux操作系统)。 - 密钥方式鉴权: SSH密钥方式登录(本地使用Linux操作系统)。	
	移动设备	- 使用Termius、JuiceSSH等SSH客户端工具登录云服务器: 通过移动设备登录Linux ECS。 - 下载华为云APP连接云服务器: 通过华为云APP登录Linux ECS。	
	macOS系统	使用系统自带的终端(Terminal): 通过macOS主机登录Linux ECS。	
	Windows	使用管理控制台远程登录方式: 通过VNC登录Linux ECS。	不依赖弹性公网IP。

相关链接

- [忘记密码怎么办?](#)
- [无法登录到Linux云服务器怎么办?](#)

2.5.2 通过 CloudShell 登录 Linux ECS

操作场景

本节为您介绍通过控制台提供的CloudShell登录云服务器的操作步骤。

登录成功后，如需使用CloudShell界面提供的复制、粘贴功能，请参见[CloudShell常用操作](#)。

约束限制

支持通过CloudShell方式登录弹性云服务器的区域，请参见[功能总览](#)中“连接Linux实例”的发布区域。

前提条件

- 云服务器状态为“运行中”。
- 请确保安全组已开放登录端口，默认使用22端口，如需使用其他端口可登录云服务器后重新设置。
修改远程登录端口请参考[修改远程登录端口](#)。配置安全组规则请参考[配置安全组规则](#)。
- 如果在创建云服务器时未设置密码，请先重置密码后再登录云服务器。
- 使用CloudShell连接云服务器支持公网连接和私网连接两种方式。当使用CloudShell通过私网远程连接云服务器时，需要具有Security Administrator权限的用户进行服务授权。
 - 若用户有Security Administrator权限，在首次使用时，会弹出如下授权页面，单击“同意授权”即可。
服务授权区域级生效，仅需在每个区域首次使用时执行一次，授权后，用户即可在当前区域使用。

图 2-51 服务授权



- 若用户无Security Administrator权限，页面将提示“请添加Security Administrator管理员”，可以联系管理员（具有admin权限的用户）为该用户添加Security Administrator权限后重试。

图 2-52 无权限



授权方式为：

- i. 创建用户组，并给用户组授权添加Security Administrator权限，详细操作请参考[创建用户组并授权](#)。
- ii. 将用户添加到用户组中，详细操作请参考[用户组添加用户](#)。

 说明

使用CloudShell通过公网远程连接云服务器时，无需进行服务授权。

操作步骤

- 1. 登录管理控制台。
- 2. 单击管理控制台左上角的 ，选择区域和项目。
- 3. 单击“”，选择“计算 > 弹性云服务器”。
- 4. 选择要登录的云服务器，单击“操作”列下的“远程登录”。
- 5. 在弹出的“登录Linux云服务器”窗口中，单击“使用CloudShell登录”。
- 6. 在CloudShell界面配置云服务器信息。

首次登录，默认会打开CloudShell配置向导，输入云服务器的相关参数进行连接。

 说明

您可以选择使用云服务器的弹性公网IP或私有IP进行登录。

- 若勾选云服务器的公网IP（弹性公网IP）。
 - i. 在CloudShell配置向导中设置云服务器的端口（默认22）、用户名、认证方式、密码（或密钥）等参数。
 - ii. 单击“连接”登录云服务器。

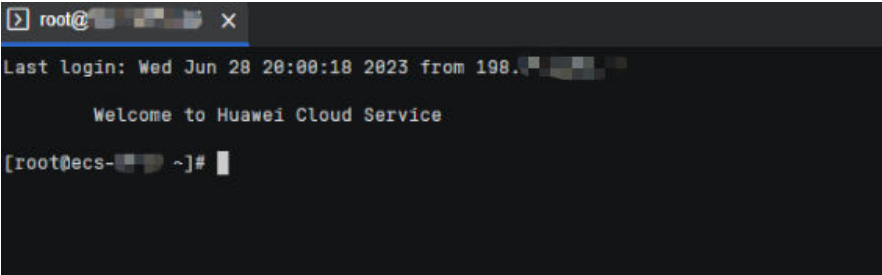
如果单击“连接”没有反应，可能是云服务器未设置登录密码或密码错误，请重置密码后重新登录。

图 2-53 CloudShell 配置向导（公网 IP）



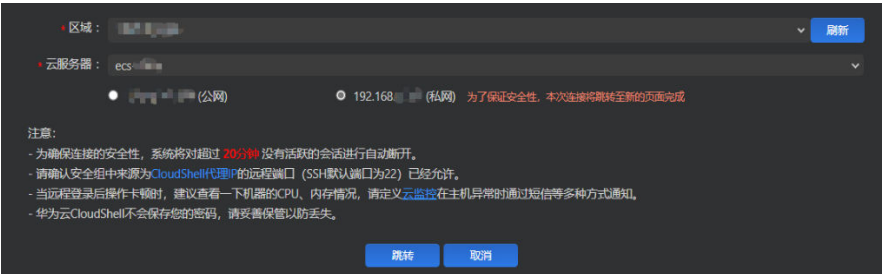
连接成功后，CloudShell界面提示如下。

图 2-54 操作结果



- 若勾选云服务器的私网IP（私有IP）。
 - i. 单击“跳转”，打开新的CloudShell配置向导页。

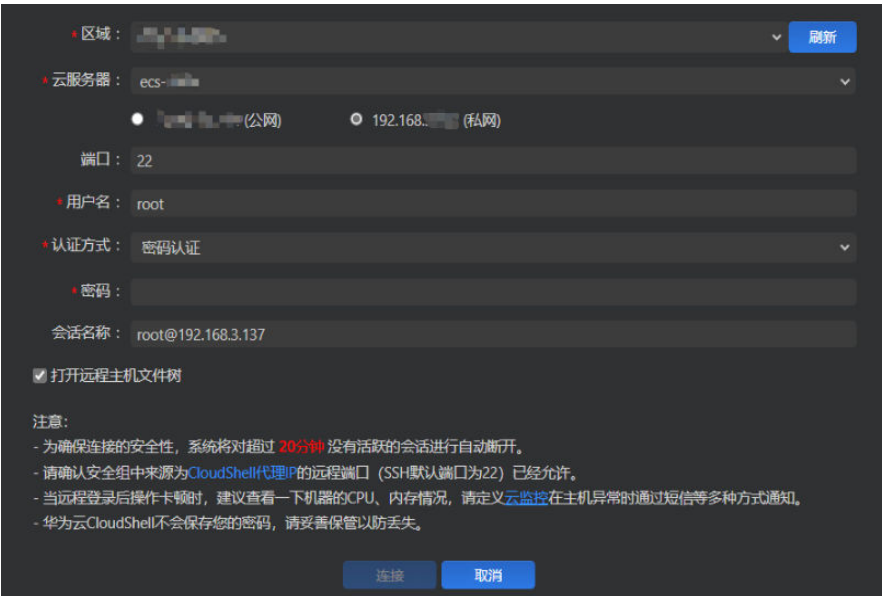
图 2-55 CloudShell 配置向导（私网 IP）1



- ii. 在CloudShell配置向导中设置云服务器的端口（默认22）、用户名、认证方式、密码（或密钥）等参数。
 - iii. 单击“连接”登录云服务器。

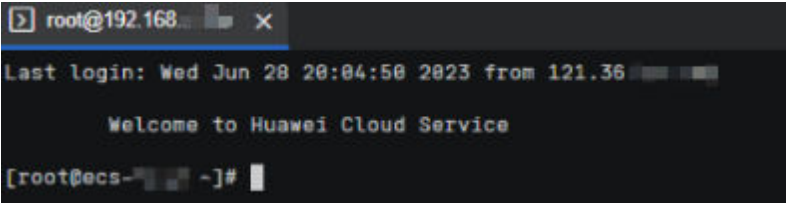
如果单击“连接”没有反应，可能是云服务器未设置登录密码或密码错误，请重置密码后重新登录。

图 2-56 CloudShell 配置向导（私网 IP）2



连接成功后，CloudShell界面提示如下。

图 2-57 操作结果



CloudShell 常用操作

- **新建会话**
选择“终端 > 新建会话”，即可配置新的终端连接会话。
- **快捷键**
您可以使用快捷键编辑输入的命令。

表 2-40 CloudShell 快捷键

快捷键	功能
Ctrl+L	将当前行移到第一行
Ctrl+U	清除当前行
Ctrl+H	向前删除一个字符
Ctrl+A	光标移动到句首
Ctrl+E	光标移动到句末

- **复制、粘贴**
CloudShell支持直接在终端中进行复制粘贴。您既可以通过右键来复制粘贴，也可以直接用“Ctrl+C”、“Ctrl+V”等快捷键实现。
- **浏览输出历史**
对于跨屏内容，可以滚动终端查看历史输出。默认情况下，终端只会记录最近1000行输出。
- **多终端分区布局**
您可以在同一个页面中创建多个CloudShell终端，并可以直接拖动窗口，随意组合成您喜欢的布局。

相关链接

- [忘记密码怎么办？](#)
- [无法登录到Linux云服务器怎么办？](#)
- [配置安全组规则](#)
- [怎样修改远程登录的端口？](#)

2.5.3 通过 VNC 登录 Linux ECS

操作场景

本节为您介绍如何通过控制台提供的远程登录功能（即VNC方式）登录到弹性云服务器上。

当您无法使用CloudShell文件或其他远程登录工具连接弹性云服务器时，可以选择通过VNC方式进行登录，该登录方式主要用于紧急运维场景，可查看弹性云服务器状态或进行相关维护操作。

登录成功后，如需使用VNC界面提供的复制、粘贴功能，请参见[后续处理](#)。

说明

对于“密钥对”方式创建的Linux弹性云服务器，如需使用控制台提供的“远程登录”功能（VNC方式），需先使用“[SSH密钥方式](#)”登录，并设置密码，然后才能使用VNC方式登录。

约束与限制

- 使用VNC方式登录弹性云服务器时，系统不支持直接的复制粘贴操作，这将降低您使用云服务器的效率。如无特殊要求，建议使用SSH方式或者CloudShell方式登录云服务器，具体操作请参见[通过SSH密钥方式登录Linux ECS](#)、[通过SSH密码方式登录Linux ECS](#)、[通过CloudShell登录Linux ECS](#)。

前提条件

对于“密钥对”鉴权方式的弹性云服务器，已使用SSH密钥方式登录Linux弹性云服务器，并设置密码。

登录 Linux 弹性云服务器（非 FPGA 加速型）

如果您登录的弹性云服务器不是FPGA加速型，登录方法如下：

- 登录管理控制台。
- 单击管理控制台左上角的，选择区域和项目。
- 单击“”，选择“计算 > 弹性云服务器”。
- 选择要登录的弹性云服务器，单击“操作”列下的“远程登录”。

图 2-58 远程登录



- 在弹出的“登录Linux云服务器”窗口中，选择“其他方式”下的VNC方式，单击“立即登录”。

- （可选）如果界面提示“Press CTRL+ALT+DELETE to log on”，请单击远程登录操作面板上方的“Ctrl+Alt+Del”按钮进行登录。

说明

请勿使用物理键盘按“CTRL+ALT+DELETE”，该操作不生效。

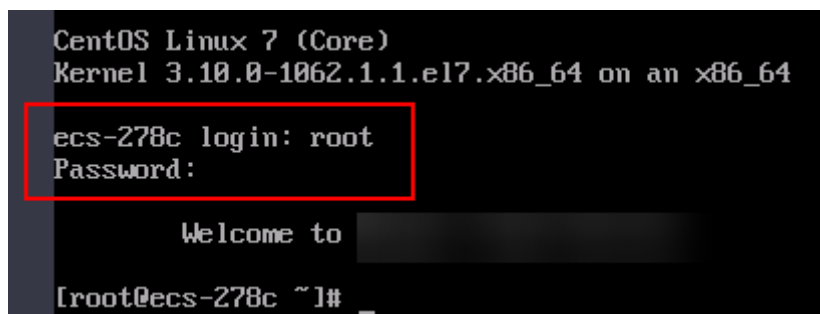
- （可选）如果远程登录界面上无法显示鼠标，查看面板上方是否有“本地鼠标”按钮，单击“本地鼠标”按钮，鼠标就可以正常显示了。

图 2-59 本地鼠标



- 根据界面提示，输入弹性云服务器密码。

图 2-60 输入用户名和密码（假设用户名为 root）



登录 Linux 弹性云服务器（FPGA 加速型）

FPGA加速型云服务器的镜像使用CentOS 7.3 64bit图形化界面，如果您登录的是FPGA加速型云服务器，且该云服务器除了root账号以外，没有其他账号，系统会提示您新建一个用户。登录方法如下：

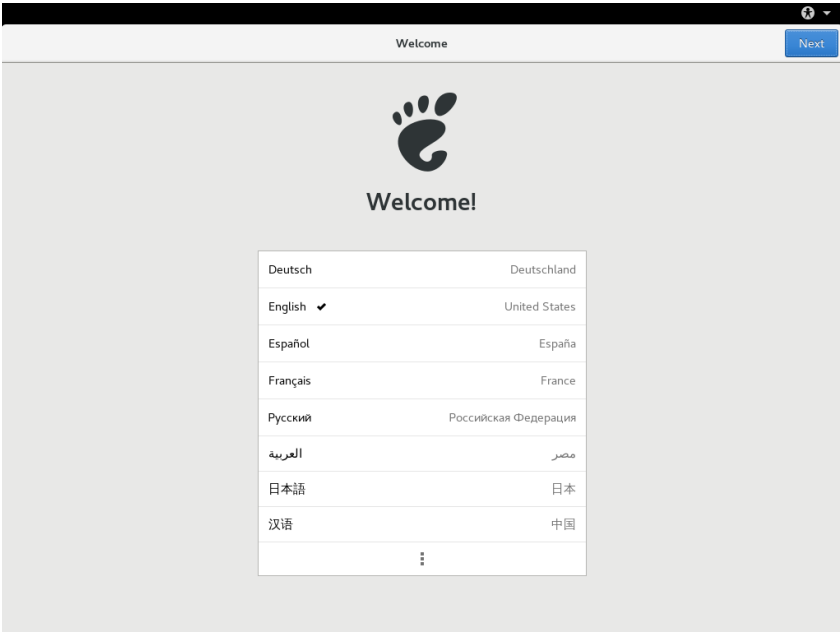
- 登录管理控制台。
- 单击管理控制台左上角的📍，选择区域和项目。
- 单击“≡”，选择“计算 > 弹性云服务器”。
- 选择要登录的弹性云服务器，单击“操作”列下的“远程登录”。

图 2-61 远程登录



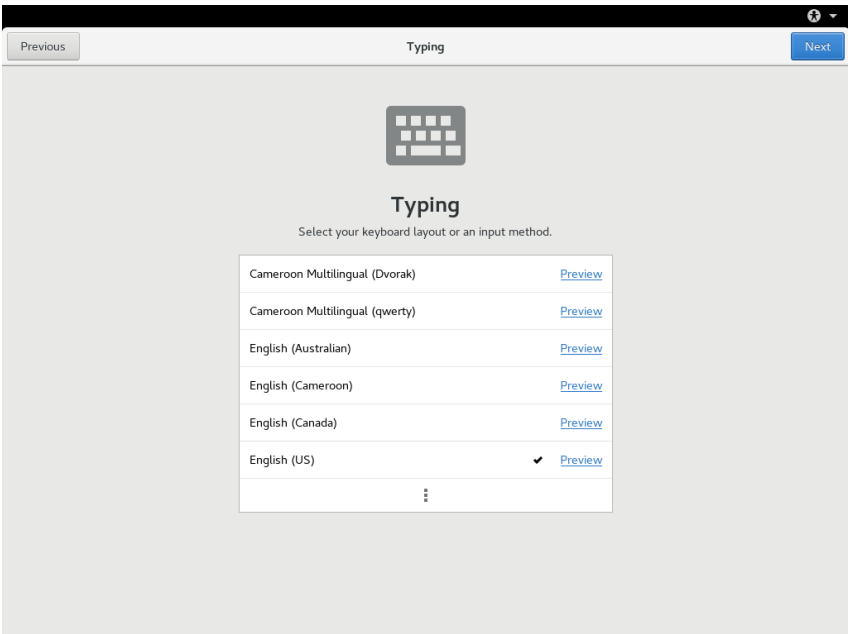
5. 根据界面提示，选择系统语言（以选择“English”为例），并单击“Next”。

图 2-62 选择语言



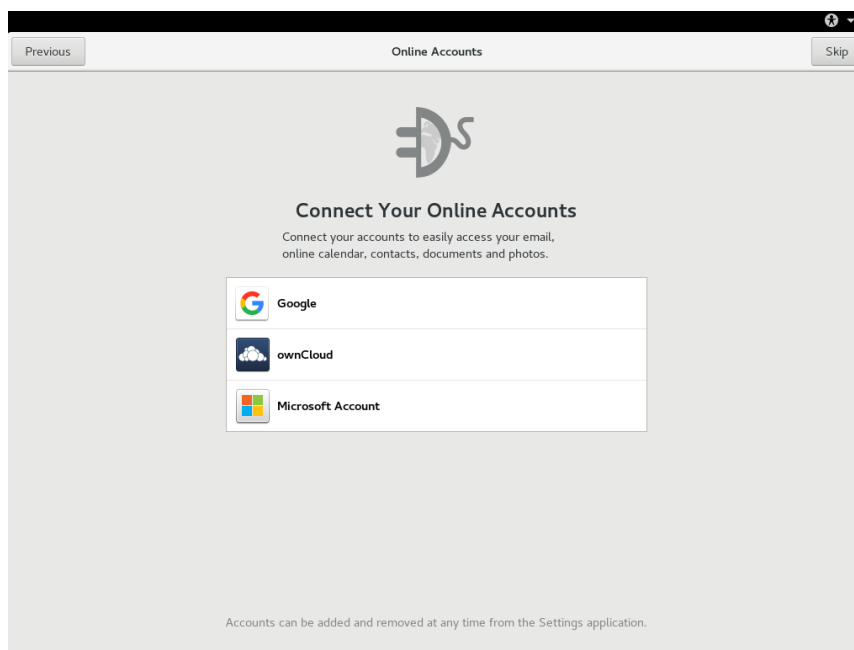
6. 选择您使用的物理键盘的类型，并单击“Next”。

图 2-63 选择键盘类型



7. 根据需要设置隐私项，并单击“Next”。
8. 设置弹性云服务器的时区，并单击“Next”。
9. （可选）根据需要联动其他账号，也可以直接单击“Skip”。

图 2-64 绑定其他账号



10. 设置新创建用户的“Full Name”和“Username”，其中
 - Full Name：全名，类似用户的昵称。
 - Username：用户名，用于创建您的主目录，且无法更改。
11. 设置密码。
12. 单击“Start using CentOS Linux”，进入弹性云服务器。

后续处理

系统支持从本地拷贝命令行到弹性云服务器，实现本地数据与弹性云服务器之间的单向复制、粘贴功能，方法如下：

1. 使用VNC方式成功登录弹性云服务器。
2. 单击页面上方的“复制粘贴”。

图 2-65 复制粘贴



3. 使用快捷键Ctrl+C，复制本地计算机的数据。
 4. 使用快捷键Ctrl+V，将本地数据粘贴至“复制粘贴”窗口。
 5. 单击“发送”。
- 将复制的数据发送至命令行窗口。

说明

对于使用图形化界面的Linux弹性云服务器，在使用VNC窗口提供的“复制粘贴”功能时，会小概率出现数据丢失的情况。这是由于弹性云服务器CPU核数过低，图形化界面占用较多CPU资源导致。此时，建议您每次发送的字符数不超过5个，或者从图形化界面切换至命令行界面（也称“文本界面”），然后再使用“复制粘贴”功能。

相关链接

- [忘记密码怎么办？](#)
- [无法登录到Linux云服务器怎么办？](#)

2.5.4 通过 SSH 密钥方式登录 Linux ECS

操作场景

本节操作介绍在Windows和Linux环境中使用SSH密钥对方式远程登录Linux云服务器的操作步骤。

前提条件

- 已获取创建该弹性云服务器时使用的密钥对私钥文件，创建密钥对请参见（[推荐](#)）[通过管理控制台创建密钥对](#)。
- 弹性云服务器已经绑定弹性公网IP，绑定方式请参见[查看ECS详细信息（列表视图）](#)。

- 已配置安全组入方向的访问规则，配置方式请参见[配置安全组规则](#)。
- 使用的登录工具（如PuTTY）与待登录的弹性云服务器之间网络连通。例如，默认的22端口没有被防火墙屏蔽。

本地使用 Windows 操作系统

如果您本地使用Windows操作系统登录Linux弹性云服务器，可以按照下面方式登录弹性云服务器。

方式一：使用PuTTY登录

以PuTTY为例介绍如何登录弹性云服务器。使用PuTTY登录弹性云服务器前，需要先将私钥文件转化为.ppk格式。

1. 判断私钥文件是否为.ppk格式。
 - 是，执行7。
 - 否，执行2。
2. 在以下路径中下载PuTTY和PuTTYgen。

<https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>

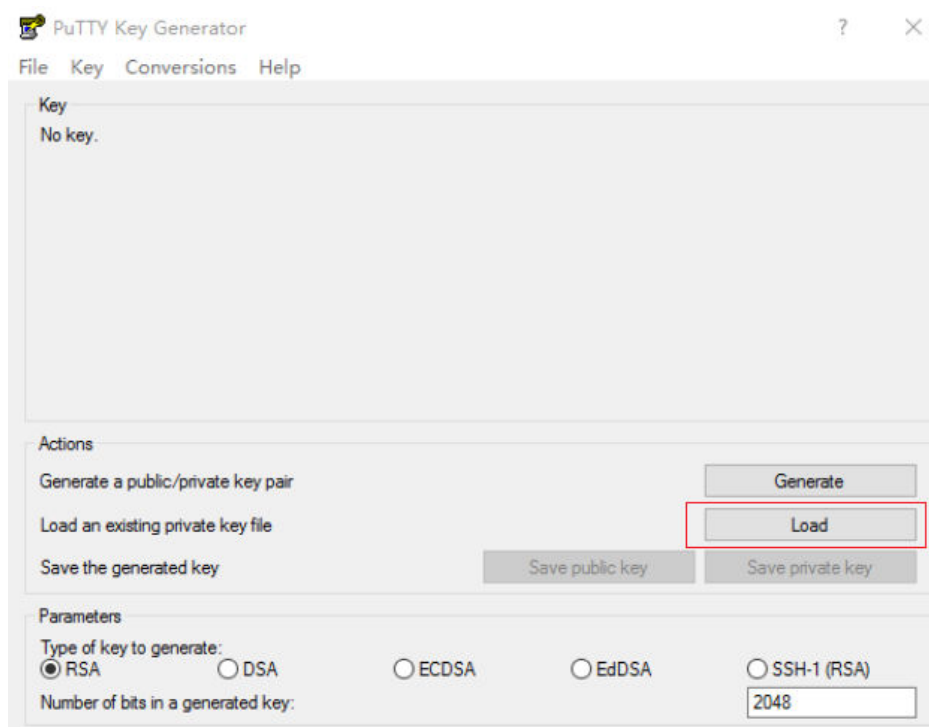
说明

PuTTYgen是密钥生成器，用于创建密钥对，生成一对公钥和私钥供PuTTY使用。

3. 运行PuTTYgen。
4. 在“Actions”区域，单击“Load”，并导入创建弹性云服务器时保存的私钥文件。

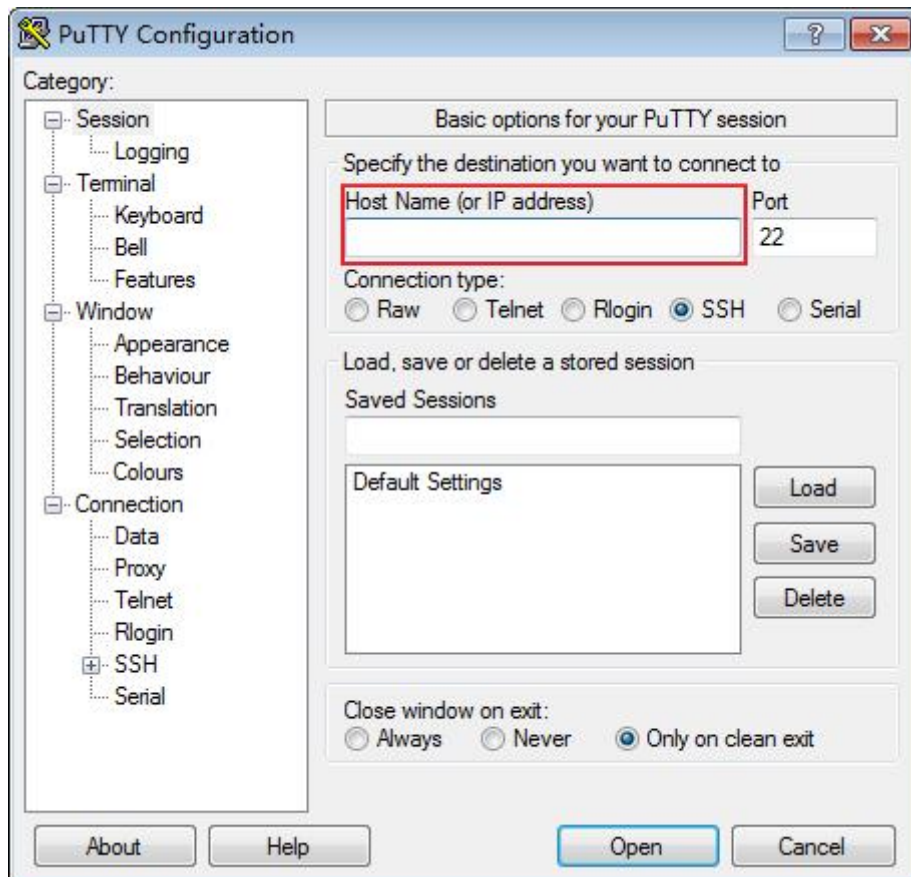
导入时注意确保导入的格式要求为“All files (*.*)”。

图 2-66 导入私钥文件



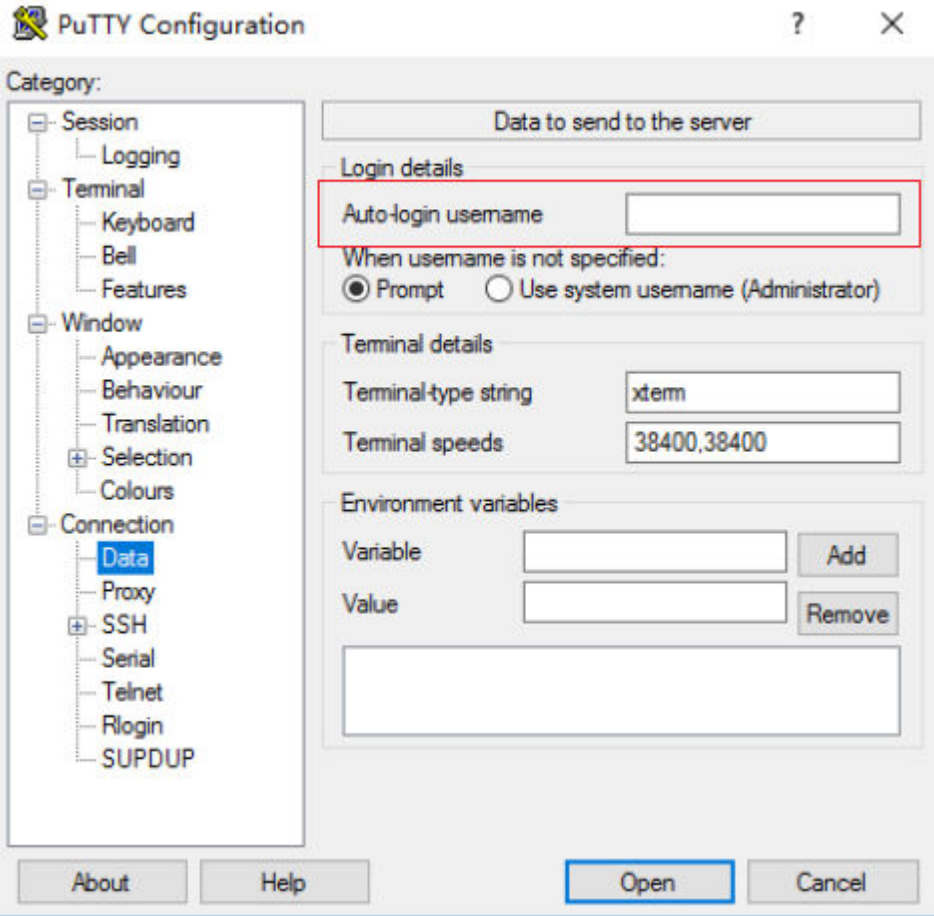
5. 在“Actions”区域，单击“Save private key”。
6. 保存转化后的私钥到本地。例如：kp-123.ppk
7. 双击“PUTTY.EXE”，打开“PuTTY Configuration”。
8. 单击“Session”，在“Host Name (or IP address)”下的输入框中输入弹性云服务器的弹性公网IP。

图 2-67 配置弹性公网 IP



9. 选择“Connection > data”，在Auto-login username处输入镜像的用户名。

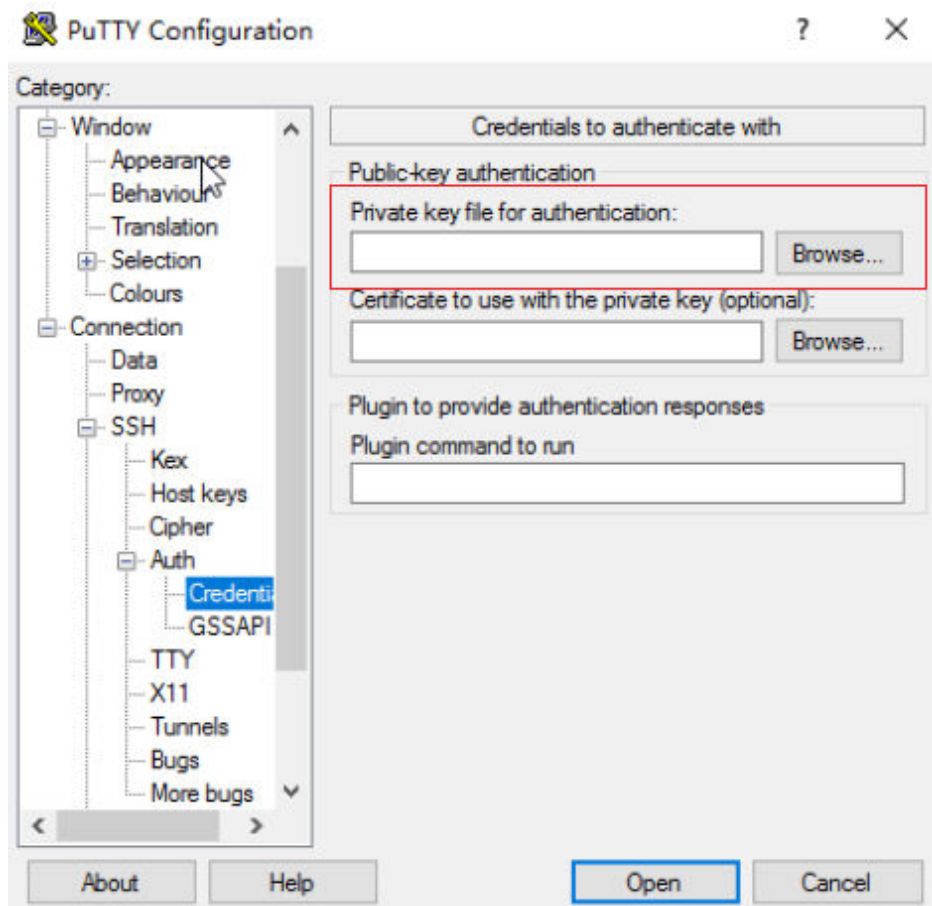
图 2-68 输入用户名



说明

- 使用“SSH密钥方式”登录弹性云服务器时：
- 如果是“CoreOS”的公共镜像，镜像的用户名为“core”。
 - 如果是“非CoreOS”的公共镜像，镜像的用户名为“root”。
10. 选择“Connection > SSH > Auth > Credentials”，在配置项“Private key file for authentication”中，单击“Browse”，选择6转化的密钥。

图 2-69 导入密钥



11. 单击“Open”。
登录弹性云服务器。

方式二：使用Xshell登录

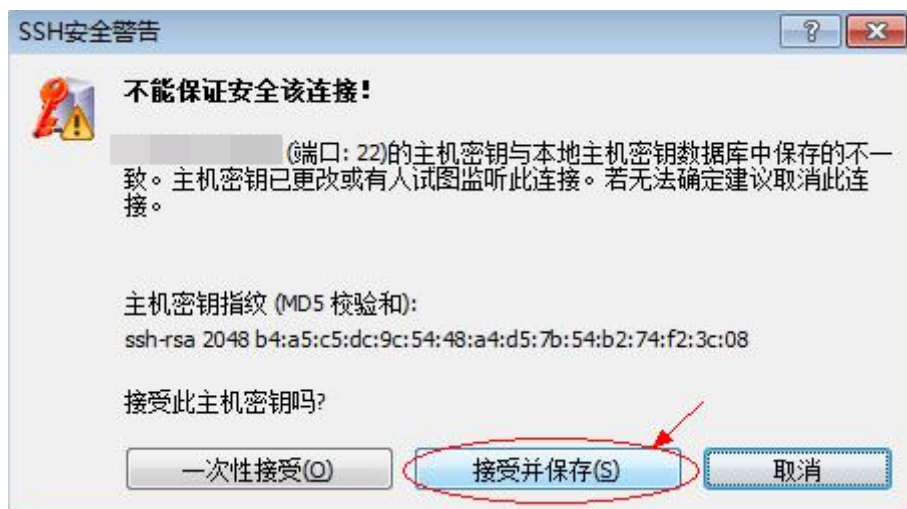
1. 打开Xshell工具。
2. 通过弹性公网IP，执行以下命令，SSH远程连接弹性云服务器。
ssh 用户名@弹性公网IP

📖 说明

使用“SSH密钥方式”登录弹性云服务器时：

- 如果是“CoreOS”的公共镜像，镜像的用户名为“core”。
 - 如果是“非CoreOS”的公共镜像，镜像的用户名为“root”。
3. （可选）如果系统弹窗提示“SSH安全警告”，此时需单击“接受并保存”。

图 2-70 SSH 安全警告



4. 选择“Public Key”，并单击“用户密钥(K)”栏的“浏览”。
5. 在“用户密钥”窗口中，单击“导入”。
6. 选择本地保存的密钥文件，并单击“打开”。
7. 单击“确定”，登录弹性云服务器。

本地使用 Linux 操作系统

如果您本地使用Linux操作系统登录Linux弹性云服务器，可以按照下面方式登录。下面步骤以私钥文件是kp-123.pem为例进行介绍。

1. 在您的linux计算机的命令中执行如下命令，变更权限。

```
chmod 400 /path/kp-123.pem
```

说明

上述命令的path为密钥文件的存放路径。

2. 执行如下命令，登录弹性云服务器。

```
ssh -i /path/kp-123.pem 默认用户名@弹性公网IP
```

假设Linux弹性云服务器的默认用户名是root，弹性公网IP为123.123.123.123，则命令如下：

```
ssh -i /path/kp-123.pem root@123.123.123.123
```

说明

- path为密钥文件的存放路径。
- 弹性公网IP地址为弹性云服务器绑定的弹性公网IP地址。

后续处理

- 以SSH密钥方式登录弹性云服务器后，可以通过设置密码（执行passwd命令），后续使用VNC方式登录Linux弹性云服务器。

相关链接

- [忘记密码怎么办？](#)

- [无法登录到Linux云服务器怎么办？](#)

2.5.5 通过 SSH 密码方式登录 Linux ECS

操作场景

本节操作介绍在Windows和Linux环境中使用SSH密码方式远程登录Linux云服务器的操作步骤。

前提条件

- 弹性云服务器状态为“运行中”。
- 弹性云服务器已经绑定弹性公网IP，绑定方式请参见[绑定弹性公网IP](#)。
- 所在安全组入方向已开放22端口，配置方式请参见[配置安全组规则](#)。
- 使用的登录工具（如PuTTY）与待登录的弹性云服务器之间网络连通。例如，默认的22端口没有被防火墙屏蔽。

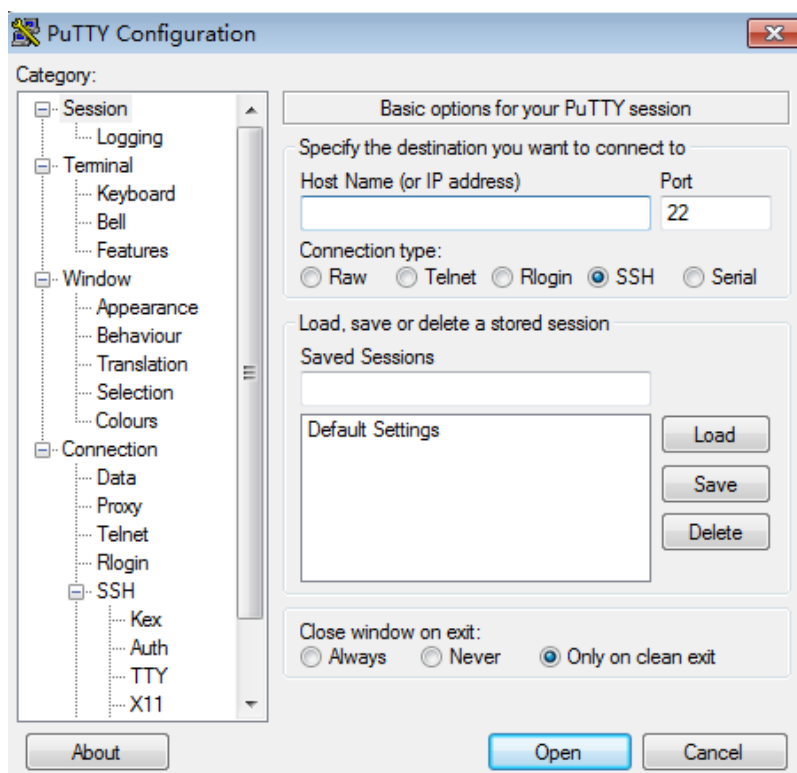
本地使用 Windows 操作系统

如果本地主机为Windows操作系统，可以按照下面方式登录云服务器。

下面步骤以PuTTY为例。

1. 在以下路径中下载PuTTY和PuTTYgen。
<https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>
2. 运行PuTTY。
3. 单击“Session”。
 - a. Host Name (or IP address)：输入云服务器的弹性公网IP。
 - b. Port：输入 22。
 - c. Connection Type：选择 SSH。
 - d. Saved Sessions：任务名称，在下一次使用putty时就可以单击保存的任务名称，即可打开远程连接。

图 2-71 单击“Session”



- 单击“Window”，在“Translation”下的“Received data assumed to be in which character set:”选择“UTF-8”。

- 单击“Open”。

如果首次登录服务器，PuTTY会显示安全警告对话框，询问是否接受服务器的安全证书。单击“是”将证书保存到本地注册表中。

- 建立到云服务器的SSH连接后，根据提示输入用户名和密码登录云服务器。

说明

如果是公共镜像（包括CoreOS），首次登录时，登录用户名、密码如下：

- 用户名：root
- 密码：购买云服务器时，您设置的密码

若购买时云服务器未设置密码，请参考[在控制台重置ECS密码](#)进行设置。

本地使用 Linux 操作系统

如果本地主机为Linux操作系统，您可以在计算机的命令行中通过以下操作登录弹性云服务器。

- 在您的linux计算机的命令行中执行如下命令，登录弹性云服务器。

```
ssh xx.xx.xx.xx
```

说明

xx.xx.xx.xx表示弹性云服务器绑定的弹性公网IP。

- 根据界面提示信息，验证远程主机SSH指纹，并输入“yes”。

```
The authenticity of host 'xx.xx.xx.xx (xx.xx.xx.xx)' can't be established.  
ECDSA key fingerprint is SHA256:rnKuzrUSYS03MCoaXXXXXXXXXXXXXXXXXXXXXXXXXXXX.  
ECDSA key fingerprint is MD5:cf:64:5b:5e:74:30:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx.
```



```
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added 'xx.xx.xx.xx' (ECDSA) to the list of known hosts.
```

- 根据界面提示，输入待登录的弹性云服务器的密码，完成登录操作。
root@xx.xx.xx.xx's password:

```
Welcome to Huawei Cloud Service
```

相关链接

- [忘记密码怎么办？](#)
- [无法登录到Linux云服务器怎么办？](#)

2.5.6 通过 macOS 主机登录 Linux ECS

操作场景

本节为您介绍如何在macOS系统主机上登录Linux云服务器。

前提条件

- 云服务器状态为“运行中”。
- 若您选择SSH密码方式登录，需在购买ECS时设置“登录凭证”为“密码”并已获得Linux云服务器用户名和密码。
忘记密码请参考[在控制台重置ECS密码](#)重置密码。
- 若您选择SSH密钥方式登录，需在购买ECS时设置“登录凭证”为“密钥对”并已获得Linux云服务器的私钥文件。
Linux云服务器的私钥文件在创建密钥对时生成，若私钥文件不慎遗失，可以通过[重置密钥对](#)的方式，重新为弹性云服务器绑定密钥对。若已授权托管私钥，可根据需要将托管的私钥导出使用，详细内容请参见[导出私钥](#)。
- 弹性云服务器已经绑定弹性公网IP，绑定方式请参见[绑定弹性公网IP](#)。
- 所在安全组入方向已开放22端口，配置方式请参见[配置安全组规则](#)。

操作步骤

您可以通过macOS系统自带的终端（Terminal）登录Linux云服务器。

- SSH密码方式
 - 打开系统自带的终端（Terminal），执行以下命令，登录云服务器。
ssh 用户名@弹性公网IP

说明

如果是公共镜像（包括CoreOS），用户名为“root”。
- SSH密钥方式
 - 打开系统自带的终端（Terminal），执行以下命令，变更权限。下面步骤以私钥文件是kp-123.pem为例进行介绍。
chmod 400 /path/kp-123.pem

📖 说明

Linux云服务器的私钥文件在创建密钥对时生成，若私钥文件不慎遗失，可以通过[重置密钥对](#)的方式，重新为弹性云服务器绑定密钥对。若已授权托管私钥，可根据需要将托管的私钥导出使用，详细内容请参见[导出私钥](#)。

上述命令的path为密钥文件的存放路径。

- b. 执行以下命令，登录云服务器。

```
ssh -i /path/kp-123.pem 用户名@弹性公网IP
```

📖 说明

- 如果是“CoreOS”的公共镜像，用户名为“core”。
- 如果是“非CoreOS”的公共镜像，用户名为“root”。

后续处理

- 以SSH密钥方式登录弹性云服务器后，可以通过设置密码（执行passwd命令），后续使用VNC方式登录Linux弹性云服务器。

2.5.7 通过移动设备登录 Linux ECS

操作场景

本节操作介绍如何在移动设备上连接Linux实例。

- 以Termius为例介绍如何在iOS设备上连接 Linux 实例，详细操作请参考[iOS设备上登录Linux云服务器](#)。
- 以JuiceSSH为例介绍如何在Android设备上连接 Linux 实例，详细操作请参考[Android设备上登录Linux云服务器](#)。

前提条件

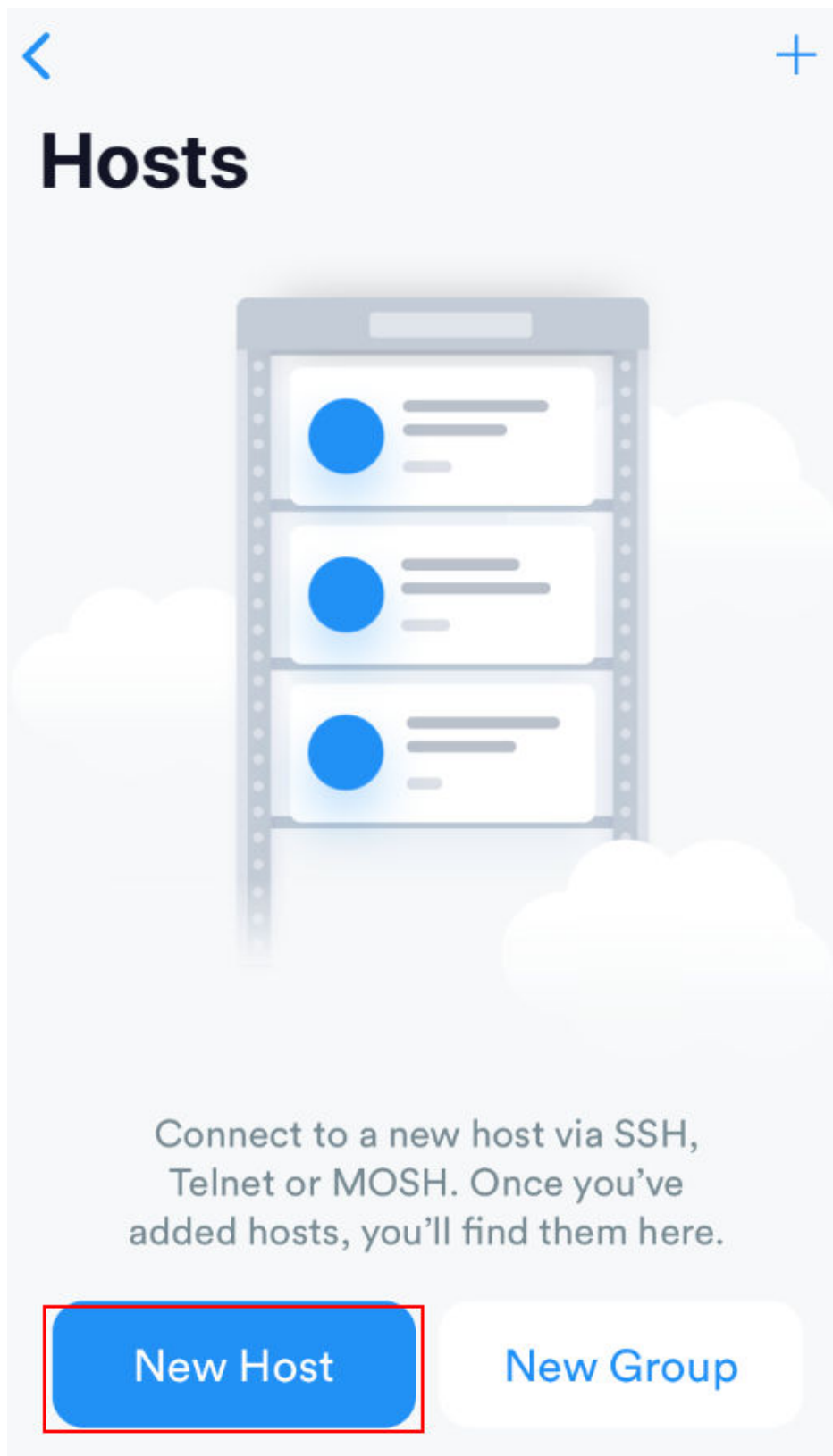
- 云服务器状态为“运行中”。
- 已获取Linux云服务器用户名和密码。忘记密码请参考[在控制台重置ECS密码](#)重置密码。
- 弹性云服务器已经绑定弹性公网IP，绑定方式请参见[绑定弹性公网IP](#)。
- 所在安全组入方向已开放22端口，配置方式请参见[配置安全组规则](#)。

IOS 设备上登录 Linux 云服务器

如果您使用iOS设备，请确保已经安装了SSH客户端工具，以Termius为例。本示例中使用CentOS 7.6操作系统，使用用户名和密码进行认证。

1. 启动Termius，单击New Host。

图 2-72 New Host



2. 在SSH页面上，输入连接信息后，单击 Save。需要输入的连接信息包括：
 - Alias: 指定Host名称，如本例中，设置为ecs01。

- Hostname: 输入需要连接的 Linux 实例的公网IP地址。
- Use SSH: 打开SSH登录配置。
- Host: 输入需要连接的Linux实例的公网IP地址。
- Port: 输入端口号22。
- 用户名: 输入用户名root。
- 密码: 输入实例登录密码。

图 2-73 输入连接信息

CancelNew HostSave

1

Alias

2

Hostname

Group

>

Tags

>

Backspace as CTRL+H

☐

SSH / MOSH

3

Use SSH

☒

Use Mosh (Beta)

☐

4

Port

22
Default

5

Username

root 

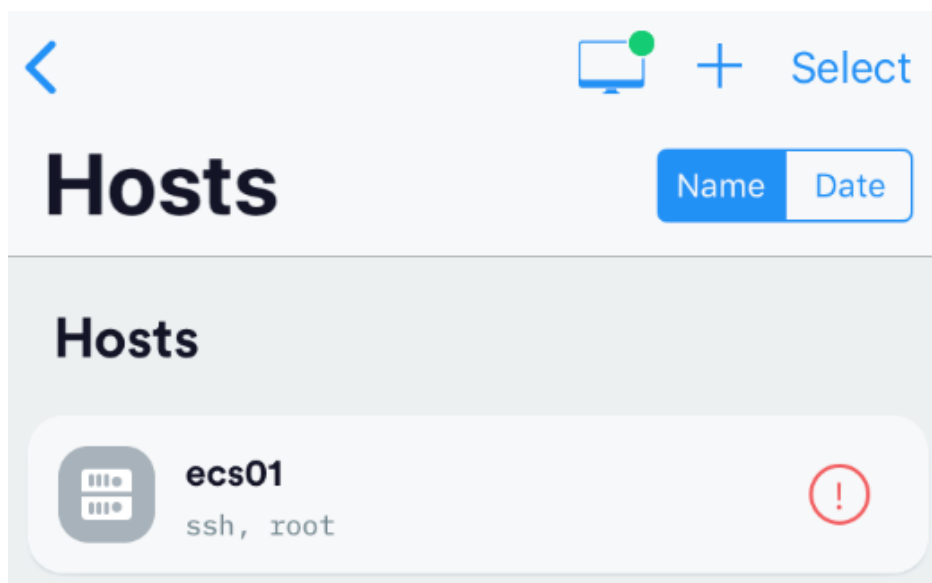
6

Password

●●●●●●●●●●

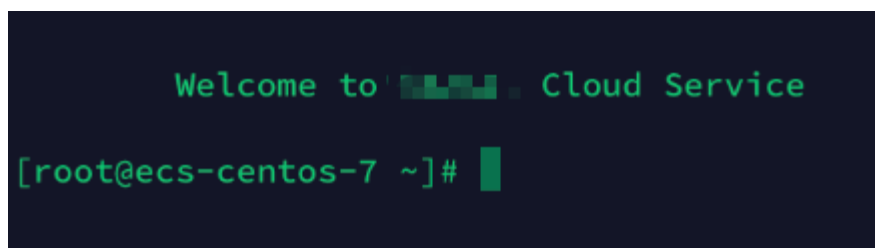
- 单击右上角的“Save”，保存登录信息，在Hosts页面，单击连接的名称远程连接服务器。

图 2-74 保存登录信息



当出现如[图2-75](#)所示页面时，您已经成功地连接了Linux云服务器。

图 2-75 已连接



Android 设备上登录 Linux 云服务器

如果您使用Android设备，请确保已经安装了JuiceSSH。本示例中使用CentOS 7.6操作系统，通过用户名和密码进行认证。

1. 启动JuiceSSH，单击“连接”。

图 2-76 启动 JuiceSSH



2. 在“连接”页面单击图标。

图 2-77 连接



无连接

你还没有配置任何连接。点击下面的按钮开始。



3. 在“新建连接”页面上，添加基本设置和高级设置的信息并保存。需要添加的信息如下：
 - 昵称：指定登录会话的名称，如本例中，设置为“linux_test”。
 - 类型：使用默认值“SSH”。
 - 地址：输入需要登录的Linux实例的弹性公网IP地址。
 - 按以下步骤设置认证：
 - i. 单击“认证”，在下拉列表里单击“新建”。
 - ii. 在“新建认证”页面上，添加如下信息后，单击图标。

- 昵称：可选项，您可以根据需要设置一个身份名称，方便后续管理。如本示例中，设置为“linux_test”。
- 用户名：输入用户名“root”。
- 密码：单击“设置（可选）”后，输入实例的登录密码，单击“确定”。

图 2-78 新建认证



← 新建认证

认证信息

昵称： linux_test

用户名： root

密码： 更新 / 清除

私钥： 设置（可选）

代码片段

JuiceSSH 高级版用户可以自动创建一个代码片段，该代码可用于添加公钥到服务器上的 ~/.ssh/authorized_keys 文件并设置正确的权限。

生成代码片段

- 端口：输入端口号“22”。

图 2-79 端口号

← 新建连接

✓

基本设置

昵称：

linux_test

类型：

SSH

地址：

认证：

linux_test

高级设置

端口：

22

连接方式：

(可选)

运行代码片段：

(可选)

Backspace 模式：

默认发送 (DEL)

连接组

添加到组

- 在“连接”页面单击创建好的连接。

图 2-80 单击连接



5. 确认提示信息后，单击“接受”。

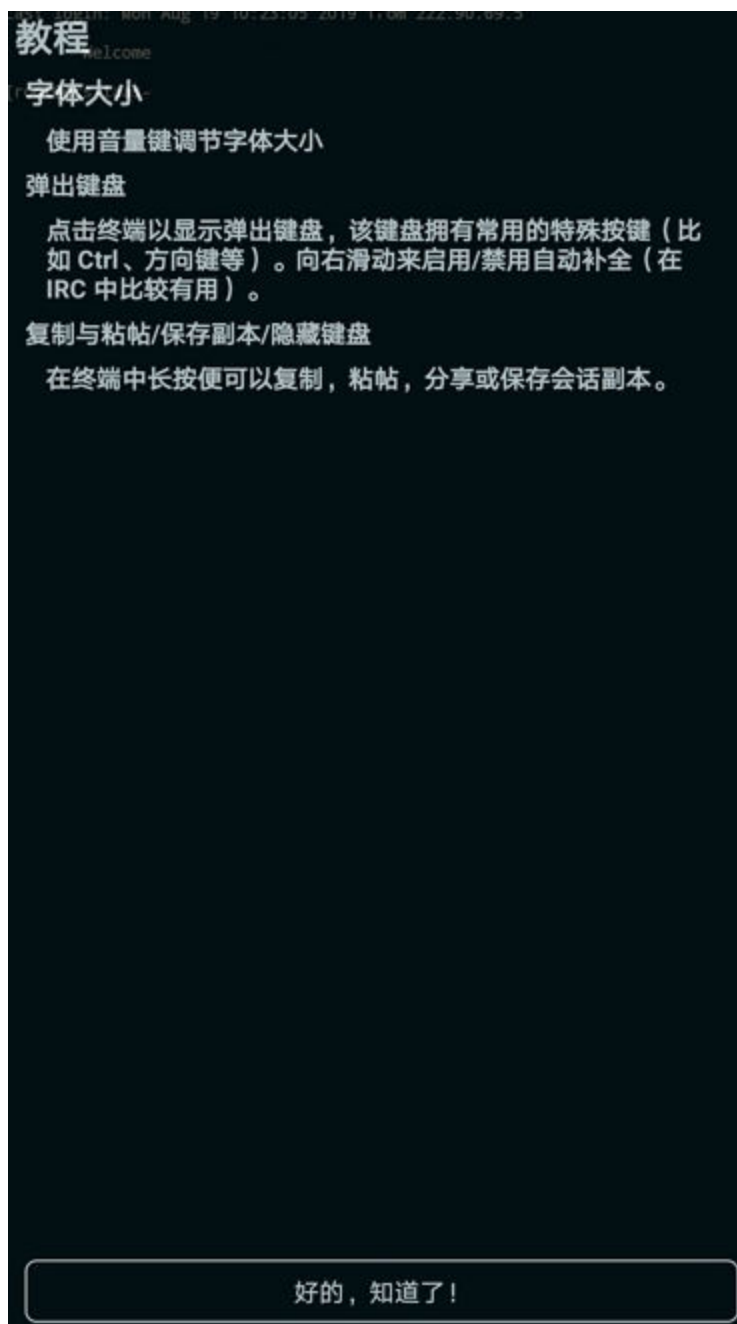


图 2-81 确认提示信息



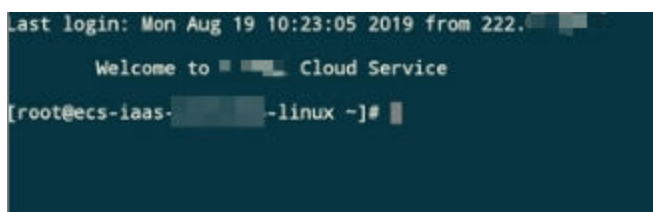
6. （可选）第一次连接时，JuiceSSH会提示您如何设置字体大小，如何弹出键盘等。确认信息后，单击“好的，我知道了！”。

图 2-82 教程



至此，您已经成功登录Linux实例。

图 2-83 登录 Linux 实例



2.5.8 通过华为云 APP 登录 Linux ECS

操作场景

本节操作介绍通过华为云APP连接Linux实例的操作步骤。

前提条件

- 云服务器状态为“运行中”。
- 云服务器已设置登录密码或绑定密钥对。
 - 忘记密码请参考[在控制台重置ECS密码](#)重置密码。
 - 创建密钥对请参见（[推荐](#)）[通过管理控制台创建密钥对](#)。
- 弹性云服务器已经绑定弹性公网IP，绑定方式请参见[绑定弹性公网IP](#)。
- 所在安全组入方向已开放22端口，配置方式请参见[配置安全组规则](#)。

操作步骤

请确保已经在移动端安装了华为云APP。本示例中使用CentOS 8.2操作系统，使用root用户名和密码进行认证。

1. 打开华为云APP，选择“控制台”。

图 2-84 华为云 APP



2. 在控制台页面上选择“我的云服务器 > 弹性云服务器”。

图 2-85 华为云 APP 控制台



3. 选择待连接的云服务器。
可通过单击页面左上方的区域，切换至云服务器所在的区域。
4. 单击“SSH”。使用华为云APP连接云服务器需要创建连接信息和认证信息。

图 2-86 选择待登录的云服务器



5. 创建认证信息。

- a. 单击“添加认证”。
- b. 填写认证信息，并单击“确定”保存。
 - 别名：创建的认证名称，如本例中，设置为“认证01”。
 - 登录名：输入用户名root。
 - 密码：输入实例登录密码。
 - 密钥：如果使用密钥认证，请输入“私钥文件”的完整内容。
 - 1) 打开创建密钥对时下载的“私钥文件”。
创建密钥对及获取私钥文件的操作，请参见[（推荐）通过管理控制台创建密钥对](#)。
 - 2) 拷贝“私钥文件”中的完整内容，并填入“密钥”部分。

图 2-87 新建认证

< 新建认证

别名 认证01

登录名 (必填) root

密码

密钥
请输入

6. 创建连接信息。
 - a. 单击“创建连接”。
 - b. 选择“手动创建连接”。
 - c. 填写连接信息。
 - 别名：创建的连接名称，如本例中，设置为“SSH01”。
 - 地址：输入需要连接的 Linux 实例的公网IP地址。
 - 连接类型：默认为SSH。
 - 使用密钥：默认关闭，使用密码登录。
如果使用密钥对方式登录，请设置为开启。
 - 账户认证：选择已创建认证信息。本例选择在5中创建的认证信息。

- 端口：默认端口号22。

图 2-88 新建连接

< 新建连接

别名 SSH01

地址（必填）

连接类型 SSH

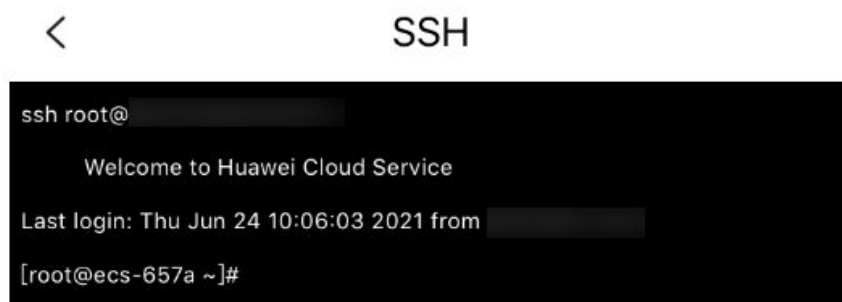
使用密钥
如不开启，默认使用密码登录

帐户认证（必填） 认证01 >

端口（必填） 22

7. 单击“连接”，当出现如图2-89所示页面时，您已经成功地连接了Linux云服务器。

图 2-89 成功连接云服务器



2.6 管理 GPU 加速型 ECS 的 GPU 驱动

2.6.1 GPU 驱动概述

GPU 驱动概述

在使用GPU加速型实例前，请确保实例已安装GPU驱动以获得相应的GPU加速能力。

GPU加速型实例支持两种类型的驱动：GRID驱动和Tesla驱动。

说明

- 当前已支持使用自动化脚本安装GPU驱动，建议优先使用自动安装方式，脚本获取以及安装指导请参考[（推荐）自动安装GPU加速型ECS的GPU驱动（Linux）](#)和[（推荐）自动安装GPU加速型ECS的GPU驱动（Windows）](#)。
- GPU虚拟化型实例，需要严格按照[表2-44](#)选择合适的驱动版本下载使用。
- 如果需要使用OpenGL/DirectX/Vulkan等图形加速能力，则需要安装GRID驱动并自行购买和配置使用GRID License。此外，GRID驱动配合vDWS类型License，也支持CUDA，用来满足既需要计算加速也需要图形加速的场景。
 - 使用公共镜像创建的图形加速型（G系列）实例默认已安装特定版本的GRID驱动，但GRID License需自行购买和配置使用，请提前确认GPU加速型实例是否已经预装或者预装版本是否符合需求。
 - 使用私有镜像创建的GPU加速型实例，如需安装GRID驱动请参考[手动安装GPU加速型ECS的GRID驱动](#)。
 - 如果需要使用计算加速能力，则需要安装Tesla驱动。
 - 使用公共镜像创建的计算加速型（P系列）实例默认已安装特定版本的Tesla驱动。
 - 使用私有镜像创建的GPU加速型实例，如需安装Tesla驱动请参考[手动安装GPU加速型ECS的Tesla驱动](#)。

表 2-41 GPU 驱动支持的加速能力

驱动类型	License	CUDA	OpenGL	DirectX	Vulkan	典型应用场景	说明
GRID驱动	需要	支持	支持	支持	支持	3D渲染、图形工作站、游戏加速	付费使用，需要购买License，满足图形图像类应用加速用途。
Tesla驱动	不需要	支持	不支持	不支持	不支持	科学计算、深度学习训练和推理	通常搭配使用NVIDIA CUDA SDK，可免费下载使用，满足通用计算类应用加速用途。

2.6.2 Tesla 驱动及 CUDA 工具包获取方式

操作场景

使用GPU加速型云服务器时，需确保已安装Tesla驱动和CUDA工具包，否则无法实现计算加速功能。本节内容提供Tesla驱动及CUDA工具包下载地址，请根据实例的类型，选择具体的驱动版本。

Tesla驱动及CUDA工具包安装操作指导请参考[手动安装GPU加速型ECS的Tesla驱动](#)。

 说明

当前已支持使用自动化脚本安装GPU驱动，建议优先使用自动安装方式，脚本获取以及安装指导请参考[（推荐）自动安装GPU加速型ECS的GPU驱动（Linux）](#)和[（推荐）自动安装GPU加速型ECS的GPU驱动（Windows）](#)。

GPU虚拟化型实例，需要严格按照[表2-44](#)选择合适的驱动版本下载使用。

Tesla 驱动下载地址

请单击[NVIDIA驱动下载](#)，根据实例的类型，选择NVIDIA产品类型、产品系列和产品。

表 2-42 Tesla 驱动产品类型对应关系

实例类型	产品类型 (Product Type)	产品系列 (Product Series)	产品 (Product)
P2vs	Tesla	V-Series	V100
P2s	Tesla	V-Series	V100
P2v	Tesla	V-Series	V100
P1	Tesla	P-Series	P100
Pi2	Tesla	T- Series	T4
Pi1	Tesla	P-Series	P4
G6	Tesla	T- Series	T4
G5	Tesla	V-Series	V100

CUDA 工具包下载地址

请从[CUDA软件包下载](#)获取CUDA软件包，您需要根据实例类型和驱动版本，选择对应的CUDA Toolkit软件包产品。

 说明

驱动版本与CUDA Toolkit版本存在对应关系，如二者版本不匹配，可能导致驱动无法使用。
版本对应关系，请参见[NVIDIA驱动下载](#)。

下面以Tesla T4下载驱动软件包及CUDA Toolkit为例进行介绍。

1. Tesla T4安装驱动软件包时，选择Linux操作系统，并指定CUDA Toolkit软件版本为11.6。

图 2-90 指定 CUDA Toolkit 软件版本

Manual Driver Search

Data Center / Tesla

T-Series

Tesla T4

Linux 64-bit

11.6

English (US)

Find

2. 选择对应的版本，下载CUDA软件包。

2.6.3 （推荐）自动安装 GPU 加速型 ECS 的 GPU 驱动（Linux）

操作场景

在使用GPU加速型实例时，需确保实例已安装GPU驱动，否则无法获得相应的GPU加速能力。

本节内容介绍如何在GPU加速型Linux实例上通过脚本自动安装GPU驱动。

使用须知

- 本操作仅支持Linux操作系统。
- 本操作当前仅支持安装Tesla驱动。
- 如果GPU加速型实例已安装GPU驱动，需要先卸载原驱动后再安装新的目标驱动。

GPU驱动自动安装脚本提供卸载驱动的能力，请在执行脚本时根据交互式界面按需选择。

- GPU驱动安装成功后，实例会自动重启。

- 仅部分Linux公共镜像支持通过脚本自动安装GPU驱动，如下所示：
 - CentOS 7.6、CentOS 7.9、CentOS 8.2。
 - Ubuntu 18.04、Ubuntu 20.04、Ubuntu22.04。如果在支持的Linux公共镜像中没有您需要的操作系统及版本，请参考[手动安装GPU加速型ECS的Tesla驱动](#)，手动安装GPU驱动。
- 如果您使用的是私有镜像，请确保镜像已安装了Cloud-init组件及安装GPU驱动所需的依赖，且需使用驱动脚本所支持的Linux操作系统及版本。
- 请根据[表2-43](#)选择需要的驱动安装包版本。

表 2-43 支持的 GPU 驱动版本

CUDA软件版本	Driver软件版本	CuDNN软件版本
10.2	440.118.02	8.0.5
11.0	450.191.01	8.1.1
11.2	460.73.01	8.1.1
11.4	470.103.01	8.2.4
12.2	535.161.08	8.9.6.50

驱动安装脚本支持区域及获取方式

您可以通过执行以下命令，获取驱动安装脚本。

- 华北-北京一

```
wget -t 10 --timeout=10 https://hgcs-drivers-cn-north-1.obs.cn-north-1.myhuaweicloud.com/release/script/auto_install.sh && bash auto_install.sh
```
- 华北-北京二

```
wget -t 10 --timeout=10 https://hgcs-drivers-cn-north-2.obs.cn-north-2.myhuaweicloud.com/release/script/auto_install.sh && bash auto_install.sh
```
- 华北-北京四

```
wget -t 10 --timeout=10 https://hgcs-drivers-cn-north-4.obs.cn-north-4.myhuaweicloud.com/release/script/auto_install.sh && bash auto_install.sh
```
- 华北-乌兰察布一

```
wget -t 10 --timeout=10 https://hgcs-drivers-cn-north-9.obs.cn-north-9.myhuaweicloud.com/release/script/auto_install.sh && bash auto_install.sh
```
- 华东-上海一

```
wget -t 10 --timeout=10 https://hgcs-drivers-cn-east-3.obs.cn-east-3.myhuaweicloud.com/release/script/auto_install.sh && bash auto_install.sh
```
- 华东-上海二

```
wget -t 10 --timeout=10 https://hgcs-drivers-cn-east-2.obs.cn-east-2.myhuaweicloud.com/release/script/auto_install.sh && bash auto_install.sh
```
- 华南-广州

```
wget -t 10 --timeout=10 https://hgcs-drivers-cn-south-1.obs.cn-south-1.myhuaweicloud.com/release/script/auto_install.sh && bash auto_install.sh
```
- 华南-广州-友好用户环境

```
wget -t 10 --timeout=10 https://hgcs-drivers-cn-south-4.obs.cn-south-4.myhuaweicloud.com/release/script/auto_install.sh && bash auto_install.sh
```
- 西南-贵阳一

```
wget -t 10 --timeout=10 https://hgcs-drivers-cn-southwest-2.obs.cn-southwest-2.myhuaweicloud.com/release/script/auto_install.sh && bash auto_install.sh
```

- 中国-香港

```
wget -t 10 --timeout=10 https://hgcs-drivers-ap-southeast-1.obs.ap-southeast-1.myhuaweicloud.com/release/script/auto_install.sh && bash auto_install.sh
```

- 亚太-曼谷

```
wget -t 10 --timeout=10 https://hgcs-drivers-ap-southeast-2.obs.ap-southeast-2.myhuaweicloud.com/release/script/auto_install.sh && bash auto_install.sh
```

- 亚太-新加坡

```
wget -t 10 --timeout=10 https://hgcs-drivers-ap-southeast-3.obs.ap-southeast-3.myhuaweicloud.com/release/script/auto_install.sh && bash auto_install.sh
```

- 非洲-约翰内斯堡

```
wget -t 10 --timeout=10 https://hgcs-drivers-af-south-1.obs.af-south-1.myhuaweicloud.com/release/script/auto_install.sh && bash auto_install.sh
```

操作步骤

以下操作以Ubuntu 20.04 64bit操作系统，P2v规格的GPU加速型实例安装CUDA 11.0对应的Tesla驱动为例进行介绍。

1. 以root账号远程登录云服务器。
2. 执行以下命令，获取驱动安装脚本并运行。

```
wget -t 10 --timeout=10 https://hgcs-drivers-cn-east-2.obs.cn-east-2.myhuaweicloud.com/release/script/auto_install.sh && bash auto_install.sh
```

3. 根据界面提示，选择需要安装的驱动版本。

图 2-91 选择驱动安装版本

```
*****Auto install begin*****
VM: Ubuntu 20.04, p2v.2xlarge.8

*****Optional Software List*****
0: [driver-450.191.01(Tesla), cuda-11.0.3, cudnn-8.1.1]
1: [driver-460.73.01(Tesla), cuda-11.2.2, cudnn-8.1.1]
2: [driver-470.103.01(Tesla), cuda-11.4.4, cudnn-8.2.4]

Please select a software to install? [0/1/2]: 0
```

4. 卸载已安装驱动。
如果云服务器已安装过驱动，请根据提示先执行驱动卸载操作。
如果云服务器本身未安装驱动，脚本会自动跳过该步骤，开始进行驱动安装。
 - a. 卸载CUDA Toolkit。

图 2-92 卸载 CUDA Toolkit (1)

```
*****Optional Software List*****
0: [driver-450.191.01(Tesla), cuda-11.0.3, cudnn-8.1.1]
1: [driver-460.73.01(Tesla), cuda-11.2.2, cudnn-8.1.1]
2: [driver-470.103.01(Tesla), cuda-11.4.4, cudnn-8.2.4]

Please select a software to install? [0/1/2]: 0

The '[driver-450.191.01(Tesla), cuda-11.0.3, cudnn-8.1.1]' will be installed.

*****uninstall software*****

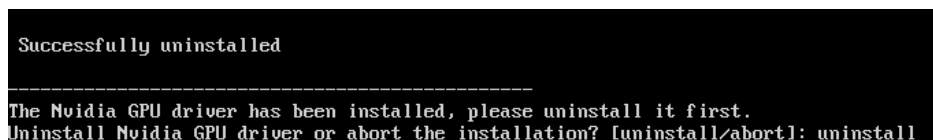
The CUDA Toolkit has been installed, please uninstall it first.
Uninstall CUDA Toolkit or abort the installation? [uninstall/abort]: uninstall
```

图 2-93 卸载 CUDA Toolkit (2)



b. 卸载GPU driver。

图 2-94 卸载 GPU driver



📖 说明

卸载完成后，开始安装驱动，此过程会持续几分钟，请耐心等待。

5. 驱动安装完成后，会自动重启云服务器后，请重新以root账号登录。
6. 执行以下命令，检查驱动是否安装成功。

nvidia-smi

如果返回信息中包含了已安装的驱动版本，说明驱动安装成功。

图 2-95 查看驱动安装结果

```
root@gpu-osdriver-test:~#  
root@gpu-osdriver-test:~# nvidia-smi  
  
Thu Jul 14 14:44:46 2022  
+-----+  
| NVIDIA-SMI 450.191.01    Driver Version: 450.191.01    CUDA Version: 11.0    |  
+-----+  
| GPU   Name               Persistence-M| Bus-Id        Disp.A | Volatile Uncorr. ECC |  
| Fan   Temp  Perf    Pwr:Usage/Cap|      Memory-Usage | GPU-Util  Compute M. |  
|=====================================+=====+  
|    0  Tesla V100-SXM2...    Off      00000000:21:01.0 Off |                    0 |               Default M. |  
| N/A   31C    P0      37W / 300W |  0MiB / 16160MiB |          3%               |  
+-----+  
+-----+  
| Processes:                                                       GPU Memory |  
|  GPU   GI    CI          PID    Type   Process name                      Usage    |  
|  ID     ID                                  |  
+-----+  
| No running processes found                                     |  
+-----+  
root@gpu-osdriver-test:~#  
root@gpu-osdriver-test:~#
```

7. 执行以下命令，检查CUDA版本是否正确。

```
/usr/local/cuda/bin/nvcc -V
```

图 2-96 检查 CUDA 版本

```
root@gpu-osdriver-test:~# /usr/local/cuda/bin/nvcc -V  
nvcc: NVIDIA (R) Cuda compiler driver  
Copyright (c) 2005-2020 NVIDIA Corporation  
Built on Wed Jul 22 19:09:09 PDT 2020  
Cuda compilation tools, release 11.0, V11.0.221  
Build cuda_11.0_bu.TC445_37.28845127_0
```

8. （可选）检查CUDA是否正常。
- 执行以下命令，进入“/usr/local/cuda/samples/1_Uutilities/deviceQuery”目录。
cd /usr/local/cuda/samples/1_Uutilities/deviceQuery
 - 执行以下命令，自动编译deviceQuery程序。
make
 - 执行以下命令，查看CUDA是否安装成功。
./deviceQuery
如果返回信息中有CUDA的版本信息，则表明CUDA安装成功。

图 2-97 查看 CUDA 安装结果

```
root@gpu-osdriver-test:/usr/local/cuda/samples/1_Uutilities/deviceQuery# ./deviceQuery
./deviceQuery Starting...

CUDA Device Query (Runtime API) version (CUDA RTI static linking)

Detected 1 CUDA Capable device(s)

Device 0: "Tesla V100-SXM2-16GB"
  CUDA Driver Version / Runtime Version      11.0 / 11.0
  CUDA Capability Major/Minor version number: 7.0
  Total amount of global memory:              16160 MBytes (16945512448 bytes)
  (80) Multiprocessors, ( 64) CUDA Cores/MP: 5120 CUDA Cores
  GPU Max Clock rate:                        1530 MHz (1.53 GHz)
  Memory Clock rate:                          877 Mhz
  Memory Bus Width:                          4096-bit
  L2 Cache Size:                             6291456 bytes
  Maximum Texture Dimension Size (x,y,z)      1D=(131072), 2D=(131072, 65536), 3D=(16384, 16384, 16384)
  Maximum Layered 1D Texture Size, (num) layers 1D=(32768), 2048 layers
  Maximum Layered 2D Texture Size, (num) layers 2D=(32768, 32768), 2048 layers
  Total amount of constant memory:            65536 bytes
  Total amount of shared memory per block:    49152 bytes
  Total number of registers available per block: 65536
  Warp size:                                 32
  Maximum number of threads per multiprocessor: 2048
  Maximum number of threads per block:        1024
  Max dimension size of a thread block (x,y,z): (1024, 1024, 64)
  Max dimension size of a grid size (x,y,z):  (2147483647, 65535, 65535)
  Maximum memory pitch:                      2147483647 bytes
  Texture alignment:                          512 bytes
  Concurrent copy and kernel execution:       Yes with 2 copy engine(s)
  Run time limit on kernels:                  No
  Integrated GPU sharing Host Memory:         No
  Support host page-locked memory mapping:    Yes
  Alignment requirement for Surfaces:         Yes
  Device has ECC support:                     Enabled
  Device supports Unified Addressing (UVA):    Yes
  Device supports Managed Memory:             Yes
  Device supports Compute Preemption:         Yes
  Supports Cooperative Kernel Launch:         Yes
  Supports MultiDevice Co-op Kernel Launch:   Yes
  Device PCI Domain ID / Bus ID / location ID: 0 / 33 / 1
  Compute Mode:
    < Default (multiple host threads can use ::cudaSetDevice() with device simultaneously) >

deviceQuery, CUDA Driver = CUDART, CUDA Driver Version = 11.0, CUDA Runtime Version = 11.0, NumDevs = 1
Result = PASS
```

2.6.4 （推荐）自动安装 GPU 加速型 ECS 的 GPU 驱动（Windows）

操作场景

在使用GPU加速型实例时，需确保实例已安装GPU驱动，否则无法获得相应的GPU加速能力。

本节内容介绍如何在GPU加速型Windows实例上通过脚本自动安装GPU驱动。

使用须知

- 如果GPU加速型实例已安装GPU驱动，需要先卸载原驱动后再安装新的目标驱动。
- 当前仅部分GPU加速型实例的规格、部分Windows操作系统版本支持通过脚本自动安装GPU驱动。
 - Windows Server 2016 数据中心版
 - Windows Server 2019 数据中心版

如果您的规格、操作系统或驱动版本不支持通过脚本自动安装GPU驱动，请参考[手动安装GPU加速型ECS的GRID驱动](#)和[手动安装GPU加速型ECS的Tesla驱动](#)，手动安装GPU驱动。

驱动安装脚本支持区域及获取方式

您可以在PowerShell上执行以下命令，获取驱动安装脚本。

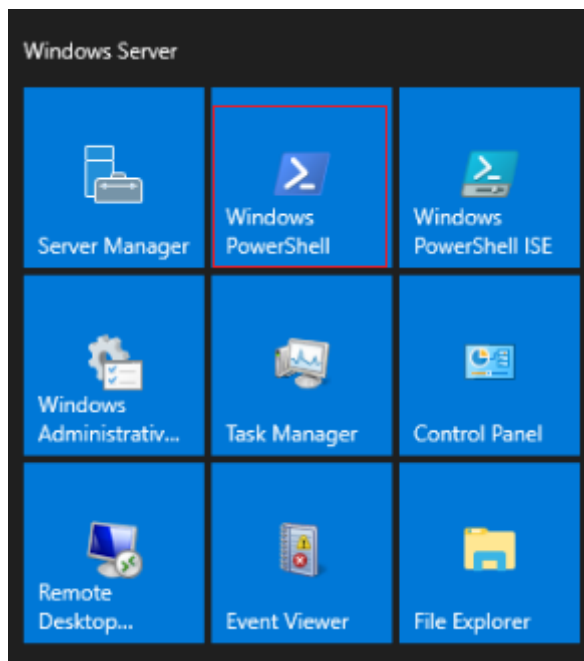
- 华北-北京一
Start-BitsTransfer -Source https://hgcs-drivers-cn-north-1.obs.cn-north-1.myhuaweicloud.com/release/script/auto_install.ps1 -Destination auto_install.ps1; ./auto_install.ps1
- 华北-北京二
Start-BitsTransfer -Source https://hgcs-drivers-cn-north-2.obs.cn-north-2.myhuaweicloud.com/release/script/auto_install.ps1 -Destination auto_install.ps1; ./auto_install.ps1
- 华北-北京四
Start-BitsTransfer -Source https://hgcs-drivers-cn-north-4.obs.cn-north-4.myhuaweicloud.com/release/script/auto_install.ps1 -Destination auto_install.ps1; ./auto_install.ps1
- 华北-乌兰察布一
Start-BitsTransfer -Source https://hgcs-drivers-cn-north-9.obs.cn-north-9.myhuaweicloud.com/release/script/auto_install.ps1 -Destination auto_install.ps1; ./auto_install.ps1
- 华东-上海一
Start-BitsTransfer -Source https://hgcs-drivers-cn-east-3.obs.cn-east-3.myhuaweicloud.com/release/script/auto_install.ps1 -Destination auto_install.ps1; ./auto_install.ps1
- 华东-上海二
Start-BitsTransfer -Source https://hgcs-drivers-cn-east-2.obs.cn-east-2.myhuaweicloud.com/release/script/auto_install.ps1 -Destination auto_install.ps1; ./auto_install.ps1
- 华南-广州
Start-BitsTransfer -Source https://hgcs-drivers-cn-south-1.obs.cn-south-1.myhuaweicloud.com/release/script/auto_install.ps1 -Destination auto_install.ps1; ./auto_install.ps1
- 华南-广州-友好用户环境
Start-BitsTransfer -Source https://hgcs-drivers-cn-south-4.obs.cn-south-4.myhuaweicloud.com/release/script/auto_install.ps1 -Destination auto_install.ps1; ./auto_install.ps1
- 西南-贵阳一
Start-BitsTransfer -Source https://hgcs-drivers-cn-southwest-2.obs.cn-southwest-2.myhuaweicloud.com/release/script/auto_install.ps1 -Destination auto_install.ps1; ./auto_install.ps1
- 中国-香港
Start-BitsTransfer -Source https://hgcs-drivers-ap-southeast-1.obs.ap-southeast-1.myhuaweicloud.com/release/script/auto_install.ps1 -Destination auto_install.ps1; ./auto_install.ps1
- 亚太-曼谷
Start-BitsTransfer -Source https://hgcs-drivers-ap-southeast-2.obs.ap-southeast-2.myhuaweicloud.com/release/script/auto_install.ps1 -Destination auto_install.ps1; ./auto_install.ps1
- 亚太-新加坡
Start-BitsTransfer -Source https://hgcs-drivers-ap-southeast-3.obs.ap-southeast-3.myhuaweicloud.com/release/script/auto_install.ps1 -Destination auto_install.ps1; ./auto_install.ps1
- 非洲-约翰内斯堡
Start-BitsTransfer -Source https://hgcs-drivers-af-south-1.obs.af-south-1.myhuaweicloud.com/release/script/auto_install.ps1 -Destination auto_install.ps1; ./auto_install.ps1

操作步骤

以下操作以Windows Server 2019 数据中心版操作系统，G6规格的GPU加速型实例安装Grid驱动为例进行介绍。

1. 远程登录云服务器。
2. 单击“启动”，打开Windows PowerShell。

图 2-98 打开 PowerShell

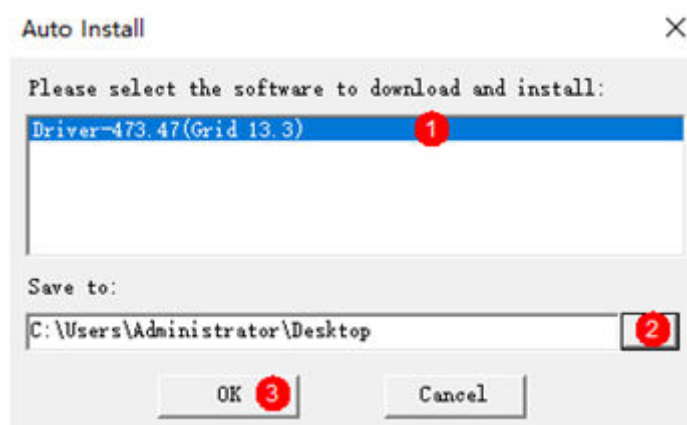


3. 在PowerShell中，执行以下命令，获取驱动安装脚本并运行。
以“华北-北京四”为例介绍，更多区域请参考[驱动安装脚本支持区域及获取方式](#)。

```
Start-BitsTransfer -Source https://hgcs-drivers-cn-north-4.obs.cn-north-4.myhuaweicloud.com/release/script/auto_install.ps1 -Destination auto_install.ps1; ./auto_install.ps1
```

4. 选择驱动版本与保存路径。

图 2-99 选择驱动版本与保存路径



5. 单击“OK”，开始安装驱动。

图 2-100 安装驱动

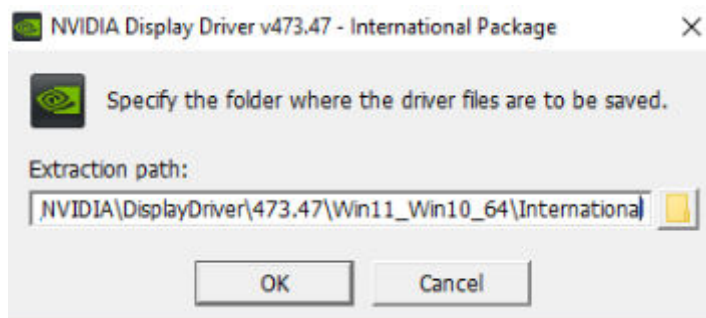
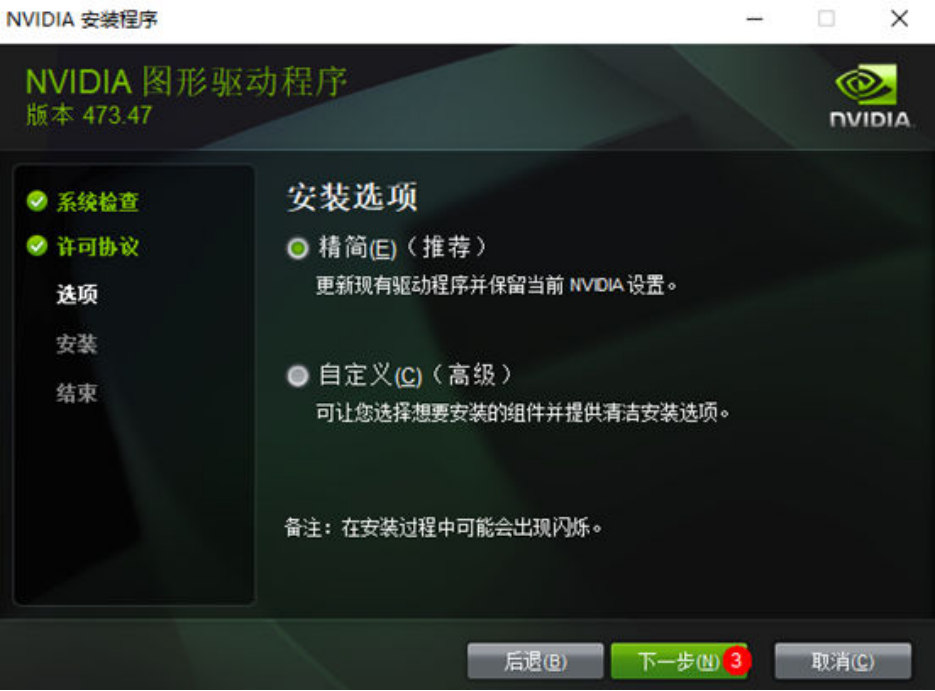


图 2-101 同意 NVIDIA 软件许可协议



图 2-102 选择安装选项



6. 驱动安装完成后，可能需要重启云服务器。
- a. 如果需要重启，单击“稍后重启”，待脚本执行完成后，手动重启云服务器。

图 2-103 稍后重启



- b. 如果不需要重启，单击“关闭”。

图 2-104 关闭



7. 返回桌面，在空白处右键单击，选择“NVIDIA控制面板”，查看驱动版本，判断驱动是否安装成功。
若显示如下版本，表示驱动安装成功。

图 2-105 驱动版本



2.6.5 手动安装 GPU 加速型 ECS 的 GRID 驱动

操作场景

GPU加速型实例如需使用OpenGL/DirectX/Vulkan等图形加速能力则需要安装GRID驱动并自行购买和配置使用GRID License。此外，GRID驱动配合vDWS类型License，也支持CUDA，用来满足既需要计算加速也需要图形加速的场景。

- 使用公共镜像创建的图形加速型（G系列）实例默认已安装特定版本的GRID驱动，但GRID License需自行购买和配置使用。
- 使用私有镜像创建的GPU加速型实例，则需要安装GRID驱动并自行购买和配置使用GRID License。

说明

如果通过私有镜像创建的GPU实例使用虚拟化类型的GPU显卡（如G6v），请确保下载和安装与公共镜像创建云服务器时相同的GRID驱动版本，以确保驱动与主机配套，云服务器可正常运行。

GRID驱动版本，请参见[表2-44](#)。

本节操作介绍如何安装GRID驱动，购买或者申请GRID License，以及如何配置License服务器。

安装GRID驱动操作步骤：

1. [购买GRID License](#)
2. [下载GRID驱动及License软件包](#)
3. [部署和配置License Server](#)
4. [安装GRID驱动并配置License](#)

说明

- NVIDIA支持用户申请90天试用版License。
- 不同规格的GPU实例介绍和应用场景请参见[GPU加速型](#)。

购买 GRID License

- 购买License
如果需要正式版本License，请联系NVIDIA或者所在国家/地区的NVIDIA代理商。
- 申请试用版License。
打开[NVIDIA官方网站](#)，填写相关信息。
注册账号和申请试用版License的注意事项请参见[NVIDIA官方帮助页](#)。

说明

试用版License的使用方法和正式版本的License一致，可以保留试用版账号激活正式版本的License，无需重新注册。试用版License有限期限为90天，账号过期将无法使用，请尽快购买正式版本。

图 2-106 申请试用版 License

Environment

* Certified Server: Other	▼	* NVIDIA GPUs: V100	▼
* VDI Hypervisor: RedHat Virtualization	▼	* VDI Remoting Client: Select an Option	▼
* VDI Seats: Select an Option	▼	Other Applications:	
* Primary Application: Select (1-3) Options	▼		

下载 GRID 驱动及 License 软件包

1. 请根据[表2-44](#)对应操作系统下载驱动安装包。
了解更多GRID驱动信息请参考[NVIDIA vGPU驱动](#)。

 说明

GPU直通型实例：根据需求选择GRID驱动版本。
GPU虚拟化型实例：请严格按照下表选择合适的驱动版本下载使用。

表 2-44 GPU 实例类型支持的 GRID 驱动版本

实例类型	GPU挂载方式	操作系统	驱动版本	CPU架构
G6v	GPU虚拟化型实例	- CentOS 8.2 64bit - CentOS 7.6 64bit - Ubuntu 20.04 server 64bit - Ubuntu 18.04 server 64bit - Windows Server 2019 Standard 64bit - Windows Server 2019 Datacenter 64bit - Windows Server 2016 Datacenter 64bit	GRID 11.1	x86_64

实例类型	GPU挂载方式	操作系统	驱动版本	CPU架构
G6	GPU直通型实例	• Huawei Cloud EulerOS 2.0 64bit • CentOS 8.2 64bit • CentOS 8.1 64bit • CentOS 8.0 64bit • CentOS 7.9 64bit • CentOS 7.8 64bit • CentOS 7.7 64bit • CentOS 7.6 64bit • CentOS 7.5 64bit • Ubuntu 22.04 64bit • Ubuntu 20.04 64bit • Ubuntu 18.04 64bit • Ubuntu 16.04 64bit • Windows Server 2022 Standard 64bit • Windows Server 2019 Standard 64bit • Windows Server 2022 Datacenter 64bit • Windows Server 2019 Datacenter 64bit • Windows Server 2016 Datacenter 64bit	按需选择版本	x86_64
G5.8xlarge.4	GPU直通型实例	• CentOS 8.2 64bit • CentOS 7.6 64bit • CentOS 7.5 64bit • Ubuntu 20.04 64bit • Ubuntu 18.04 64bit • Windows Server 2019 Standard 64bit • Windows Server 2019 Datacenter 64bit • Windows Server 2016 Datacenter 64bit	按需选择版本	x86_64

实例类型	GPU挂载方式	操作系统	驱动版本	CPU架构
G3	GPU直通型实例	- Windows Server 2019 Standard 64bit - Windows Server 2019 Datacenter 64bit - Windows Server 2016 Datacenter 64bit	按需选择版本	x86_64
G1	GPU虚拟化型实例	Windows Server 2016 Datacenter 64bit	vGPU 4.1: GRID for UVP	x86_64
P2vs	GPU直通型实例	- CentOS 7.5 64bit - Ubuntu 16.04 server 64bit - Windows Server 2016 Standard 64bit	按需选择版本	x86_64
P2s	GPU直通型实例	- Huawei Cloud EulerOS 2.0 64bit - CentOS 8.2 64bit - CentOS 8.1 64bit - CentOS 8.0 64bit - CentOS 7.9 64bit - CentOS 7.8 64bit - CentOS 7.7 64bit - CentOS 7.6 64bit - Ubuntu 22.04 server 64bit - Ubuntu 20.04 server 64bit - Ubuntu 18.04 server 64bit - Ubuntu 16.04 server 64bit - Windows Server 2022 Standard 64bit - Windows Server 2019 Standard 64bit - Windows Server 2022 Datacenter 64bit - Windows Server 2019 Datacenter 64bit - Windows Server 2016 Datacenter 64bit	按需选择版本	x86_64

实例类型	GPU挂载方式	操作系统	驱动版本	CPU架构
P2v	GPU直通型实例	- CentOS 7.4 64bit - EulerOS 2.2 64bit - Ubuntu 20.04 server 64bit - Ubuntu 18.04 server 64bit - Ubuntu 16.04 server 64bit - Windows Server 2019 Standard 64bit - Windows Server 2019 Datacenter 64bit - Windows Server 2016 Datacenter 64bit	按需选择版本	x86_64
P1	GPU直通型实例	- CentOS 7.3 64bit - Ubuntu 16.04 server 64bit - EulerOS 2.2 64bit - Debian 8.0.0 64bit - Windows Server 2022 Standard 64bit - Windows Server 2019 Standard 64bit - Windows Server 2022 Datacenter 64bit - Windows Server 2019 Datacenter 64bit - Windows Server 2016 Datacenter 64bit	按需选择版本	x86_64

实例类型	GPU挂载方式	操作系统	驱动版本	CPU架构
Pi2	GPU直通型实例	• Huawei Cloud EulerOS 2.0 64bit • CentOS 8.2 64bit • CentOS 8.1 64bit • CentOS 8.0 64bit • CentOS 7.9 64bit • CentOS 7.8 64bit • CentOS 7.7 64bit • CentOS 7.6 64bit • CentOS 7.5 64bit • Ubuntu 22.04 server 64bit • Ubuntu 20.04 server 64bit • Ubuntu 18.04 server 64bit • Ubuntu 16.04 server 64bit • Windows Server 2022 Standard 64bit • Windows Server 2019 Standard 64bit • Windows Server 2022 Datacenter 64bit • Windows Server 2019 Datacenter 64bit • Windows Server 2016 Datacenter 64bit	按需选择版本	x86_64

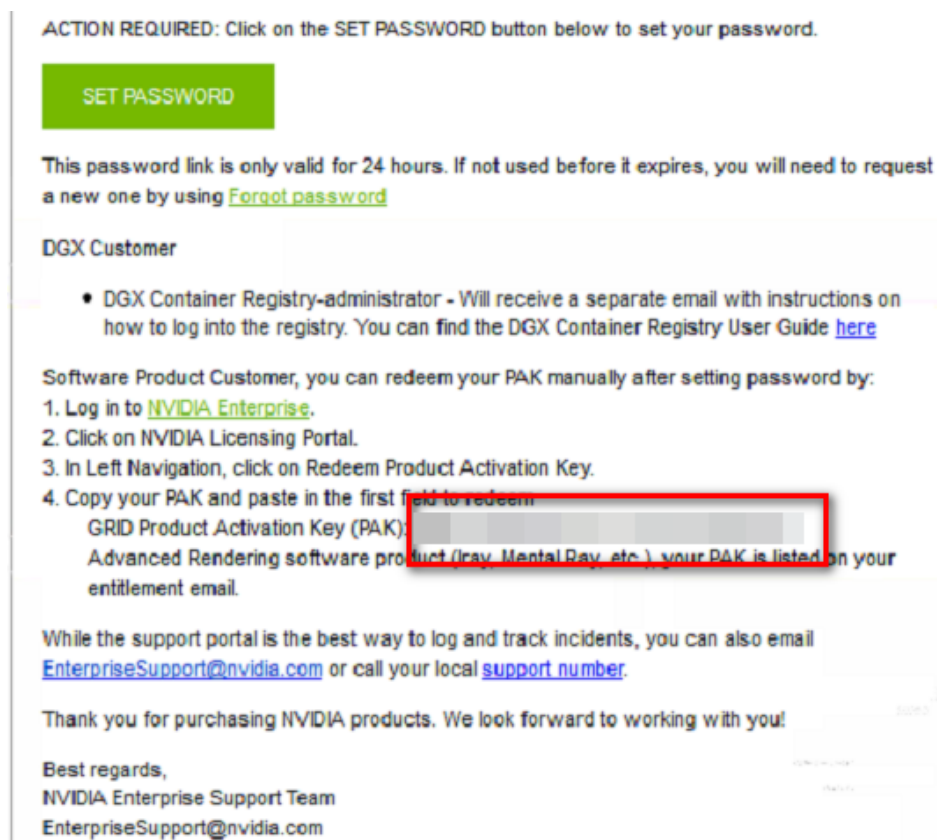
实例类型	GPU挂载方式	操作系统	驱动版本	CPU架构
Pi1	GPU直通型实例	- CentOS 7.3 64bit - Ubuntu 20.04 server 64bit - Ubuntu 16.04 server 64bit - Ubuntu 14.04 server 64bit - Windows Server 2019 Standard 64bit - Windows Server 2019 Datacenter 64bit - Windows Server 2016 Datacenter 64bit	按需选择版本	x86_64

2. 注册成功后，登录[NVIDIA官网](#)，填写账户信息。
3. 判断是否为首次注册使用NVIDIA。

a. 是，执行4。

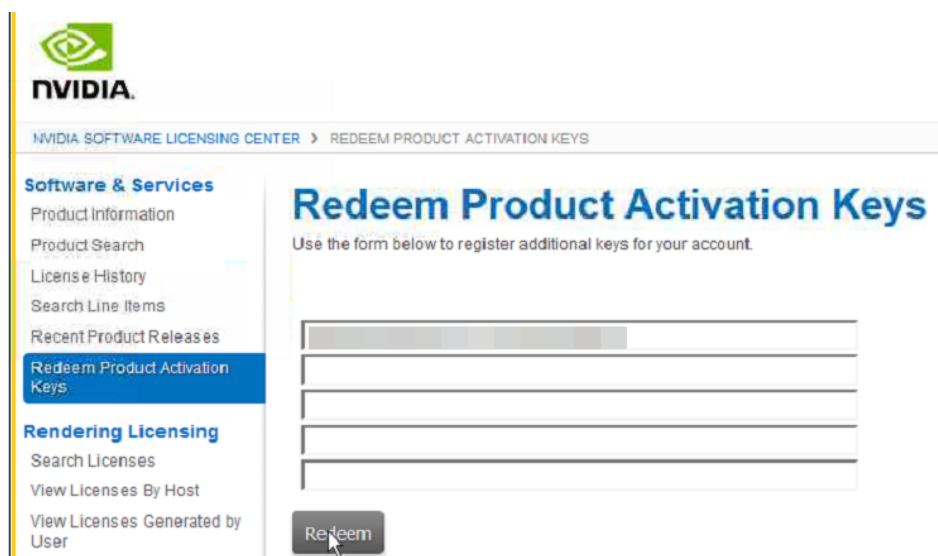
b. 否，执行6。
4. 在注册NVIDIA用户成功的邮件中，查询PAK，如[图2-107](#)所示。

图 2-107 注册 PAK



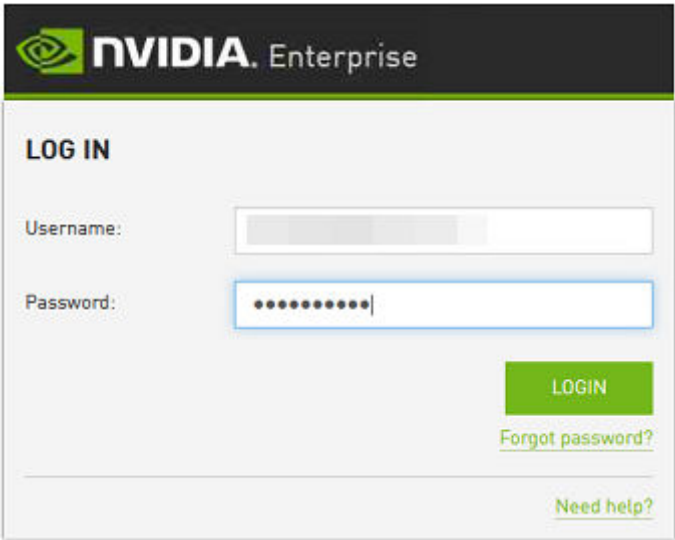
5. 将4中查找的PAK填写在“Redeem Product Activation Keys”页面，并单击“Redeem”。

图 2-108 Redeem Product Activation Keys



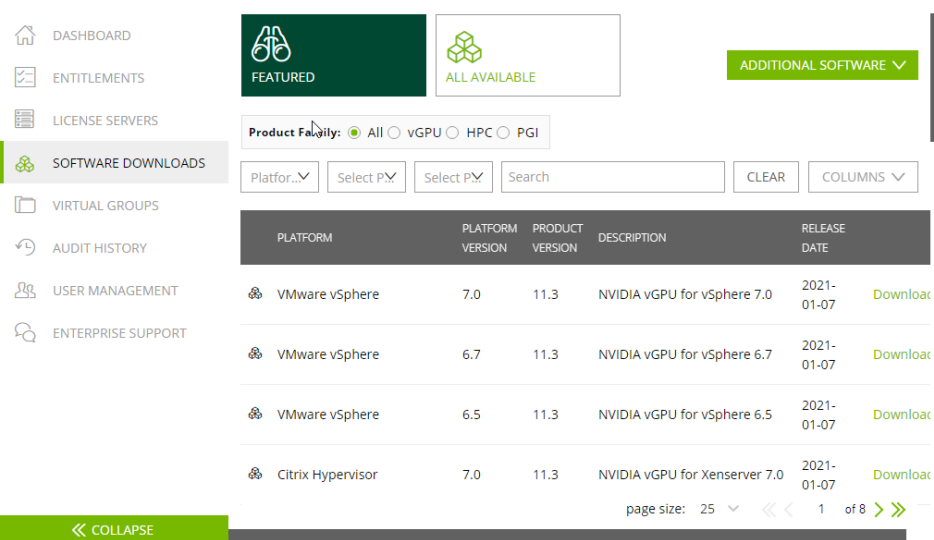
6. 输入“用户名”和“密码”，并单击“登录”。

图 2-109 登录 NVIDIA 官网



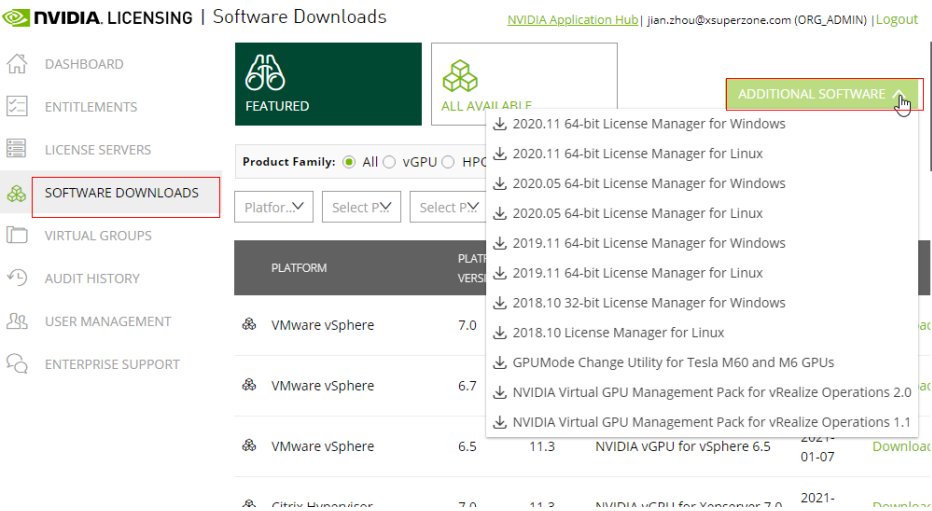
7. 根据界面提示，进入NVIDIA网站，并选择“SOFTWARE DOWNLOADS”。

图 2-110 打开 NVIDIA 网站



8. 对照表2-44选择相应版本的GRID驱动下载。
9. 解压缩GRID驱动包，并选择和弹性云服务器操作系统匹配的驱动进行安装。
10. 在“SOFTWARE DOWNLOADS”页面，单击“ADDITIONAL SOFTWARE”，下载License软件包。

图 2-111 选择 SOFTWARE DOWNLOADS



部署和配置 License Server

以CentOS 7.5操作系统的云服务器为例演示部署和配置License Server。

说明

- 云服务器规格不小于2vCPU，内存不小于4GiB。
 - 请提前记录云服务器MAC地址。
 - 如用作生产用途，建议采用高可用模式部署，主备高可用模式部署License Server 请参考 [NVIDIA官方License Server高可用部署文档](#)。
- 配置网络：
 - 如使用VPC网络访问License Server：请确保License Server和使用GRID驱动的GPU加速型实例处在同一个VPC子网内。
 - 如使用公网IP访问License Server：请配置License Server所在的安全组，增加方向规则：TCP 7070和TCP 8080。
 - 安装License Server。
 - 执行以下命令，解压缩安装包。其中“安装程序.zip”为10获取到的安装包名称。

unzip 安装程序.zip
 - 执行以下命令，为安装程序添加执行权限。

chmod +x setup.bin
 - 以root用户运行安装程序。

sudo ./setup.bin -i console
 - 在Introduction部分，单击回车键继续。

```
=====
Introduction
-----

InstallAnywhere will guide you through the installation of License Server.

It is strongly recommended that you quit all programs before continuing with
this installation.

Respond to each prompt to proceed to the next step in the installation. If
you want to change something on a previous step, type 'back'.

You may cancel this installation at any time by typing 'quit'.

PRESS <ENTER> TO CONTINUE: █
```

- e. 在License Agreement部分，通过单击回车键进行翻页，翻页结束后接受许可协议。
- 当您达成许可协议时，系统会提示您接受许可协议条款，请输入“Y”，并单击回车键。

```
DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT? (Y/N): Y █
```

- f. 在Choose Install Folder部分，单击回车键，保持默认的License Server软件安装路径。
- g. 在Choose Local Tomcat Server Path部分，输入Tomcat的本地路径，默认为/var/lib/tomcat版本号，例如：/var/lib/tomcat8。
- h. 在Choose Firewall Options部分，确认需要在防火墙中打开的端口，单击回车键，保持默认选项即可。

```
Choose Firewall Options
-----

The license server listens on port 7070. This port must be opened in the
firewall for other machines to obtain licenses from this server.

The license server's management interface listens on port 8080. Leave this
port closed to prevent unauthorized access to the management interface.

->1- License server (port 7070)
   2- Management interface (port 8080)

ENTER A COMMA-SEPARATED LIST OF NUMBERS REPRESENTING THE DESIRED CHOICES, OR
PRESS <ENTER> TO ACCEPT THE DEFAULT: █
```

- i. 在Pre-Installation Summary部分，确认信息并单击回车键启动安装。

```
Pre-Installation Summary
-----

Please Review the Following Before Continuing:

Product Name:
    License Server

Install Folder:
    /opt/flexnetls/nvidia

Link Folder:
    /root/NVIDIA Corporation/License Server

Disk Space Information (for Installation Target):
    Required:    105,216,774 Bytes
    Available: 35,501,248,512 Bytes

PRESS <ENTER> TO CONTINUE: █
```

- j. 在Install Complete部分，单击回车键，结束安装。

```
Install Complete
-----

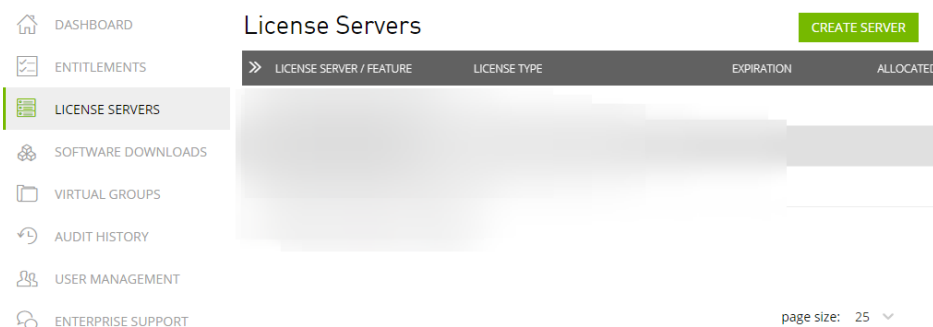
License Server has been successfully installed to:

    /opt/flexnetls/nvidia

PRESS <ENTER> TO EXIT THE INSTALLER:
```

3. 获取License文件。
a. 新建页签，登录[NVIDIA网站](#)，选择“LICENSE SERVERS”。

图 2-112 选择 LICENSE SERVERS



- b. 单击“CREATE SERVER”。
c. 在“Create License Server”界面，根据界面提示配置参数。

图 2-113 填写 LICENSE SERVERS 信息

Create License Server

Server Name

Name this license server

Feature

Select a feature

Licenses

1

ADD

Description

Provide a short description

MAC Address

MAC Address (XX:XX:XX:XX:XX:XX or XX-XX-XX-XX-XX-XX)

Failover License Server

Failover License Server

Failover MAC Address

Failover MAC Address

Added Features

FEATURE	COUNT
No features have been added yet	

CANCEL

RESET

CREATE LICENSE SERVER

表 2-45 LICENSE SERVERS 信息填写说明

参数	说明
Server Name	自定义需要的License Server名称。
Description	License Server的描述信息。
MAC Address	填写用于搭建License Server的ECS实例的MAC地址。 您可以登录实例，使用ipconfig -a命令进行查询。
Feature	在Licenses框中输入需要的license数目，单击“ADD”。 如果是主备部署的情况需要把备服务器的名称填入 Failover License Server，MAC地址填入 Failover MAC Address中。

- d. 单击“CREATE LICENSE SERVER”。
- e. 下载License文件。

图 2-114 下载 License 文件

DASHBOARD

ENTITLEMENTS

LICENSE SERVERS

SOFTWARE DOWNLOADS

VIRTUAL GROUPS

License Servers

CREATE SERVER

LICENSE SERVER / FEATURE	LICENSE TYPE	EXPIRATION	ALLOCATED
test			

DOWNLOAD LICENSE FILE

MANAGE LICENSES

REMOVE FEATURES

ADD FEAT

DELETE SERVER

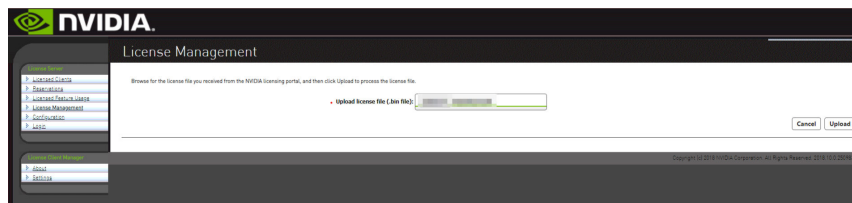
Quadro-Virtual-DWS-5.0 CONCURRENT_COUNTED_SINGLE 1 / 1

4. 在Web浏览器中，根据安装时配置的管理页面链接，访问License Server管理界面的主页。

默认访问链接为：<http://弹性公网IP地址:8080/licserver>。

5. 在左侧导航树中，单击“License Server > License Management”。
6. 使用License服务器配置菜单导入，并单击“Upload”上传许可证*.bin文件，完成License Server的配置。

图 2-115 上传许可证文件



安装 GRID 驱动并配置 License

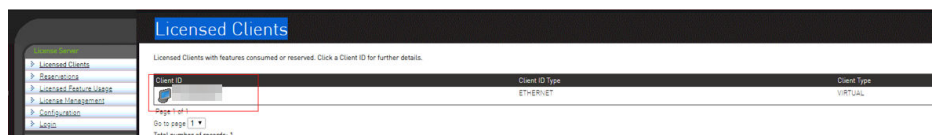
1. 以Windows操作系统GPU加速型实例为例，选择合适版本的GRID驱动进行安装。

说明

微软的远程登录协议不支持使用GPU的3D硬件加速能力，如需使用请安装VNC/PCoIP/NICE DCV等第三方桌面协议软件，并通过相应客户端连接GPU实例，使用GPU图形图像加速能力。

2. 使用第三方桌面协议连接后，在Windows控制面板中打开NVIDIA控制面板。
3. 在一级许可证服务器中填入部署的License server的IP和端口，并单击应用。当出现“您的系统已获GRID vGPU许可”则代表安装GRID驱动成功，并且可以在License Server管理控制台Licensed Clients中看到已安装GRID驱动并使用了License的GPU实例的MAC地址。

图 2-116 License Server 管理控制台



2.6.6 手动安装 GPU 加速型 ECS 的 Tesla 驱动

操作场景

GPU加速型云服务器，需要安装Tesla驱动和CUDA工具包以实现计算加速功能。

- 使用公共镜像创建的加速型（P系列）实例默认已安装特定版本的Tesla驱动。
- 使用私有镜像创建的GPU加速型云服务器，需在创建完成后安装Tesla驱动，否则无法实现计算加速功能。

本节操作介绍GPU云服务器安装Tesla驱动及CUDA工具包的操作步骤。

📖 说明

当前已支持使用自动化脚本安装GPU驱动，建议优先使用自动安装方式，脚本获取以及安装指导请参考[（推荐）自动安装GPU加速型ECS的GPU驱动（Linux）](#)和[（推荐）自动安装GPU加速型ECS的GPU驱动（Windows）](#)。

GPU虚拟化型实例，需要严格按照[表2-44](#)选择合适的驱动版本下载使用。

安装须知

- 云服务器已绑定弹性公网IP。
- 云服务器未安装Tesla驱动以及CUDA工具包。

📖 说明

- 从NVIDIA官网下载CUDA工具包进行安装，通常会同时自动安装一个和CUDA版本匹配的Tesla驱动，免去用户单独安装Tesla驱动的步骤。但是对NVIDIA驱动版本有强制要求或依赖时，请务必先单独从NVIDIA官网下载并安装匹配的Tesla驱动，然后再安装CUDA工具包。
- 如果云服务器已经安装了Tesla驱动，请检查当前驱动版本是否可用。如需安装新版本的驱动请卸载旧版本的Tesla驱动，避免因驱动程序冲突导致安装失败。
- 如果NVIDIA驱动版本与云服务器不兼容，会导致安装完成后驱动不显示，请参考[T4 GPU设备显示异常](#)进行处理。

安装指引：

- [Tesla驱动及CUDA工具包获取方式](#)
- 安装NVIDIA驱动
 - [Linux操作系统云服务器安装Tesla驱动](#)
 - [Windows操作系统云服务器安装Tesla驱动](#)
- 安装CUDA驱动
 - [Linux操作系统安装CUDA工具包](#)
 - [Windows操作系统安装CUDA工具包](#)

Linux 操作系统云服务器安装 Tesla 驱动

以下操作以Ubuntu 20.04 64bit操作系统，GPU实例安装CUDA 10.1对应的Tesla驱动为例。

📖 说明

Linux内核版本和驱动的版本存在兼容性关系。如果驱动安装失败，请检查驱动安装日志(安装日志通常位于/var/log/nvidia-installer.log)。日志中如提示失败原因为驱动编译错误，例如get_user_pages参数不匹配，说明当前内核版本与驱动版本不兼容，请选择合适的内核版本和驱动版本重新安装。建议内核版本与驱动版本发布时间不要相差过大。

1. 登录云服务器。
2. 根据操作系统选择命令更新系统软件。
 - Ubuntu
更新软件安装源：`apt-get -y update`
安装必要程序：`apt-get install gcc g++ make`
 - CentOS
更新软件安装源：`yum -y update --exclude=kernel* --exclude=centos-release* --exclude=initscripts*`

- 安装必要程序：`yum install -y kernel-devel-`uname -r` gcc gcc-c++`
3. 下载NVIDIA驱动包。
单击[NVIDIA驱动下载](#)根据实例的类型，选择驱动。

图 2-117 选择 NVIDIA 驱动

Manual Driver Search

Search by product, product type or series

Data Center / Tesla

T-Series

Tesla T4

Linux 64-bit

11.6

English (US)

Find

4. 根据需求选择驱动版本，以下操作以选择Tesla 418.67为例。

图 2-118 选择驱动版本

Tesla Driver for Linux x64					View
Driver Version: 418.67	CUDA Toolkit: 10.1	Release Date: Tue May 07, 2019	File Size: 107.23 MB	Info: 	

5. 单击需要下载的驱动右侧的“View”，进入对应下载界面。
6. 右键单击“Download”，复制下载的连接地址。
7. 在云服务器内部执行如下命令进行下载。

wget 复制的连接地址

例如：`wget http://us.download.nvidia.com/tesla/418.67/NVIDIA-Linux-x86_64-418.67.run`

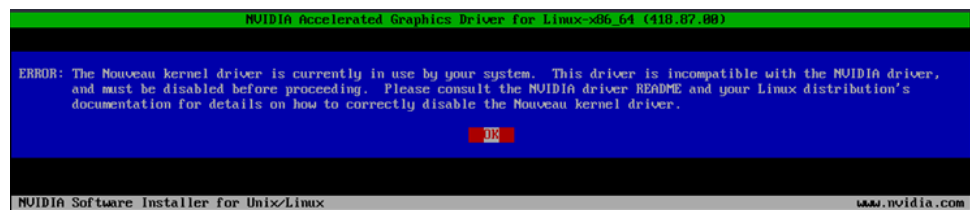
图 2-119 获取安装包

```
root@ecs-474b:~# wget http://us.download.nvidia.com/tesla/418.67/NVIDIA-Linux-x86_64-418.67.run
--2020-03-26 17:59:31-- http://us.download.nvidia.com/tesla/418.67/NVIDIA-Linux-x86_64-418.67.run
Resolving us.download.nvidia.com (us.download.nvidia.com)... 129.227.66.140, 129.227.66.139
Connecting to us.download.nvidia.com (us.download.nvidia.com)|129.227.66.140:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://us.download.nvidia.cn/tesla/418.67/NVIDIA-Linux-x86_64-418.67.run [following]
--2020-03-26 17:59:34-- https://us.download.nvidia.cn/tesla/418.67/NVIDIA-Linux-x86_64-418.67.run
Resolving us.download.nvidia.cn (us.download.nvidia.cn)... 60.222.11.61, 60.222.11.11, 123.134.184.166, ...
Connecting to us.download.nvidia.cn (us.download.nvidia.cn)|60.222.11.61:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 107232512 (102M) [application/octet-stream]
Saving to: 'NVIDIA-Linux-x86_64-418.67.run'

NVIDIA-Linux-x86_64-418.67.run 100%[=====] 102.26M 1.07MB/s in 5m 2s
2020-03-26 18:04:40 (346 KB/s) - 'NVIDIA-Linux-x86_64-418.67.run' saved [107232512/107232512]
```

8. 执行以下命令安装驱动。
sh NVIDIA-Linux-x86_64-418.67.run
9. （可选）如果执行驱动安装命令后出现如下提示信息，需要禁用nouveau驱动。

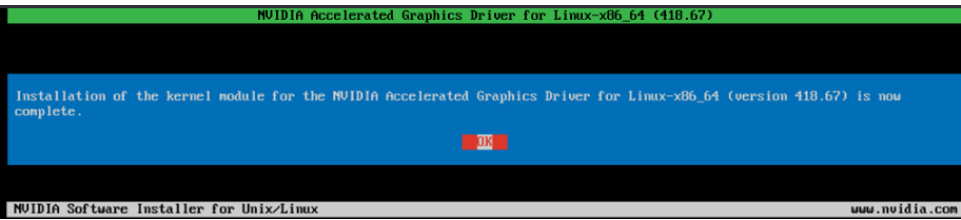
图 2-120 禁用 nouveau 驱动



- a. 执行以下命令，查看是否安装Nouveau驱动。
lsmod | grep nouveau
 - 如果回显信息中包含Nouveau驱动信息，说明Nouveau驱动已安装，则需要禁用Nouveau驱动，请执行步骤9.b。
 - 如果回显信息没有Nouveau驱动信息，说明Nouveau驱动已被禁用，请执行步骤10。
 - b. 执行如下命令编辑blacklist.conf文件。
如果没有“/etc/modprobe.d/blacklist.conf”文件，请新建一个。
vi /etc/modprobe.d/blacklist.conf
添加如下语句添加至文件结尾。

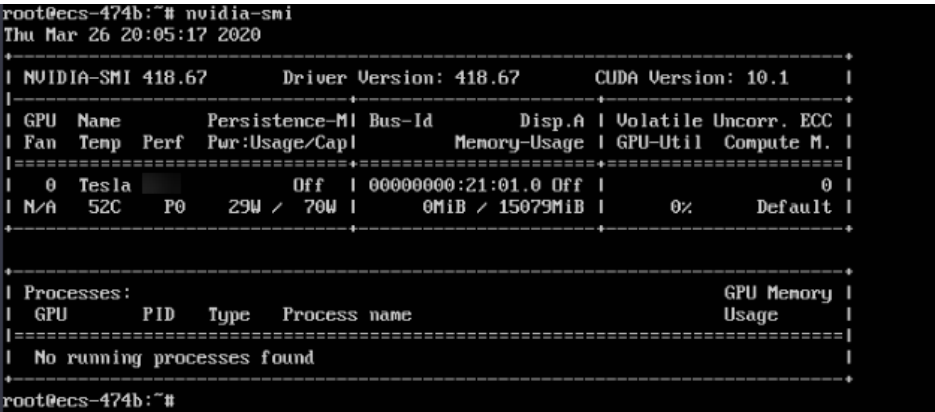
```
blacklist nouveau
options nouveau modeset=0
```
 - c. 执行以下命令，备份并新建一个initramfs。
 - Ubuntu系统：
sudo update-initramfs -u
 - CentOS系统：
mv /boot/initramfs-\$(uname -r).img /boot/initramfs-\$(uname -r).img.bak
dracut -v /boot/initramfs-\$(uname -r).img \$(uname -r)
 - d. 执行以下命令，重启云服务器。
reboot
10. 根据安装提示，连续三次选择“OK”。完成驱动的安装。

图 2-121 NVIDIA 驱动安装完成



- 11. 执行命令设置systemd。
systemctl set-default multi-user.target
- 12. 执行**reboot**，重启云服务器。
- 13. 登录云服务器，执行**nvidia-smi**，如果回显信息中包含了已安装的驱动版本，说明驱动安装成功。

图 2-122 查看 NVIDIA 驱动的版本



Windows 操作系统云服务器安装 Tesla 驱动

以下操作以Windows Server 2016 Standard 64bit操作系统，GPU实例安装Tesla驱动为例。

- 1. 登录云服务器。
- 2. 下载NVIDIA驱动包。
单击[NVIDIA驱动下载](#)根据实例的类型，选择驱动版本。

图 2-123 选择驱动类型（Windows）

Manual Driver Search

Search by product, product type or series

Q

Data Center / Tesla

▼

i

T-Series

▼

Tesla T4

▼

Windows Server 2016

▼

10.1

▼

English (US)

▼

Find

3. 根据需求选择驱动版本，本节操作以安装Tesla 425.25为例。

图 2-124 选择驱动版本（Windows）

Tesla Driver for Windows

Driver Version:	CUDA Toolkit:	Release Date:	File Size:	Info:	View
425.25	10.1	Tue May 07, 2019	417.62 MB	Production Branch WHQL	

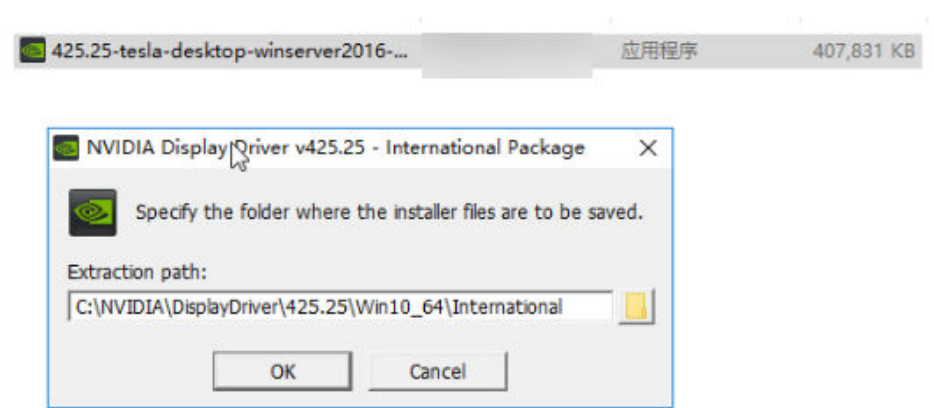
4. 单击需要下载的驱动，进入对应下载界面。
5. 单击“Download”，下载安装包。
6. 双击驱动安装驱动，单击“运行”。

图 2-125 运行 NVIDIA 驱动安装程序



7. 选择安装路径，单击“OK”。

图 2-126 选择 NVIDIA 驱动安装路径



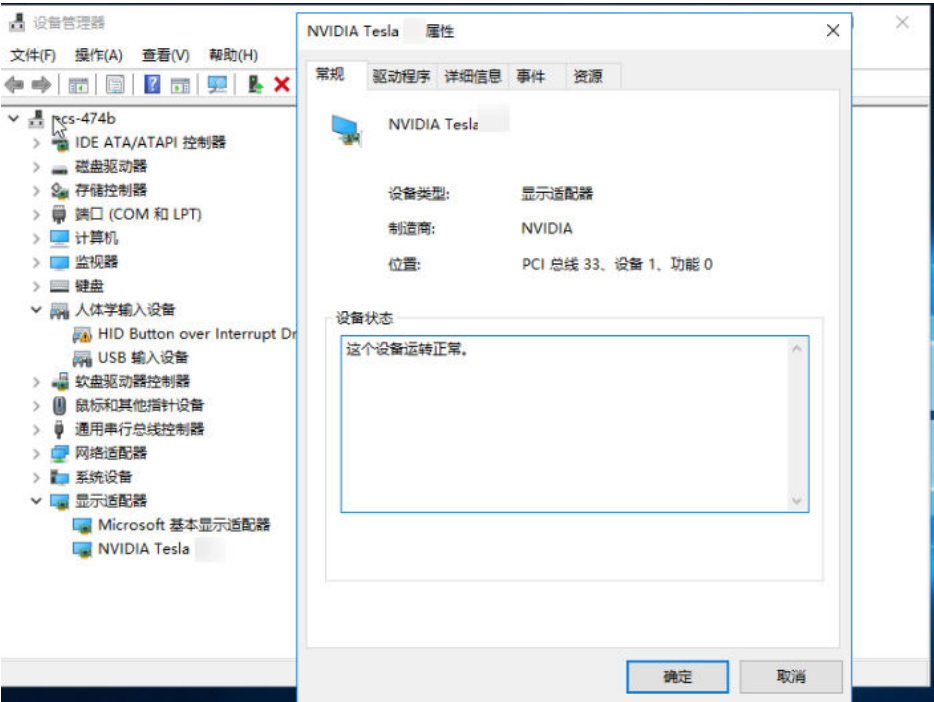
8. 根据安装提示完成NVIDIA程序的安装。

图 2-127 完成 NVIDIA 驱动的安装



- 9. 重启云服务器。
- 10. 检查驱动是否安装成功。
 - a. 进入“设备管理器”，查看“显示适配器”。

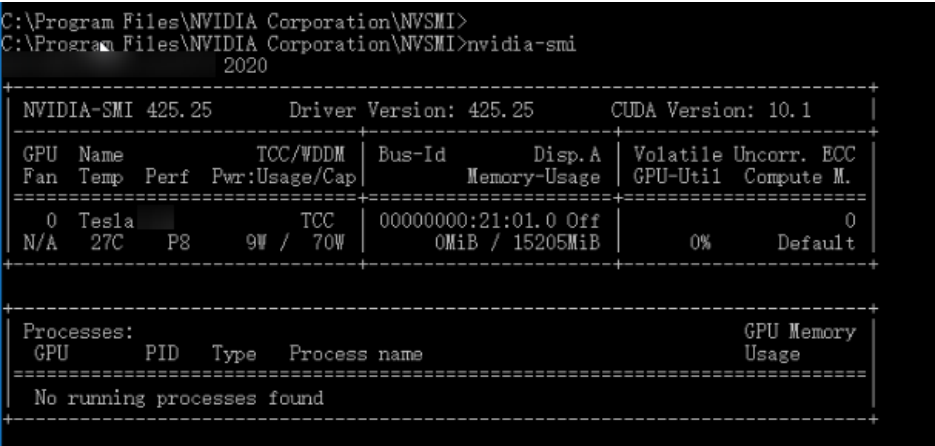
图 2-128 显示适配器



- b. 打开云服务器cmd窗口，执行以下命令：
cd C:\Program Files\NVIDIA Corporation\NVSMI

nvidia-smi
如果回显信息中包含了已安装的驱动版本，说明驱动安装成功。

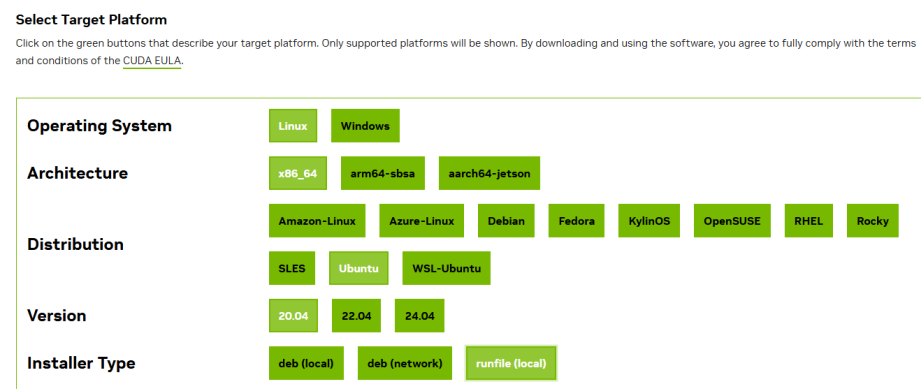
图 2-129 查看 NVIDIA 驱动安装版本



Linux 操作系统安装 CUDA 工具包

- 以下操作以Ubuntu 20.04 64bit操作系统，GPU实例使用run包安装CUDA 10.1为例。
- 1. 登录云服务器。
 - 2. 根据操作系统选择命令更新系统软件。
 - Ubuntu
更新软件安装源：**apt-get -y update**
安装必要程序：**apt-get install gcc g++ make**
 - CentOS
更新软件安装源：**yum -y update --exclude=kernel* --exclude=centos-release* --exclude=initscripts***
安装必要程序：**yum install -y kernel-devel`uname -r` gcc gcc-c++**
 - 3. 在CUDA下载页面中，按照[Tesla驱动及CUDA工具包获取方式](#)中的对应的索引项在页面中进行选择。

图 2-130 选择 CUDA 的版本



- 4. 选择完成后，页面会自动呈现出Ubuntu 20.04 64bit对应的CUDA 10.1的下载地址，复制下载地址。

5. 在云服务器内部执行如下命令进行下载。
wget 复制的链接地址
例如：**wget https://developer.nvidia.com/compute/cuda/10.1/Prod/local_installers/cuda_10.1.105_418.39_linux.run**

图 2-131 Linux 云服务器下载 CUDA

```
root@ecs-474b:~# wget https://developer.nvidia.com/compute/cuda/10.1/Prod/local_installers/cuda_10.1.105_418.39_linux.run
-- https://developer.nvidia.com/compute/cuda/10.1/Prod/local_installers/cuda_10.1.105_418.39_linux.run
Resolving developer.nvidia.com (developer.nvidia.com)... 129.227.66.139, 129.227.66.140
Connecting to developer.nvidia.com (developer.nvidia.com)|129.227.66.139|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://developer.download.nvidia.com/compute/cuda/10.1/secure/Prod/local_installers/cuda_10.1.105_418.39_linux.run?FFJqELqU0U0EH-9_YUp4zpYc3t1j8q9J5clzHL2kX5Uo-f721Gy8tP3hm2JdJ2QntuMtpR-7nmp4Eb6Qjd7YB4BhuW56Di4V3prth0y22SX6Xugu950k94i6Sb9he5n1SJHhbPXUgVLzUhhijXhuBUCkMBMsuvm4X_uk_k2AY1oWbtU7D2sMaF8oU8 [following]
-- https://developer.download.nvidia.com/compute/cuda/10.1/secure/Prod/local_installers/cuda_10.1.105_418.39_linux.run?FFJqELqU0U0EH-9_YUp4zpYc3t1j8q9J5clzHL2kX5Uo-f721Gy8tP3hm2JdJ2QntuMtpR-7nmp4Eb6Qjd7YB4BhuW56Di4V3prth0y22SX6Xugu950k94i6Sb9he5n1SJHhbPXUgVLzUhhijXhuBUCkMBMsuvm4X_uk_k2AY1oWbtU7D2sMaF8oU8
Resolving developer.download.nvidia.com (developer.download.nvidia.com)... 129.227.66.139, 129.227.66.140
Connecting to developer.download.nvidia.com (developer.download.nvidia.com)|129.227.66.139|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://developer.download.nvidia.cn/compute/cuda/10.1/secure/Prod/local_installers/cuda_10.1.105_418.39_linux.run?FFJqELqU0U0EH-9_YUp4zpYc3t1j8q9J5clzHL2kX5Uo-f721Gy8tP3hm2JdJ2QntuMtpR-7nmp4Eb6Qjd7YB4BhuW56Di4V3prth0y22SX6Xugu950k94i6Sb9he5n1SJHhbPXUgVLzUhhijXhuBUCkMBMsuvm4X_uk_k2AY1oWbtU7D2sMaF8oU8 [following]
-- https://developer.download.nvidia.cn/compute/cuda/10.1/secure/Prod/local_installers/cuda_10.1.105_418.39_linux.run?FFJqELqU0U0EH-9_YUp4zpYc3t1j8q9J5clzHL2kX5Uo-f721Gy8tP3hm2JdJ2QntuMtpR-7nmp4Eb6Qjd7YB4BhuW56Di4V3prth0y22SX6Xugu950k94i6Sb9he5n1SJHhbPXUgVLzUhhijXhuBUCkMBMsuvm4X_uk_k2AY1oWbtU7D2sMaF8oU8
Resolving developer.download.nvidia.cn (developer.download.nvidia.cn)... 60.222.11.61, 60.222.11.10, 123.134.184.165, ...
Connecting to developer.download.nvidia.cn (developer.download.nvidia.cn)|60.222.11.61|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 242314285 (2.3G) [application/octet-stream]
Saving to: 'cuda_10.1.105_418.39_linux.run'

cuda_10.1.105_418.39_linux.run 100%[=====] 2.26G 34.2MB/s in 74s
```

6. CUDA工具包下载完成后，按照NVIDIA官网安装指引进行安装。
按照NVIDIA官网的Installation Instructions进行安装。
7. 执行以下命令安装CUDA。
sh cuda_10.1.243_418.87.00_linux.run
8. 在安装界面输入“accept”，回车进入下一步。

图 2-132 安装 CUDA_1

```
End User License Agreement
-----

Preface
-----

The Software License Agreement in Chapter 1 and the Supplement
in Chapter 2 contain license terms and conditions that govern
the use of NVIDIA software. By accepting this agreement, you
agree to comply with all the terms and conditions applicable
to the product(s) included herein.

NVIDIA Driver

Description

This package contains the operating system driver and

Do you accept the above EULA? (accept/decline/quit):
accept
```

9. 选择“Install”，回车进入安装过程。

图 2-133 安装 CUDA_2

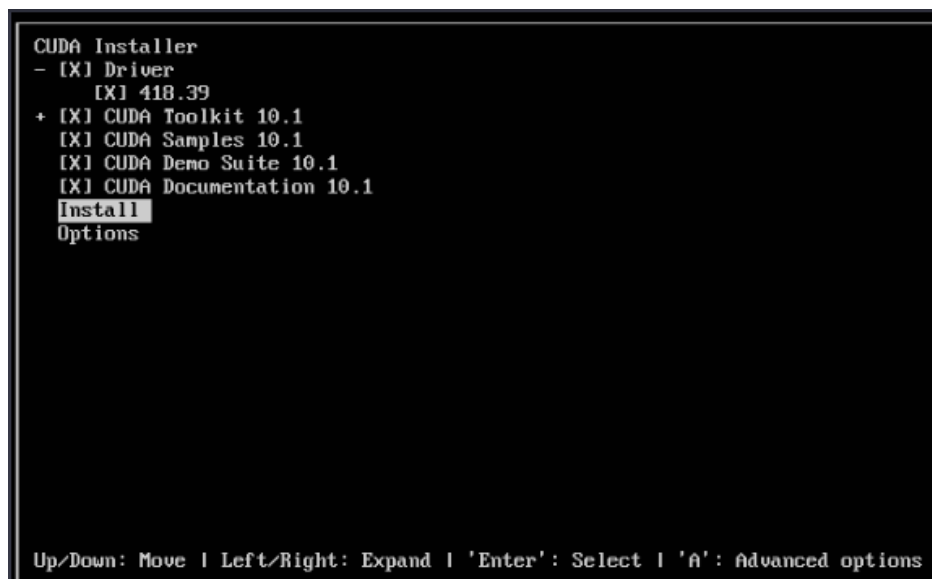
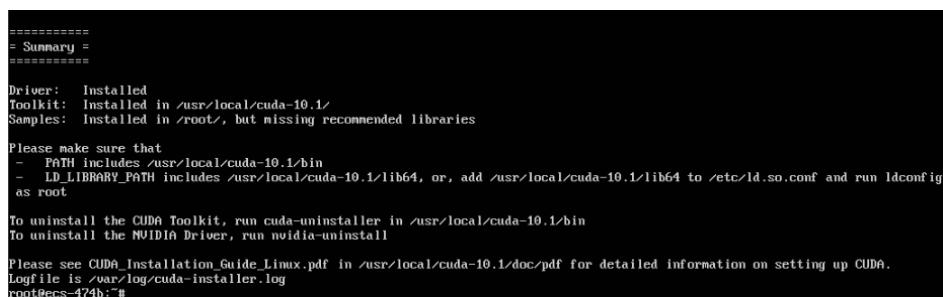


图 2-134 安装 CUDA 完成



10. （可选）检查CUDA是否安装成功。

如果您安装的CUDA版本为11.5及以前，可参考如下操作查看CUDA是否安装成功。如果CUDA版本为11.6及以后，可跳过该步骤。

- 执行以下命令进入/usr/local/cuda-10.1/samples/1_Uutilities/deviceQuery目录下。

```
cd /usr/local/cuda-10.1/samples/1_Uutilities/deviceQuery
```

- 执行make命令，自动编译deviceQuery程序。
- 执行以下命令查看CUDA是否安装成功。

```
./deviceQuery
```

如回显信息中有CUDA的版本信息证明CUDA安装成功。

图 2-135 deviceQuery 回显信息

```
root@ecs-474b:/usr/local/cuda-10.1/samples/1_Utilities/deviceQuery# ./deviceQuery
./deviceQuery Starting...

CUDA Device Query (Runtime API) version (CUDA RT static linking)
Detected 1 CUDA Capable device(s)

Device 0: "Tesla M40"
  CUDA Driver Version / Runtime Version      10.1 / 10.1
  CUDA Capability Major/Minor version number: 7.5
  Total amount of global memory:              15080 MBytes (15812263936 bytes)
  (40) Multiprocessors, ( 64) CUDA Cores/MP: 2560 CUDA Cores
  GPU Max Clock rate:                        1590 MHz (1.59 GHz)
  Memory Clock rate:                         5001 Mhz
  Memory Bus Width:                          256-bit
  L2 Cache Size:                             4194304 bytes
  Maximum Texture Dimension Size (x,y,z)     1D=(131072), 2D=(131072, 65536), 3D=(16384, 16384, 16384)
  Maximum Layered 1D Texture Size, (num) layers 1D=(32768), 2048 layers
  Maximum Layered 2D Texture Size, (num) layers 2D=(32768, 32768), 2048 layers
  Total amount of constant memory:            65536 bytes
  Total amount of shared memory per block:    49152 bytes
  Total number of registers available per block: 65536
  Warp size:                                  32
  Maximum number of threads per multiprocessor: 1024
  Maximum number of threads per block:        1024
  Max dimension size of a thread block (x,y,z): (1024, 1024, 64)
  Max dimension size of a grid size (x,y,z):  (2147483647, 65535, 65535)
  Maximum memory pitch:                       2147483647 bytes
  Texture alignment:                           512 bytes
  Concurrent copy and kernel execution:       Yes with 3 copy engine(s)
  Run time limit on kernels:                   No
  Integrated GPU sharing Host Memory:          No
  Support host page-locked memory mapping:    Yes
  Alignment requirement for Surfaces:         Yes
  Device has ECC support:                     Enabled
  Device supports Unified Addressing (UVA):    Yes
  Device supports Compute Preemption:         Yes
  Supports Cooperative Kernel Launch:         Yes
  Supports MultiDevice Co-op Kernel Launch:   Yes
  Device PCI Domain ID / Bus ID / location ID: 0 / 33 / 1
  Compute Mode:
    < Default (multiple host threads can use ::cudaSetDevice() with device simultaneously) >

deviceQuery, CUDA Driver = CUDART, CUDA Driver Version = 10.1, CUDA Runtime Version = 10.1, NumDevs = 1
Result = PASS
root@ecs-474b:/usr/local/cuda-10.1/samples/1_Utilities/deviceQuery#
```

11. 执行以下命令查看CUDA的版本。
`/usr/local/cuda/bin/nvcc -V`

图 2-136 查看 CUDA 的版本

```
root@ecs-474b:/usr/local/cuda-10.1/samples/1_Utilities/deviceQuery# /usr/local/cuda/bin/nvcc -V
nvcc: NVIDIA (R) Cuda compiler driver
Copyright (c) 2005-2019 NVIDIA Corporation
Built on Fri_Feb__8_19:08:17_PST_2019
Cuda compilation tools, release 10.1, V10.1.105
root@ecs-474b:/usr/local/cuda-10.1/samples/1_Utilities/deviceQuery#
```

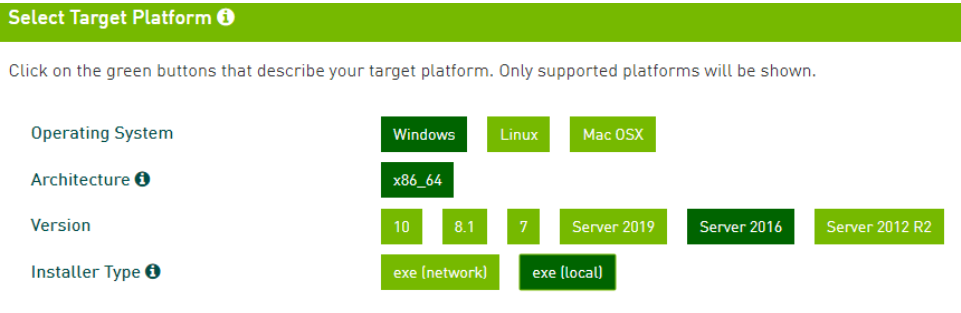
12. 执行以下命令启动持久模式。
`sudo nvidia-smi -pm 1`
启用持久模式设置可以优化Linux实例上GPU设备的性能。

Windows 操作系统安装 CUDA 工具包

以下操作以Windows Server 2016 Standard 64bit操作系统GPU实例安装CUDA 10.1为例。

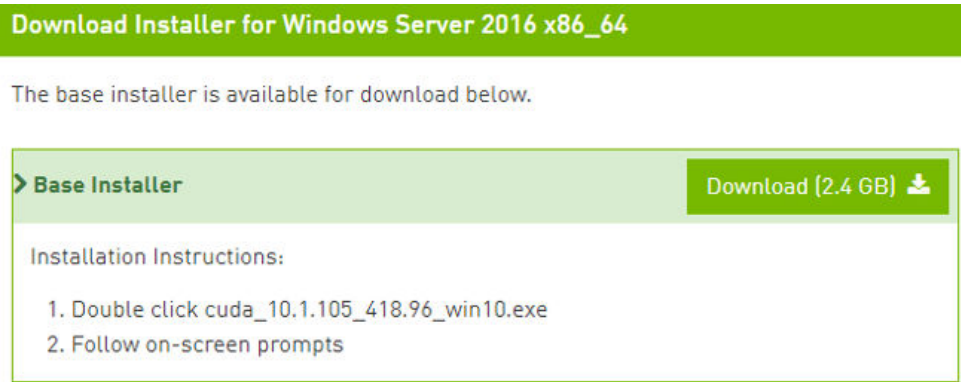
- 1. 登录云服务器。
- 2. 在CUDA下载页面中，按照[CUDA工具包下载地址](#)中的对应的索引项在页面中进行选择。

图 2-137 选择 CUDA 版本



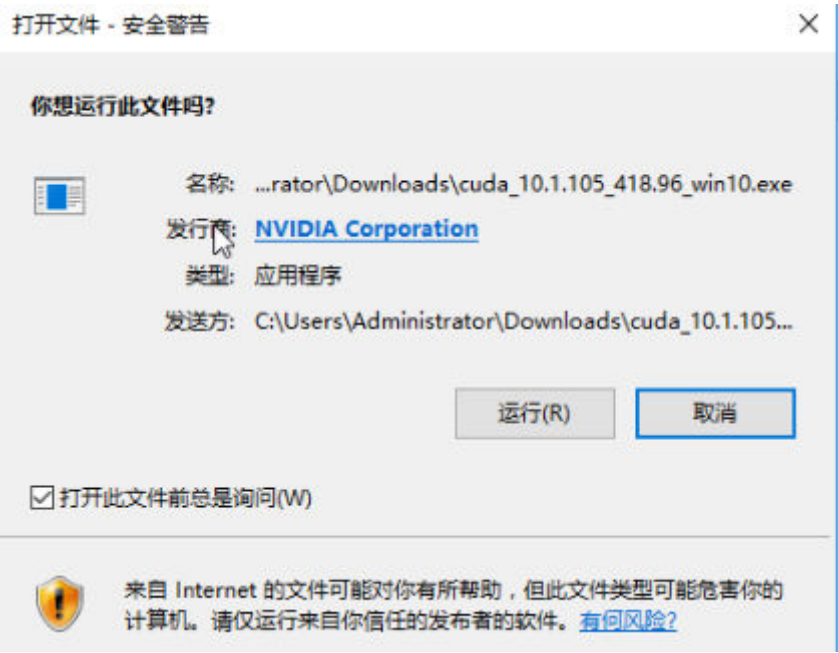
3. 选择完成后，页面会自动呈现出Windows Server 2016 Standard 64bit对应的CUDA 10.1的下载地址。

图 2-138 Windows 云服务器下载 CUDA



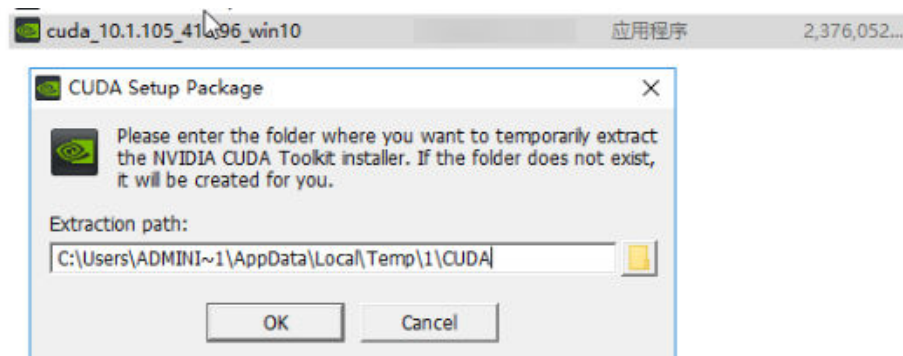
4. 单击“Download”下载CUDA工具包。
5. 双击打开安装文件，单击“运行”安装CUDA工具包。

图 2-139 Windows 云服务器安装 CUDA



6. 选择安装地址，在“CUDA Setup Package”界面，单击“OK”

图 2-140 选择 CUDA 安装路径



7. 根据安装提示完成CUDA的安装。

图 2-141 CUDA 安装完成



8. 检查CUDA是否安装成功。
打开cmd命令窗口，执行以下命令。
nvcc -V
如果回显信息中出现CUDA的版本信息，说明CUDA安装成功。

图 2-142 CUDA 安装成功

```
C:\Users\Administrator>nvcc -V
nvcc: NVIDIA (R) Cuda compiler driver
Copyright (c) 2005-2019 NVIDIA Corporation
Built on Fri_Feb__8_19:08:26_Pacific_Standard_Time_2019
Cuda compilation tools, release 10.1, V10.1.105

C:\Users\Administrator>
```

2.6.7 卸载 GPU 加速型 ECS 的 GPU 驱动

操作场景

当GPU加速型云服务器需手动卸载GPU驱动时，可参考本文档进行操作。

GPU驱动卸载命令与GPU驱动的安装方式和操作系统类型相关，例如：

- [Windows操作系统卸载驱动](#)
- [Linux操作系统卸载驱动](#)

Windows 操作系统卸载驱动

以Windows Server 2016 数据中心版 64位操作系统为例，介绍GPU加速型云服务器卸载NVIDIA驱动（驱动版本462.31）的操作步骤。

1. 登录弹性云服务器。
2. 单击“开始”，打开“控制面板”。
3. 在控制面板中，单击“卸载程序”。

图 2-143 单击卸载程序



4. 右键单击要卸载的NVIDIA驱动，单击“卸载/更改”。

图 2-144 卸载驱动



5. 在弹出的“NVIDIA 卸载程序”界面，单击“卸载”。

图 2-145 NVDIA 卸载程序



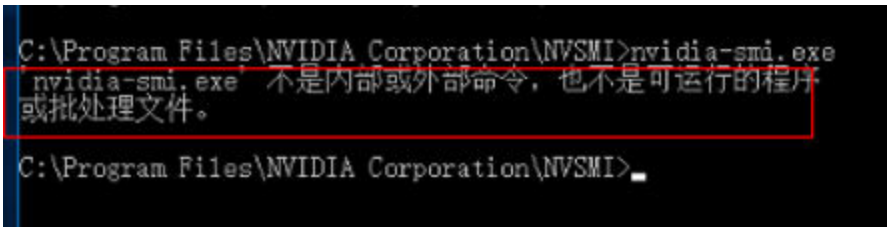
6. 卸载完成后，单击“稍后启动”。
7. 检查驱动是否卸载成功。
- a. 在控制面板，单击“设备管理器”。
- 如果“显示适配器”中没有NVIDIA显卡，表明驱动卸载成功。

图 2-146 查看显示适配器



- b. 打开云服务器cmd窗口，执行以下命令：
- ```
cd C:\Program Files\NVIDIA Corporation\NVSMI
nvidia-smi.exe
```

图 2-147 命令执行结果



如果回显信息为该文件不存在，则说明驱动卸载成功。

确认NVIDIA驱动卸载完成后，可以先不重启云服务器，直接安装新的NVIDIA驱动。

Linux 操作系统卸载驱动

对于使用run安装包安装的NVIDIA Tesla驱动，建议您按照以下步骤卸载NVIDIA Tesla驱动。

**说明**

如果您使用run安装包安装NVIDIA Grid驱动，则卸载NVIDIA驱动即可，只需执行下面的步骤1。

以Ubuntu20.04 server 64bit为例，介绍Tesla 460.73.01、CUDA 11.2卸载的操作步骤。

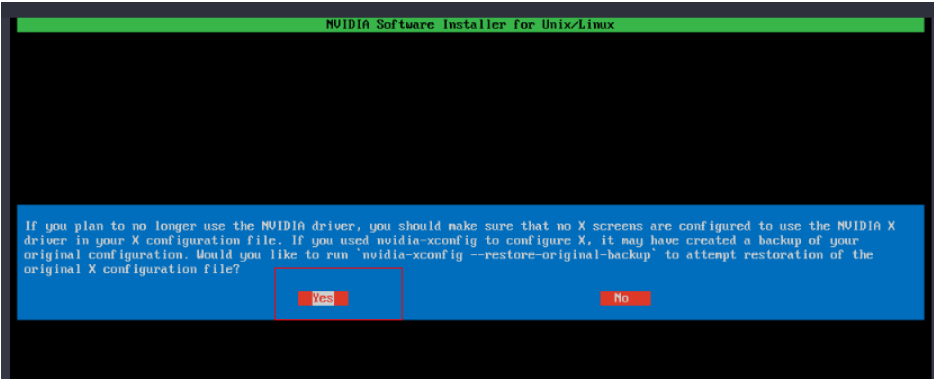
1. 卸载NVIDIA驱动。
- a. 执行以下命令，查询“nvidia-uninstall”所在路径。  
**whereis nvidia-uninstall**  
“nvidia-uninstall”一般在“/usr/bin/”目录下。

图 2-148 查询卸载路径



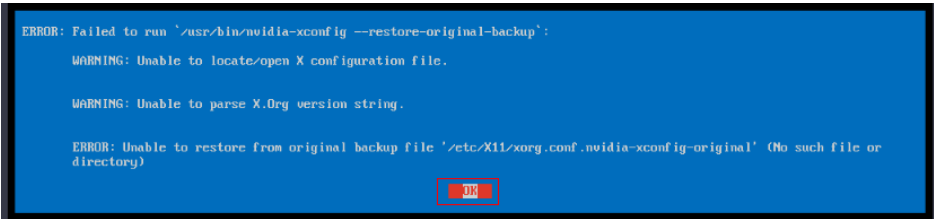
- b. 执行以下命令，基于查询的“nvidia-uninstall”路径，卸载驱动。  
**/usr/bin/nvidia-uninstall**
- c. 选择” Yes” ，单击回车键。

图 2-149 卸载驱动选择界面



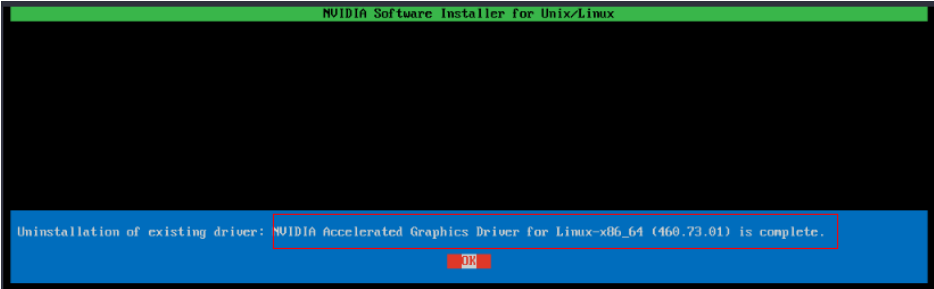
- d. 选择” OK” ，单击回车键。

图 2-150 卸载过程选择界面



- e. 驱动卸载成功，单击回车键。

图 2-151 卸载成功界面



2. 卸载CUDA库和cuDNN库

当需要升级CUDA驱动版本时，需要卸载对应的CUDA库后，再安装对应的CUDA版本。

- a. 执行以下命令，卸载CUDA库。

```
/usr/local/cuda/bin/cuda-uninstaller
```

“cuda-uninstaller”一般在“/usr/local/cuda/bin”目录下。

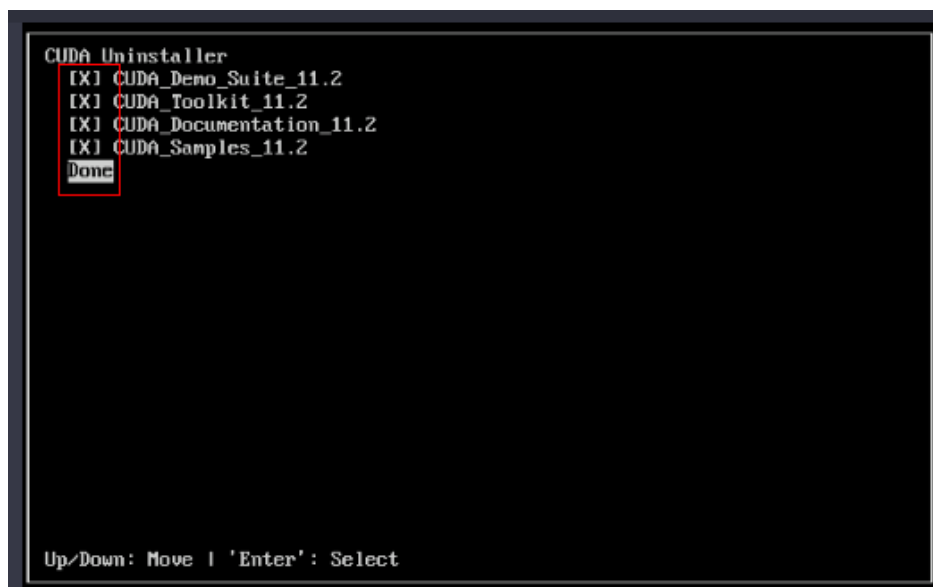
#### 说明

不同CUDA版本的卸载命令可能存在差异，如果未找到“cuda-uninstaller”文件，可在“/usr/local/cuda/bin/”目录下查看是否存在“uninstall\_cuda”开头的文件。

如果有，则将命令中的“cuda-uninstaller”替换为“uninstall\_cuda”开头的文件名。

- b. 在卸载界面，勾选全部选项后，移动光标至“Done”，单击回车键。

图 2-152 卸载 CUDA 驱动



CUDA库卸载成功，会返回”Successfully uninstalled”。

- c. 移除CUDA库和cuDNN库：

```
rm -rf /usr/local/cuda-11.2
```

## 2.7 管理 ECS 配置信息

### 2.7.1 更改时区

#### 操作场景

弹性云服务器默认设置的时区，是您制作镜像时选择的时区。对于使用公共镜像创建的弹性云服务器，无论所在区域，默认时区均为东八区。如需修改，请参见本节内容，将其更改为所需的本地时间或网络中的其他时区。

弹性云服务器登录成功后，如果发现弹性云服务器系统时间与本地时间不一致，建议更改时区，将弹性云服务器系统时间与本地时间进行同步。



## 更改 Linux 弹性服务器的时区

针对不同的Linux操作系统，更改时区的操作略有不同。本节以CentOS 6.x 64bit为例，介绍更改Linux弹性云服务器时区的操作方法。

1. 登录弹性云服务器。
2. 执行以下命令，切换至root账号。

```
su - root
```

3. 执行以下命令，查询支持使用的时区。

```
ls /usr/share/zoneinfo/
```

其中，“/usr/share/zoneinfo”目录显示了时区数据文件的目录结构。您可以通过该目录结构，查找您所需时区的文件。

“/usr/share/zoneinfo”目录中显示的信息，部分为时区，部分为目录。其中，目录包含了针对特定城市的时区文件，您可以在该目录查找要用于弹性云服务器的所在城市时区。

示例如下：

- 假设您需要使用中国上海所在的时区，则需先执行命令**ls /usr/share/zoneinfo/Asia**打开目录。  
其时区文件目录为“/usr/share/zoneinfo/Asia/Shanghai”
- 假设您需要使用法国巴黎所在的时区，则需先执行命令**ls /usr/share/zoneinfo/Europe**打开目录，其时区文件目录为“/usr/share/zoneinfo/Europe/Paris”。

4. 设置新时区。

- a. 执行以命令，打开“/etc/sysconfig/clock”文件。

```
vim /etc/sysconfig/clock
```

- b. 查找ZONE条目，将其更改为所需的时区文件名称。

示例如下：

- 假设更改为中国上海所在时区，需将ZONE条目更改为：  
ZONE="Asia/Shanghai"
- 假设更改为法国巴黎所在时区，需将ZONE条目更改为：  
ZONE="Europe/Paris"

5. 按“ESC”，执行以下命令，保存并退出文件。

```
:wq
```

6. 执行以下命令，查询弹性云服务器中是否已经存在“/etc/localtime”文件。

```
ls /etc/localtime
```

- 是，执行7。
- 否，跳转8。

7. 执行以下命令，删除已有的“/etc/localtime”文件。

```
rm /etc/localtime
```

8. 执行以下命令，在“/etc/localtime”与时区文件之间创建一个符号链接，使得弹性云服务器在引用本地时间信息时找到此时区文件。

```
ln -sf /usr/share/zoneinfo/Asia/city1 /etc/localtime
```

9. 执行以下命令，重启系统，使得所有服务和应用程序接受新时区信息。



### reboot

10. 重新登录弹性云服务器，使用root账号执行以下命令，查询弹性云服务器的时区，确认是否更改成功。

### ls -lh /etc/localtime

回显信息如下所示：

```
ls -lh /etc/localtime
lrwxrwxrwx 1 root root 33 Nov 27 11:01 /etc/localtime -> /usr/share/zoneinfo/Asia/city1
```

## 更改 Windows 弹性云服务器的时区

1. 登录弹性云服务器。
2. 左键单击任务栏右下方的时间，选择“更改日期和时间设置”。系统进入“日期和时间”页面

图 2-153 日期和时间



3. 单击“更改时区”。系统进入“时区设置”页面。
4. 在“设置时区”栏的下拉框中选择待更换的时区。
5. 单击“确定”，完成Windows弹性云服务器的时区更换。

## 2.7.2 开启/关闭 ECS 超线程

### 操作场景

购买x86架构弹性云服务器时，您可以通过设置“CPU选项”，开启或关闭超线程。若不设置，则默认开启超线程。

对于支持超线程的x86架构弹性云服务器实例：

- 开启超线程：适用于需要CPU内核在同一时间并行处理更多的信息和后台任务的场景，开启多线程可以大幅提升计算体验。
- 关闭超线程：适用于计算密集型，且关闭超线程时性能优于开启超线程的场景，例如材料计算等HPC场景。

您可以在购买x86架构弹性云服务器或变更规格时，开启或关闭超线程。

### 背景知识

x86架构弹性云服务器的处理器运用超线程HT（Hyper-Threading）技术，允许在CPU的每个物理内核上公开两个执行上下文，即一个物理内核包含两个虚拟的“逻辑内核”，可以处理不同的软件线程。vCPU（virtual CPU）即为虚拟的“逻辑内核”。

规格名称展示vCPU数，即逻辑内核数。在x86架构弹性云服务器上可以查看实际的CPU逻辑内核数。查看方法，请参见[查看ECS实际的CPU逻辑内核数](#)。

当前绝大多数x86架构规格已经默认开启了超线程，如果在创建x86架构弹性云服务器或者变更规格时关闭了超线程，则在弹性云服务器上查看到的CPU核数是规格的Flavor名称中展示的vCPU数量的一半。

例如，对于c7.xlarge.2，其vCPU数，即逻辑内核数为4，4个逻辑内核对应了底层4个HT（超线程）。若关闭了超线程，则c7.xlarge.2的vCPU数，即逻辑内核数为2，2个逻辑内核对应了底层2个物理核。

### 约束与限制

- x86弹性云服务器购买完成后无法修改超线程状态，需要通过变更规格的方式修改ECS实例的超线程状态。
- 该操作不涉及收费。
- 支持开启或关闭超线程的规格，请参见[规格清单（X86）](#)。

### 开启/关闭超线程（购买时）

1. 登录控制台，进入[购买弹性云服务器](#)页面。  
根据业务需要，完成基础配置、网络配置以及高级配置。详细内容，请参见[购买弹性云服务器](#)。
2. 勾选“现在配置”，展开“高级选项”。
3. 勾选“指定CPU选项”。

图 2-154 设置 CPU 选项



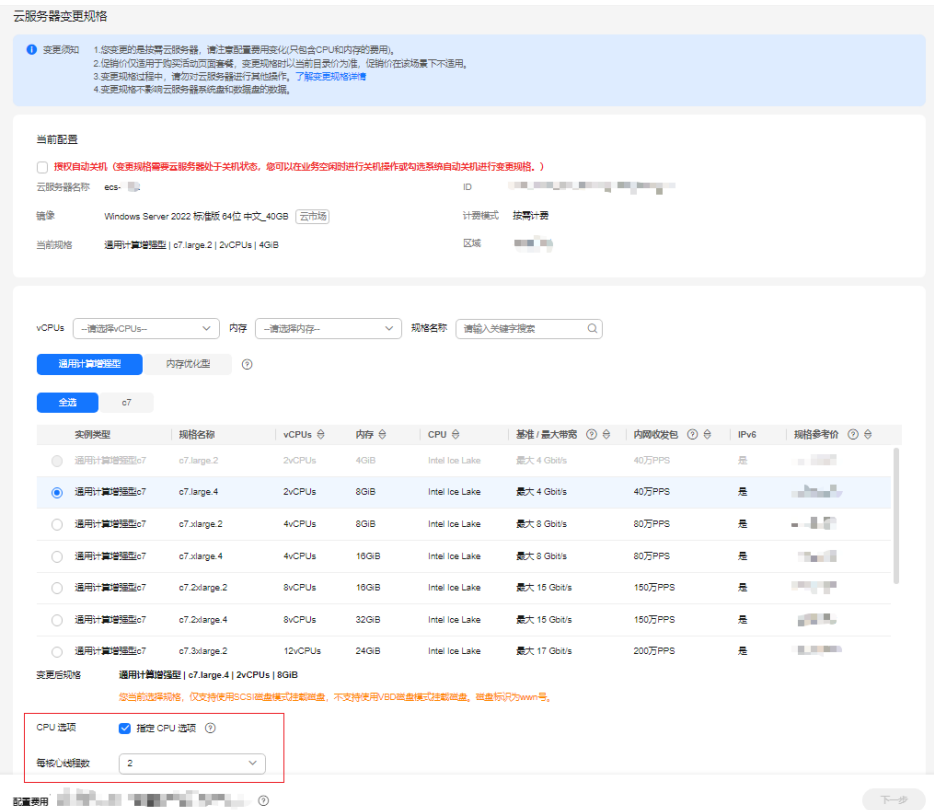
4. 设置“每核心线程数”。
- 当勾选“指定CPU选项”时，显示该参数。在“每核心线程数”下拉框进行设置。
- 1：关闭超线程

– 2：开启超线程，默认开启
5. 单击“下一步：确认配置”，确认参数并完成弹性云服务器的购买。
- 购买后，您可以通过[查询云服务器详情](#)中的“cpu\_options”参数查询超线程状态。

开启/关闭超线程（变更规格时）

1. 登录管理控制台。
2. 单击管理控制台左上角的，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”。
4. 在弹性云服务器列表，单击待变更的弹性云服务器“操作”列下的“更多 > 变更规格”。
- 系统进入“云服务器变更规格”页面。
5. 根据界面提示，选择变更后的弹性云服务器类型、vCPU和内存。
- 变更规格前请先将云服务器关机，或根据页面提示勾选“授权自动关机”。

图 2-155 变更规格



6. （可选）勾选“指定CPU选项”。
- 当需要为云服务器实例开启或关闭超线程时，勾选“指定CPU选项”。

7. （可选）设置“每核心线程数”。  
当勾选“指定CPU选项”时，显示该参数。在“每核心线程数”下拉框进行设置。
  - 1：关闭超线程
  - 2：开启超线程，默认开启
8. 单击“下一步”。
9. 确认变更后的配置无误后，阅读并勾选同意服务协议，单击“提交申请”开始变更。  
变更完成后，您可以通过[查询云服务器详情](#)中的“cpu\_options”参数查询超线程状态。

## 查看 ECS 实际的 CPU 逻辑内核数

您可以登录ECS后，在ECS上查看实际的CPU逻辑内核数。

- 对于Linux系统ECS
  - a. [登录ECS](#)。
  - b. 执行以下命令，查询ECS的CPU逻辑内核数。

**lscpu**

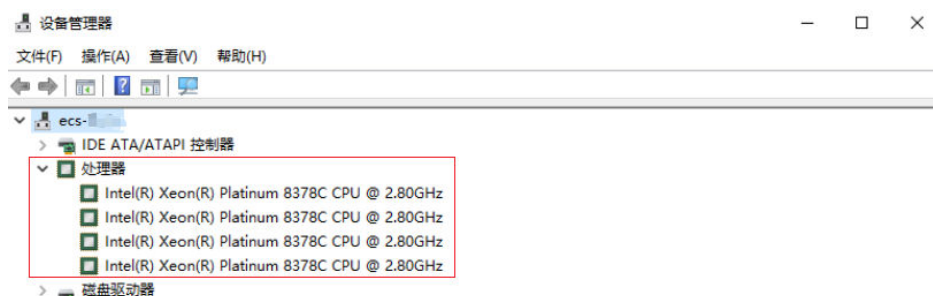
如图2-156所示，“CPU(s)”表示CPU逻辑内核数。

图 2-156 查询结果

```
[root@ecs-~]# lscpu
Architecture: x86_64
CPU op-mode(s): 32-bit, 64-bit
Byte Order: Little Endian
CPU(s): 4
On-line CPU(s) list: 0-3
Thread(s) per core: 2
Core(s) per socket: 2
Socket(s): 1
NUMA node(s): 1
Vendor ID: GenuineIntel
```

- 对于Windows系统ECS
  - a. [登录ECS](#)。
  - b. 打开“控制面板 > 设备管理器”，展开“处理器”，即可查看当前ECS实际的CPU逻辑内核数（线程）。

图 2-157 查询结果



## 2.7.3 使用实例自定义数据和元数据

### 2.7.3.1 通过元数据获取 ECS 基本信息

#### 操作场景

弹性云服务器元数据包含了弹性云服务器在云平台的基本信息，例如云服务ID、主机名、网络信息等。弹性云服务器元数据支持两种风格，可以分别通过兼容Openstack和兼容EC2的API获取，如表2-46所示。对于支持的元数据类型，本节详细介绍了其URI和使用方法。

#### 使用须知

如果元数据中包含了敏感数据，您应当采取适当的措施来保护敏感数据，比如限制访问范围、加密等。

防火墙配置示例如下所示：

- Windows  
如果您不希望管理员之外的用户访问实例自定义数据，请以管理员身份开启防火墙后，在PowerShell 中执行下面的命令，阻止非管理员用户访问实例自定义数据：  

```
PS C:\>$RejectPrincipal = New-Object -TypeName System.Security.Principal.NTAccount ("Everyone")
PS C:\>$RejectPrincipalSID = $RejectPrincipal.Translate([System.Security.Principal.SecurityIdentifier]).Value
PS C:\>$ExceptPrincipal = New-Object -TypeName System.Security.Principal.NTAccount ("Administrator")
PS C:\>$ExceptPrincipalSID = $ExceptPrincipal.Translate([System.Security.Principal.SecurityIdentifier]).Value
PS C:\>$PrincipalSDDL = "O:LSD:(D;;CC;;;$ExceptPrincipalSID)(A;;CC;;;$RejectPrincipalSID)"
PS C:\>New-NetFirewallRule -DisplayName "Reject metadata service for $($RejectPrincipal.Value), exception: $($ExceptPrincipal.Value)" -Action block -Direction out -Protocol TCP -RemoteAddress 169.254.169.254 -LocalUser $PrincipalSDDL
```
- Linux  
如果您不希望root之外的用户访问自定义实例自定义数据，请以root用户权限执行下面的命令，阻止非root用户访问自定义实例自定义数据：  

```
iptables --append OUTPUT --proto tcp --destination 169.254.169.254 --match owner ! --uid-owner root --jump REJECT
```

#### 弹性云服务器元数据类别支持列表

表2-46中不包含兼容EC2类型的ami-id、ami-launch-index、ami-manifest-path、block-device-mapping/、instance-action、instance-id、reservation-id、ramdisk-id、kernel-id元数据项，以上元数据项均无实际含义，不建议使用。

表 2-46 弹性云服务器元数据类别支持列表

| 元数据类型       | 实例元数据项                     | 约束说明                                                                                                                                                          |
|-------------|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| OpenStack类型 | /meta_data.json            | 查询弹性云服务器的元数据信息。<br>元数据的关键字段请参见 <a href="#">表2-47</a> 。                                                                                                        |
| OpenStack类型 | /password                  | 查询弹性云服务器的密码。<br>Windows系统使用keypairs创建弹性云服务器初始化时cloudbase-init用于保存密文密码。                                                                                        |
| OpenStack类型 | /user_data                 | 查询弹性云服务器的自定义数据。<br>用户根据需要自行指定脚本和配置文件用于弹性云服务器初始化，详细操作请参考 <a href="#">通过实例自定义数据配置ECS实例</a> 。<br>若linux虚拟化使用密码方式，则保存注入密码的脚本。                                     |
| OpenStack类型 | /network_data.json         | 查询弹性云服务器的网络信息。                                                                                                                                                |
| OpenStack类型 | /securitykey               | 获取临时的AK、SK。<br>对弹性云服务器获取临时的AK、SK，需要在IAM上对op_svc_ecs账户进行委托授权，并对相应的弹性云服务器资源进行授权委托管理。<br><b>说明</b><br>委托的授权权限由用户自行设置，建议根据实际业务需要进行最小化授权。<br>ECS服务本身不会使用委托对资源进行操作。 |
| OpenStack类型 | /spot/instance-action      | 查询竞价实例关机提示。                                                                                                                                                   |
| 兼容EC2类型     | /meta-data/hostname        | 查询弹性云服务器的主机名称。<br>请参考以下链接为弹性云服务器去掉后缀.novalocal:<br><a href="#">弹性云服务器的主机名带后缀.novalocal</a>                                                                    |
| 兼容EC2类型     | /meta-data/local-hostname  | 该字段含义同hostname一致。                                                                                                                                             |
| 兼容EC2类型     | /meta-data/public-hostname | 该字段含义同hostname一致。                                                                                                                                             |
| 兼容EC2类型     | /meta-data/instance-type   | 查询弹性云服务器的规格名称。                                                                                                                                                |
| 兼容EC2类型     | /meta-data/local-ipv4      | 查询弹性云服务器的固定IP地址。<br>多网卡情况下，只显示主网卡的地址。                                                                                                                         |

| 元数据类型    | 实例元数据项                                                    | 约束说明                                                     |
|----------|-----------------------------------------------------------|----------------------------------------------------------|
| 兼容EC2类型  | /meta-data/<br>placement/<br>availability-zone            | 查询弹性云服务器的AZ信息。                                           |
| 兼容EC2类型  | /meta-data/<br>public-ipv4                                | 查询弹性云服务器的弹性公网IP地址。<br>多网卡情况下，只显示主网卡的弹性公网IP地址。            |
| 兼容EC2类型  | /meta-data/<br>public-keys/0/<br>openssh-key              | 查询弹性云服务器的公钥。                                             |
| 兼容EC2类型  | /user-data                                                | 查询弹性云服务器的自定义数据。                                          |
| 兼容EC2类型  | /meta-data/<br>security-groups                            | 查询弹性云服务器所使用的安全组名称。                                       |
| 华为云元数据类型 | /meta-data/<br>latest/instance-<br>identity/<br>document  | 查询弹性云服务器的实例身份文档。                                         |
| 华为云元数据类型 | /meta-data/<br>latest/instance-<br>identity/<br>signature | 查询弹性云服务器的实例身份文档签名。<br>支持传入自定义audience参数，用于防止<br>签名被非法冒用。 |

表 2-47 metadata 关键字段

| 参数                    | 参数类型   | 描述                                                                                     |
|-----------------------|--------|----------------------------------------------------------------------------------------|
| uuid                  | String | 弹性云服务器的ID。                                                                             |
| availability_zone     | String | 弹性云服务器所在可用区。                                                                           |
| meta                  | Dict   | 元数据信息，包括镜像名称、镜像ID、VPC ID等信息。                                                           |
| hostname              | String | 弹性云服务器主机名。<br>请参考以下链接为弹性云服务器去掉后缀.novalocal:<br><a href="#">弹性云服务器的主机名带后缀.novalocal</a> |
| enterprise_project_id | String | 查询弹性云服务器的企业项目ID信息。                                                                     |

前提条件

- 已登录弹性云服务器。



- 请确保安全组出方向规则满足如下要求，否则访问元数据请求失败：
  - 协议：TCP
  - 端口范围：80
  - 远端地址：169.254.0.0/16

#### 📖 说明

如果您使用的是默认安全组出方向规则，则已经包括了如上要求，可以正常访问元数据。  
默认安全组出方向规则请参见[默认安全组和规则](#)。

## Metadata ( OpenStack 元数据 API )

用于查询弹性云服务器的元数据。

- URI  
/169.254.169.254/openstack/latest/meta\_data.json

- 方法  
支持GET请求。

- 示例：  
Linux操作系统：以使用CURL工具为例，介绍查询弹性云服务器元数据的方法。

**curl http://169.254.169.254/openstack/latest/meta\_data.json**

Windows操作系统：以使用Invoke-RestMethod工具为例，介绍查询弹性云服务器元数据的方法。

**Invoke-RestMethod http://169.254.169.254/openstack/latest/meta\_data.json | ConvertTo-Json**

```
{
 "random_seed": "rEocCViRS+dNwlydGlxJHUP+00poeUsAdBFkbPbYQTmpNwpoEb43k9z+96TyrekNKS
+iLYDdRny4kKGoNPEVBCc05Hg1TcDbIAPfJwgJS1okqEtlcofUhKmL3K0fto
+5KKXEDU3GNuGwyZXjdVb9HQWU+E1jztAjjqsaHnU+g/tawABTVySLBKlAT8fMGax1mTGgArucn/
WzDcy19DGioKPE7F8iLtSQ4Ww3VClK5VYB/h0x+4r7IVHrPmYX/
bi1Yhm3Dc4rRYNaTjdOV5gUOsbo3oAeQkmKwQ/
NO0N8qw5Ya4l8ZUW4tMav4mOsRySOOB35v0bvaJc6p
+50DTbWNeX5A2MLiEhTP3vsPrmvk4LRF7CLz2J2TGIM14OoVBw7LARwmv9cz532zHki/c8tlhRzLmOTXh/
wL36zFW10DeuReUGmxth7IGNmRMQKV6+mil78jm/KMPpgAdK3vwYF/
GcelOFJD2HghMUUCeMbwYnvijLTejuBpwhJMNIHA/NvLEsxJDxqBCoss/Jfe+yCmUFyxovJ
+L8oNkTzkmtCNzw3Ra0hiKchGhqK3BleToV/kVx5DdF081xrEA
+qyoM6CVyftEoz1zIRryo9bJ65Eg6Jd8dj1UCVsDqRY1pljgzE/
Mzsw6AaaCVhaMJL7u7YMVdyKzA6z65Xtvujz0Vo=",
 "uuid": "ca9e8b7c-f2be-4b6d-a639-f10b4d994d04",
 "availability_zone": "lt-test-1c",
 "enterprise_project_id": "0",
 "hostname": "ecs-ddd4.novalocal",
 "launch_index": 0,
 "instance_type": "s3.medium.2",
 "meta": {
 "metering.image_id": "3a64bd37-955e-40cd-ab9e-129db56bc05d",
 "metering.imagetype": "gold",
 "metering.resourcespeccode": "s3.medium.2.linux",
 "admin_pass": "",
 "metering.cloudServiceType": "hws.service.type.ec2",
 "image_name": "CentOS 7.6 64bit",
 "metering.resourcetype": "1",
 "vpc_id": "3b6c201f-aeb3-4bce-b841-64756e66cb49",
 "os_bit": "64",
 "cascaded.instance_extrainfo": "pcibridge:1",
 "os_type": "Linux",
 "charging_mode": "0",
 "__support_agent_list": "hss,ces"
```



```
},
"region_id": "xxx",
"project_id": "6e8b0c94265645f39c5abbe63c4113c6",
"name": "ecs-ddd4"
}
```

## User data ( OpenStack 元数据 API )

用于查询弹性云服务器的自定义数据。该值仅在创建弹性云服务器时指定，不支持修改。

- URI  
/169.254.169.254/openstack/latest/user\_data
- 方法  
支持GET请求。
- 示例

Linux操作系统：

**curl http://169.254.169.254/openstack/latest/user\_data**

Windows操作系统：

**Invoke-RestMethod http://169.254.169.254/openstack/latest/user\_data**

```
ICAgICAgDQoiQSBjbG91ZCBkb2VzIG5vdCBrbm93IHdoeSBpdCBtb3ZlcyBpbjBqdXN0IHN1Y2ggYSBkaXJlY
3Rpb24gYW5kIGF0IHN1Y2ggYSBzcGVlZC4uLkI0IGZlZWxzIGFuIGltcHVsc2lubi4uLnRoaXMgaXMgdGhllH
BsYWNlIHVlGdviG5vdy4gQnV0IHRob2ZSBza3kga25vd3MgdGhllHJlYXNvbnMgYW5kIHRob2ZSBwYXR0ZXJu
cyBiZWphbmQgYWxslGNsb3VkcycgYW5kIHlvdSB3aWxslGtub3csiHRvbywgd2h1biB5b3UgbGlmdCB5b3
Vyc2VsZiBoaWdoIGVub3VnaCB0byBzZWUgYmV5b25kIGhvcml6b25zLiINCg0KLlJpY2hhcmQgQmFjaA=
=
```

### 说明

如果创建弹性云服务器时未注入自定义数据，此时，该接口的查询结果是404，如图2-158所示。

图 2-158 404 Not Found

```
[root@pythonsdktempest-1519783681 ~]# curl http://169.254.169.254/openstack/latest/user_data
<html>
<head>
<title>404 Not Found</title>
</head>
<body>
<h1>404 Not Found</h1>
The resource could not be found.

</body>
</html>
```

## Network data ( OpenStack 元数据 API )

查询弹性云服务器的网络信息，支持查询云服务器挂载的全部网卡的信息，包括网卡所在子网的DNS地址、网络带宽、网卡ID、网卡私有IP地址、网卡弹性公网IP地址、网卡的MAC地址。

- URI  
/openstack/latest/network\_data.json
- 方法  
支持GET请求
- 示例

### 📖 说明

instance\_max\_bandwidth、instance\_min\_bandwidth的单位是Mbps，如果取值为-1，说明对带宽大小无限制。

Linux操作系统：

**curl http://169.254.169.254/openstack/latest/network\_data.json**

Windows操作系统：

**Invoke-RestMethod http://169.254.169.254/openstack/latest/network\_data.json | ConvertTo-Json**

```
{
 "services": [{
 "type": "dns",
 "address": "xxx.xx.x.x"
 },
 {
 "type": "dns",
 "address": "100.125.21.250"
 }
],
 "qos": {
 "instance_min_bandwidth": 100,
 "instance_max_bandwidth": 500
 },
 "networks": [{
 "network_id": "67dc10ce-441f-4592-9a80-cc709f6436e7",
 "type": "ipv4_dhcp",
 "link": "tap68a9272d-71",
 "id": "network0"
 }
],
 "links": [{
 "vif_id": "68a9272d-7152-4ae7-a138-3ef53af669e7",
 "public_ipv4": "100.100.xx.xx",
 "ethernet_mac_address": "fa:16:3e:f7:c1:47",
 "mtu": null,
 "local_ipv4": "192.169.10.10",
 "type": "cascading",
 "id": "tap68a9272d-71"
 }
]
}
```

## Security Key ( OpenStack 元数据 API )

获取临时的AK、SK。

### 📖 说明

- 您如果需要在弹性云服务器获取临时的AK、SK，需要在IAM对弹性云服务器进行云服务委托授权，并在相应的弹性云服务器的详情页面“管理信息 > 委托”栏目中添加委托。  
详细操作请参考[委托其他云服务管理资源](#)。
- 临时的AK、SK有效期24个小时。临时的AK、SK过期时间的响应参数为UTC时间格式，北京时间为UTC+8小时。建议您根据业务需要，在过期时间到期前重新获取AK、SK。
- 使用临时AK、SK时，需要在消息的header中增加'X-Security-Token':{securitytoken}。其中，securitytoken就是调用接口返回的值。
- URI  
/openstack/latest/securitykey
- 方法  
支持GET请求
- 示例

## Linux操作系统:

```
curl http://169.254.169.254/openstack/latest/securitykey
```

Windows操作系统:

**Invoke-RestMethod http://169.254.169.254/openstack/latest/securitykey**

## Instance Action ( OpenStack 元数据 API )

用于查询竞价实例关机提示。

### 说明

如果您的竞价实例即将被中断，该接口会返回预计关机的时间。

- URI  
/openstack/latest/spot/instance-action
- 方法  
支持GET请求。
- 示例

## Linux操作系统:

```
curl http://169.254.169.254/openstack/latest/spot/instance-action
```

Windows操作系统:

**Invoke-RestMethod http://169.254.169.254/openstack/latest/spot/instance-action**

```
{"action": "terminate", "timestamp": "2023-06-01 09:15:00"}
```

## User data ( EC2-兼容的 API )

用于查询弹性云服务器的自定义。该值仅在创建弹性云服务器时指定，不支持修改。

- URI  
/169.254.169.254/latest/user-data
- 方法  
支持GET请求。
- 示例

## Linux操作系统:

```
curl http://169.254.169.254/latest/user-data
```

Windows操作系统:

**Invoke-RestMethod http://169.254.169.254/latest/user-data**

ICAgICAGDQoiQSBJbG91ZCBkb2VzIG5vdCBrbm93IHdoeSBpdCBtb3ZlcyBpbjBqdXN0IHN1Y2ggYSBkaXJlY3Rpb2t4YgW5kiGvOIHN1Y2ggYSBzcGVZC2UkLkglZGVZCWxzIjFuGfGlTcXhvSc2vlbi4uLnRoXMGxaMgdGHlHXBSwYNllHRvIGdvlG5dydg4qVnOIHROZSBza3kg2o5Vz3MgdGhlHlYXNvbmcgYW5kSHRoZWxwYXRlZHUu cyBiZWWhpbmQgYWxsIGNsbn3VkcywgYW5kIHlvdB3BaWxslGTub3csIHrvbywgd2hlib5b3UgbGlm dB5b3 Vyc2VsZiBoaWdoiGVub3VnaCB0byBzZWUwYmV5b25klGhvcml6b25zLiilNCgOKLVjpY2hhcmQgQmFjaA=

## Hostname ( EC2-兼容的 API )

用于查询弹性云服务器的主机名称，后面会追加.novalocal后缀。

- URI  
/169.254.169.254/latest/meta-data/hostname
- 方法  
支持GET请求。
- 示例  
Linux操作系统：  
**curl http://169.254.169.254/latest/meta-data/hostname**  
Windows操作系统：  
**Invoke-RestMethod http://169.254.169.254/latest/meta-data/hostname**  
vm-test.novalocal

## Instance Type ( EC2-兼容的 API )

用于查询弹性云服务器的规格名称。

- URI  
/169.254.169.254/latest/meta-data/instance-type
- 方法  
支持GET请求。
- 示例  
Linux操作系统：  
**curl http://169.254.169.254/latest/meta-data/instance-type**  
Windows操作系统：  
**Invoke-RestMethod http://169.254.169.254/latest/meta-data/instance-type**  
s3.medium.2

## Local IPv4 ( EC2-兼容的 API )

用于查询弹性云服务器的固定IP地址。多网卡情况下，只显示主网卡的地址。

- URI  
/169.254.169.254/latest/meta-data/local-ipv4
- 方法  
支持GET请求。
- 示例  
Linux操作系统：  
**curl http://169.254.169.254/latest/meta-data/local-ipv4**  
Windows操作系统：  
**Invoke-RestMethod http://169.254.169.254/latest/meta-data/local-ipv4**  
192.1.1.2

## Availability Zone ( EC2-兼容的 API )

用于查询弹性云服务器的AZ信息。

- URI  
/169.254.169.254/latest/meta-data/placement/availability-zone
- 方法  
支持GET请求。
- 示例  
Linux操作系统：  
**curl http://169.254.169.254/latest/meta-data/placement/availability-zone**  
Windows操作系统：  
**Invoke-RestMethod http://169.254.169.254/latest/meta-data/placement/availability-zone**  
az1.dc1

## Public IPv4 ( EC2-兼容的 API )

用于查询弹性云服务器的弹性公网IP地址。多网卡情况下，只显示主网卡的弹性公网IP地址。

- URI  
/169.254.169.254/latest/meta-data/public-ipv4
- 方法  
支持GET请求。
- 示例  
Linux操作系统：  
**curl http://169.254.169.254/latest/meta-data/public-ipv4**  
Windows操作系统：  
**Invoke-RestMethod http://169.254.169.254/latest/meta-data/public-ipv4**  
46.1.1.2

## Public Keys ( EC2-兼容的 API )

用于查询弹性云服务器的公钥。

- URI  
/169.254.169.254/latest/meta-data/public-keys/0/openssh-key
- 方法  
支持GET请求。
- 示例  
Linux操作系统：  
**curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key**  
Windows操作系统：  
**Invoke-RestMethod http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key**  
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQBDI5Fw5k8Fgzajn1zJwLoV3+wMP+6CyvsSilc/hioggSnYu/AD0Yqm8vVO0kWLun1rFbdO+QUZKyVr/OPUjQSw4SRh4qsTKf/+eFoWTjplFvd1WCBZzS/WRenxIwR00KkcZHSJro763+wYcwKieb4eKRxaQoQvoFgVjLBULXAjH4eKoKTVNtMXAvPP9aMy2SLgsJNtMb9ArfziAibIQynq7UIfLnN3VclzPeiWrqtzjyOp6CPUXnL0lVPTvbLe8sUteBsJZWlL6K4i

```
+Y0lf3ryqnmQgC21yW4Dzu+kwk8FVT2MgWkCwiZd8gQ/+uJzrJFyMfUOBikIOBfuUENIJUhaB
Generated-by-Nova
```

## ECS 实例身份文档（华为云元数据类型）

用于查询弹性云服务器的实例身份文档。

- URI

/169.254.169.254/meta-data/latest/instance-identity/document

- 方法

支持GET请求。

- 示例

Linux操作系统：

**curl** http://169.254.169.254/meta-data/latest/instance-identity/document

Windows操作系统：

**Invoke-RestMethod** http://169.254.169.254/meta-data/latest/instance-identity/document

```
{"architecture":"x86_64","availability_zone":"az1","created_at":"2025-06-05
07:20:58.580117+0:00","domain_id":"808000042306xxxxxx","flavor":"c7.large.2","hypervisor":"kvm","id":
:"d776bea4-b128-4f36-b521-9bf625xxxxxx","image_id":"bfccced4-909b-497a-ba85-
efebd85df6a1","private_ipv4":"192.168.1.101","project_id":"c592fc8cad84600ab6d3aa62xxxxxx","region":
:"region1"}
```

## ECS 实例身份文档签名（华为云元数据类型）

用于查询弹性云服务器的实例身份文档签名。

- URI

/169.254.169.254/meta-data/latest/instance-identity/signature?  
audience=xxxxx

### 说明

?audience=xxxxx非必填，具体说明，请参见[验证实例身份文档签名](#)。

- 方法

支持GET请求。

- 示例

Linux操作系统：

**curl** http://169.254.169.254/meta-data/latest/instance-identity/signature

Windows操作系统：

**Invoke-RestMethod** http://169.254.169.254/meta-data/latest/instance-identity/signature

```
MIILBgYJKoZIhvcNAQcCoIIK9zCCCuMCAQExDzANBg1ghkgBZQMEAgEFADCCAZQGCSqGSIb3DQEHAaC
CAYUEggGBeyJhcmNoaXR1Y3R1cmUiOiJ4ODZfNjQlLCJhdmFpbGFiaWxpdmH1fem9uZSI6ImNuLXudXRodZ
UzdCBYZSI6ImNyZMF0ZWRFYXQiOiIyMD1LTAAZLTAA1IDA30jluOjU4LjUAMDEXNysuMDouMCI6ImRvbWVp
bi9pZCI6IjgwODAuMDAuNDIzMDYuMDAuMDAiLCJmbGFZ63li0iIjNy5sYXIn2S4yliwiaHluZXIZaXNvcil6I
mt2bSIsImkljoiZDc3NmUIYTQtYjE5OC88ZjM2LWI1MjEtOWImYz11MtzBjOWM3liwiaW1hZ2UfawQiOiIj
MZZjYUKNKMD1iLTQSNZEtYmEANS11ZMU.....
.....
.....
.....
.....
```

```
+ra8oU3snPL1miTU5Pt85WXn7dMHxEa7Eh++T5HCik+jnREx+nXDtD/
CdfnJsRLUkHiRIKkHbKMZXYMa6Yo5NivF99GlpWjMSdNouGHuBIFeJkPH7i4So3ZsItlbZFfuUP39DYaYf02
IESrD4viDC96LBAh0X1IE/oOLUuzu/darNdHDMU617tn+CHOYNBEP+LkCthWKOC
+OBdLdmEASXAUTXDKOXT86tk1Mw0kmbxos
+2ufec5gFNLN7iUTahFomsZKA1rlxO0oSuSdrZISiAZat9C3TACiKxDU4tACYzb3R
+SuMx7CJNCbeY8XudXeoWCR18ebsHTk6aiMGbpo9T7Xbbve5AuukkufaocR406LhaZBnSnc6jyT9us1faZ
RFiU350Uo3b
+U0nBDArQFsFGfaCi6MeLEak1YDAabzWciURGSlihZWTLiaJXKWUnbUULRhGT1m8wloi11Z1E9EZ
+9ZbR4FLInsoPXo1hobmtfPCukfjYsnxucUoguCJsCuN9sxZH9L7WeTJo9T
```

## 相关链接

[Linux操作系统云服务器无法获取元数据怎么办？](#)

### 2.7.3.2 通过实例自定义数据配置 ECS 实例

#### 使用场景

当您有如下需求时，可以考虑使用实例自定义数据注入功能来配置弹性云服务器：

- 需要通过脚本简化弹性云服务器配置
- 通过脚本初始化系统
- 已有脚本，在创建弹性云服务器的时候一并上传到服务器
- 其他可以使用脚本完成的功能

#### 使用限制

- Linux：
  - 用于创建弹性云服务器的镜像安装了Cloud-init组件。
  - 实例自定义数据大小限制：小于等于32KB。
  - 如果通过文本方式上传实例自定义数据，数据只能包含ASCII码字符；如果通过文件方式上传实例自定义数据，可以包含任意字符，同时，要求文件大小小于等于32KB。
  - 必须是公共镜像，或继承于公共镜像的私有镜像，或自行安装了Cloud-init组件的私有镜像。
  - 必须满足相应Linux弹性云服务器自定义脚本类型的格式要求。
  - 使用的VPC网络必须开启DHCP，安全组出方向规则保证80端口开放。
  - 选择“密码”登录方式时，不支持实例自定义数据注入功能。
- Windows
  - 用于创建弹性云服务器的镜像安装了Cloudbase-init组件。
  - 实例自定义数据大小限制：小于等于32KB。
  - 如果通过文本方式上传实例自定义数据，数据只能包含ASCII码字符；如果通过文件方式上传实例自定义数据，可以包含任意字符，同时，要求文件大小小于等于32KB。
  - 必须是公共镜像，或继承于公共镜像的私有镜像，或自行安装了Cloudbase-init组件的私有镜像。
  - 使用 VPC网络必须开启DHCP，安全组出方向规则保证80端口开放。

使用方法

- 1. 根据实际需要写User-Data脚本，脚本格式必须符合User-Data脚本，详细规范请参见[相关链接](#)。
- 2. 创建弹性云服务器时，需将实例自定义数据脚本内容粘贴到“高级选项 > 现在配置 > 实例自定义数据注入”的文本框，或选择实例自定义数据文件上传。

说明

实例自定义数据注入支持使用文件和文本两种方式：

文本：将实例自定义数据脚本内容粘贴到文本框中。

文件：将实例自定义数据脚本内容保存至文本文件后再将上传。

图 2-159 实例自定义数据注入



- 3. 系统创建弹性云服务器，弹性云服务器启动后自动执行Cloud-init或Cloudbase-init组件，读取实例自定义数据脚本。

关于 Linux 云服务器的实例自定义数据脚本

Linux弹性云服务器的自定义实例自定义数据脚本（简称“脚本”）采用开源的Cloud-init架构实现，该架构以云服务器的元数据为数据来源，对弹性云服务器进行各项自动化配置。自定义脚本类型兼容开源Cloud-init，详情请参考Cloud-init开源说明：<http://cloudinit.readthedocs.io/en/latest/topics/format.html>。

- 脚本的执行时间：弹性云服务器的状态变为“running”之后，执行文件/etc/init之前。

说明

- 脚本默认以root用户权限执行。
- 脚本类型：包括“User-Data Script”和“Cloud-Config Data”。

表 2-48 Linux 云服务器脚本类型介绍

| -  | User-Data Script               | Cloud-Config Data                             |
|----|--------------------------------|-----------------------------------------------|
| 描述 | 以脚本作为自定义配置的手段，如shell和python脚本。 | Cloud-init中预定义的对云服务器部分服务进行配置的手段，如yum源、SSH 密钥。 |



| -  | User-Data Script                                                                                                      | Cloud-Config Data                  |
|----|-----------------------------------------------------------------------------------------------------------------------|------------------------------------|
| 格式 | 首行必须是“#!”（如“#!/bin/bash和#!/usr/bin/env python”），且前面不能有空格。<br>首次启动时，将在rc.local-like级别上执行，rc.local-like意味着“在启动序列中非常靠后”。 | 首行必须是“#cloud-config”，且前面不能有空格。     |
| 限制 | 在采用Base64编码前，脚本内容（包括首行在内）不能超过32KB。                                                                                    | 在采用Base64编码前，脚本内容（包括首行在内）不能超过32KB。 |
| 频率 | 仅在首次启动弹性云服务器时执行一次。                                                                                                    | 配置的服务不同，执行频率也会不同。                  |

- 如何查看注入Linux弹性云服务器的自定义数据？
  - 登录弹性云服务器。
  - 执行以下命令，以root用户权限查看实例自定义数据。

curl http://169.254.169.254/openstack/latest/user\_data
- 脚本使用示例：

该示例介绍如何以不同格式输入Linux弹性云服务器的脚本，并查看脚本的运行结果。

**示例一：脚本类型为User-Data Script**

创建弹性云服务器时，选择“文本”形式并输入实例自定义数据脚本，脚本如下：

#!/bin/bash  
echo "Hello, the time is now \$(date -R)" | tee /root/output.txt

创建成功后，连接并启动弹性云服务器，执行命令`cat [file]`，查看脚本的运行结果。

[root@XXXXXXXX ~]# cat /root/output.txt  
Hello, the time is now Mon, 16 Jul 2016 16:03:18+0800

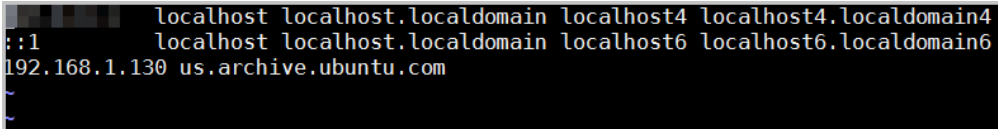
**示例二：脚本类型为Cloud-Config Data**

创建弹性云服务器时，选择“文本”形式并输入实例自定义数据脚本，脚本如下：

#cloud-config  
bootcmd:  
- echo 192.168.1.130 us.archive.ubuntu.com >> /etc/hosts

创建成功后，连接并启动弹性云服务器，执行命令`cat /etc/hosts`查看脚本的运行结果。

图 2-160 查看运行结果



关于 Windows 弹性云服务器的实例自定义数据脚本

Windows弹性云服务器的实例自定义数据脚本（简称“脚本”）采用开源的 cloudbase-init架构实现，该架构以弹性云服务器的元数据为数据来源，对弹性云服务器进行各项自动化配置，为Windows弹性云服务器提供执行初始化脚本的能力。自定义脚本类型兼容开源Cloudbase-init，详情请参考Cloudbase-init开源说明：<https://cloudbase-init.readthedocs.io/en/latest/userdata.html>。

- 脚本类型：包括“Batch批处理程序”和“PowerShell脚本”。

表 2-49 Windows 云服务器脚本类型介绍

| -  | Batch批处理程序                         | PowerShell脚本                       |
|----|------------------------------------|------------------------------------|
| 格式 | 以“rem cmd”开头且作为首行，且前面不能有空格。        | 以“#ps1”开头且作为首行，且前面不能有空格。           |
| 限制 | 在采用Base64编码前，脚本内容（包括首行在内）不能超过32KB。 | 在采用Base64编码前，脚本内容（包括首行在内）不能超过32KB。 |

- 如何查看注入Windows弹性云服务器的实例自定义数据？
  - a. 登录弹性云服务器。
  - b. 在浏览器栏访问如下地址，查看注入的实例自定义数据。  
**`http://169.254.169.254/openstack/latest/user_data`**
- 脚本使用示例  
该示例介绍如何以不同格式输入Windows弹性云服务器的脚本，并查看脚本的运行结果。

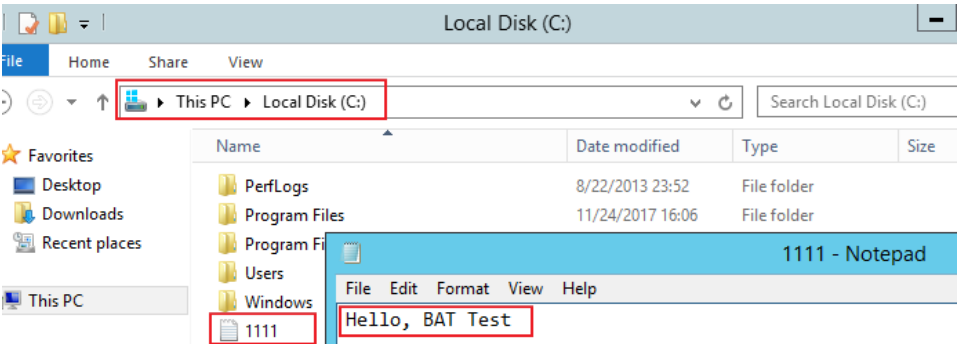
示例一：Batch批处理程序

创建弹性云服务器时，选择“文本”形式并输入实例自定义数据，脚本如下：

```
rem cmd
echo "Hello, BAT Test" > C:\1111.txt
```

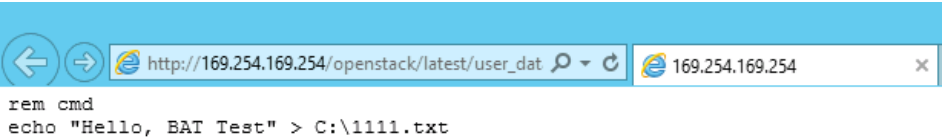
创建成功后，连接并启动弹性云服务器，查看脚本的运行结果：在C:\盘添加了一个名称为“1111”的文本文档，如图2-161所示。

图 2-161 新建文本文档\_Batch



如需查看注入Windows弹性云服务器的实例自定义数据，可以在浏览器访问：[http://169.254.169.254/openstack/latest/user\\_data](http://169.254.169.254/openstack/latest/user_data)，如图2-162所示。

图 2-162 查看实例自定义数据\_Batch



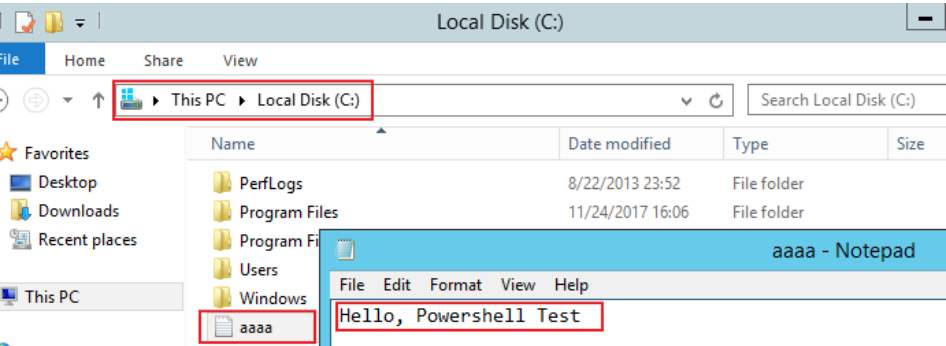
示例二：PowerShell脚本

创建弹性云服务器时，选择“文本”形式并输入实例自定义数据，脚本如下：

```
#ps1
echo "Hello, Powershell Test" > C:\aaaa.txt
```

创建成功后，连接并启动弹性云服务器，查看脚本的运行结果：在C:\盘添加了一个名称为“aaaa”的文本文档。

图 2-163 新建文本文档\_PowerShell



如需查看注入Windows弹性云服务器的实例自定义数据，可以在浏览器访问：[http://169.254.169.254/openstack/latest/user\\_data](http://169.254.169.254/openstack/latest/user_data)，如图2-164所示。

图 2-164 查看实例自定义数据\_PowerShell



案例 1

该样例介绍如何通过实例自定义数据注入，为Linux弹性云服务器简化云服务器配置。

当您需要设置vim的“语法高亮显示”、“制表符占用4个空格”和“显示行数”属性时，就可以写一个脚本.vimrc，并将其注入到“/root/.vimrc”。在您创建完云服务器时，您的vim配置便完成了。这样做可以大幅提高系统配置的效率，特别是在您一次性创建多台弹性云服务器时。

实例自定义数据注入示例：

```
#cloud-config
write_files:
- path: /root/.vimrc
 content: |
 syntax on
 set tabstop=4
 set number
```

案例 2

该样例介绍如何通过实例自定义数据注入，设置Linux弹性云服务器密码。

说明

新密码必须符合密码复杂度要求，密码规则如表2-50所示。

表 2-50 密码设置规则

| 参数 | 规则                                                                                                                                                                                                                                                                                                                                                      |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 密码 | <ul style="list-style-type: none"><li>密码长度范围为8到26位。</li><li>密码至少包含以下4种字符中的3种：<ul style="list-style-type: none"><li>大写字母</li><li>小写字母</li><li>数字</li><li>Windows操作系统云服务器支持的特殊字符：!@\$%^_-=+[{()}];./?~#*</li><li>Linux操作系统云服务器支持的特殊字符：!@\$%^_-=+[{()}];./?~#*</li></ul></li><li>密码不能包含用户名或用户名的逆序。</li><li>Windows操作系统的云服务器，不能包含用户名中超过两个连续字符的部分。</li></ul> |

实例自定义数据注入示例:

使用密文密码（推荐使用）：

```
#!/bin/bash
echo 'root:6V6azyeLwcD3CHlpY$BN3VVq18fmCkj66B4zdHLWevqcxlig' | chpasswd -e;
```

其中，\$6\$V6azyeLwcD3CHlpY\$BN3VVq18fmCkj66B4zdHLWevqcxlig为密文密码，生成方法如下：

1. 执行以下命令，生成加密盐值
- ```
python -c "import crypt, getpass, pwd;print crypt.mksalt()"
```
- 回显信息如下：
- ```
6V6azyeLwcD3CHlpY
```
2. 执行以下命令，根据盐值生成密文密码
- ```
python -c "import crypt, getpass, pwd;print crypt.crypt('Cloud.1234','\$6\$V6azyeLwcD3CHlpY')"
```
- 回显信息如下：
- ```
6V6azyeLwcD3CHlpY$BN3VVq18fmCkj66B4zdHLWevqcxlig
```

弹性云服务器创建成功后，您可以使用该密码登录。

案例 3

该样例介绍如何通过实例自定义数据注入，重置Linux弹性云服务器密码。

假设您需要将root用户密码重置为”\*\*\*\*\* “。

 说明

新密码必须符合密码复杂度要求，密码规则如[表2-51](#)所示。

表 2-51 密码设置规则

| 参数 | 规则                                                                                                                                                                                                                                                                                                                                                    |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 密码 | <ul style="list-style-type: none"><li>密码长度范围为8到26位。</li><li>密码至少包含以下4种字符中的3种：<ul style="list-style-type: none"><li>大写字母</li><li>小写字母</li><li>数字</li><li>Windows操作系统云服务器支持的特殊字符：!@\$%^_-=+[{()};./?~#*</li><li>Linux操作系统云服务器支持的特殊字符：!@\$%^_-=+[{()};./?~#*</li></ul></li><li>密码不能包含用户名或用户名的逆序。</li><li>Windows操作系统的云服务器，不能包含用户名中超过两个连续字符的部分。</li></ul> |

实例自定义数据注入示例（请严格遵守下面示例中的缩进标准）：

```
#cloud-config
chpasswd:
 list: |
 root:*****
 expire: False
```

弹性云服务器创建成功后，您可以使用重置的密码登录弹性云服务器。为了保证密码安全，建议您在第一次登录弹性云服务器后，修改root用户密码。

案例 4

该样例介绍如何通过实例自定义数据注入，为Windows弹性云服务器新增用户并设置密码。

假设您要创建的用户名为abc、密码为“\*\*\*\*\*”的普通用户，并将其添加至administrators用户组。

 说明

新密码必须符合密码复杂度要求，密码规则如[表2-51](#)所示。

实例自定义数据注入示例：

```
rem cmd
net user abc ***** /add
net localgroup administrators abc /add
```

弹性云服务器创建成功后，您可以使用新创建的用户名和密码登录弹性云服务器。

## 案例 5

该样例介绍如何通过实例自定义数据注入，为Linux弹性云服务器更新系统软件包，并且开启httpd相关服务。注入成功后，您的弹性云服务器就可以使用httpd服务了。

实例自定义数据注入示例：

```
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

## 案例 6

该样例介绍如何通过实例自定义数据注入，激活Linux弹性服务器的root用户远程登录权限。注入成功后，您可以使用SSH密钥方式，以root账户登录弹性云服务器。

实例自定义数据注入示例：

```
#cloud-config
disable_root: false
runcmd:
- sed -i 's/^PermitRootLogin.*$/PermitRootLogin without-password/' /etc/ssh/sshd_config
- sed -i '/^KexAlgorithms.*$/d' /etc/ssh/sshd_config
- service sshd restart
```

## 相关链接

更多关于实例自定义数据注入案例的介绍，请参见Cloud-init/Cloudbase-init官网：

- <https://cloudinit.readthedocs.io/en/latest/>
- <https://cloudbase-init.readthedocs.io/en/latest/>

### 2.7.3.3 验证实例身份文档签名

## 操作场景

实例标识签名，包含实例身份文档签名（signature）、实例身份文档（document）和签名证书（server.pem）。

- 实例身份文档签名（signature），用于供第三方验证实例标识文档的真实性和内容。

实例标识签名采用**PKCS #7**格式加密，纯数字化，安全可靠。

实例标识签名支持传入自定义audience参数，用于防止签名被非法冒用。audience参数可以是随机字符串、时间戳、规律性变化的信息或者根据算法生成的数据。传入audience参数后，即使他人获取了标识文档和标识签名的部分信息，也很难猜测到audience参数的取值。通过audience参数实现鉴权。

具体使用方法，请参见**ECS实例身份文档（华为云元数据类型）**和**ECS实例身份文档签名（华为云元数据类型）**。

- 实例身份文档（document），用于提供实例的身份信息，包括实例ID、IP地址等，包含的属性如**表2-52**所示。

表 2-52 实例身份文档属性说明

| 参数                | 说明         |
|-------------------|------------|
| architecture      | 实例架构。      |
| availability_zone | 实例所属可用区。   |
| created_at        | 实例创建时间。    |
| domain_id         | 租户域ID。     |
| flavor            | 实例规格名称。    |
| hypervisor        | 实例虚拟化类型。   |
| id                | 实例ID。      |
| image_id          | 实例的镜像ID。   |
| private_ipv4      | 实例的私网IP地址。 |
| project_id        | 项目ID。      |
| region            | 实例所属区域。    |

- 签名证书（server.pem），用于签名。  
本文介绍如何获取实例标识签名并验证其合法性。

操作步骤

1. 远程登录弹性云服务器。
2. 执行以下命令，获取实例身份文档签名，并保存至signer.p7b。  
`curl http://169.254.169.254/meta-data/latest/instance-identity/signature > signer.p7b`
3. 执行以下命令，验证实例身份文档签名的合法性。  
`echo '-----BEGIN PKCS7-----' > signer`  
`cat signer.p7b >> signer`  
`echo " " >> signer`  
`echo '-----END PKCS7-----' >> signer`  
`openssl smime -verify -noattr -in signer -inform PEM -noverify`  
如果返回Verification successful，表示验签成功。

图 2-165 验签成功



4. 验证服务证书合法性。
  - a. 执行以下命令，提取服务证书。  
`openssl pkcs7 -in signer -inform PEM -print_certs -out server.pem`
  - b. 执行以下命令，验证证书链。  
`openssl verify -verbose -CAfile root.crt server.pem`



### 说明

root.crt请参考[root.crt证书](#)。

当结果输出OK表示证书链合法。

图 2-166 证书链合法

```
root@i-ctrl-nova06:/home/fsp/ddd # openssl verify -verbose -CAfile root.crt server.pem
server.pem: OK
```

## root.crt 证书

```
-----BEGIN CERTIFICATE-----
MIIF9zCCA9+gAwIBAgIKBEnIQUn/qRh2SjANBgkqhkiG9w0BAQsFADCBhjELMAkG
A1UEBhMCQ04xCjAIBgNVBAGMAS0xCjAIBgNVBACMAS0xHDAaBgNVBAoME0h1YXdl
aSB1ZWNobm9sb2dpZXNFTATBgNVBAsMDEh1YXdlSBDBG91ZDEqMCgGA1UEAwWh
SHVhd2VpIENsb3VklEluc3RhbmNlIE1ldGFkYXRhIENBMCAxDTI1MDUwODE0NDkw
MloYDzIwNTUwNTA4MTQ0OTAyWjCBhjELMAkGA1UEBhMCQ04xCjAIBgNVBAGMAS0x
CjAIBgNVBACMAS0xHDAaBgNVBAoME0h1YXdlSB1ZWNobm9sb2dpZXNFTATBgNV
BAsMDEh1YXdlSBDBG91ZDEqMCgGA1UEAwWhSHVhd2VpIENsb3VklEluc3RhbmNl
IE1ldGFkYXRhIENBMIIcljANBgkqhkiG9w0BAQEFAAOCAg8AMIICGKCAgEArulD
1aDj9Q5op4MKOOcYnrf+txrO05ecSNtKBfrazmmB2uB3/NIF4kg5tycBdNqO+qgp
b4IAhih6EOM1cl21Pfk27Gzr2WML91GCG5pDpc42pn/yMyuupjGA0HH1Pp/lrdPj
JmG0E9HUXgyJ+lIVo9OrnrLTP7URkFJE+dEoDBtTHD7SaTiK48ssYXAYrLUS9RZA
6wZ+WWldTY6/1o3gROMKRQT5EK2Ny4H7ZUmZe1CPYWLZsNsRYQ3+GiMcB7DG9R4C
xs4inp0RQ3Fsr2RLXwyA7V9AI2YNKa1bEy3/TE/qSQFWs5KrYxj8rVw+fhhpOGJU
FrIQOY89rgUhfK2SdsRspBLqzIX5dMDYrMDOChS9Ldlc6w990U7CYkfxToc7oQ/y
LOiCbcXvwezX+wfxmIUlsJo2kr5MJ41Fsp1C+oeBUCenJuyrcgw2ZSlfPCe6NVJW
zFp5FOo+SnBwXqgo+Ec63fkCkEwuRghhQtYzlvFROkKpjBi8zdJO00pvQKQpmc1O
jbxZBeiC4dFLOyWbmghfPDhA7eG6o0om3drlq2hd9Z7HDEqc6GlgX3rCyy0YcQn1
wiqYZE/73m3n3JsvqRXbnGxJ1SZkod/yGmowOtZ731HQ/Bw5itMOrOZFntWhXB1e
PTwNDWzZxULJXctlpCtwRYZ9tn8pn6GvDCAv2o0CAwEAANjMGEwHwYDVR0jBBgw
FoAU8oc+3dg4k8Hkc7nZJAeYgPElayMwHQYDVR0OBBYEFKHPt3YOJPB5HO52SQH
mldXJWsjMA8GA1UdEwEB/wQFMAMBAf8wDgYDVR0PAQH/BAQDAgGGMA0GCSqGSIb3
DQEBcwUAA4ICAQAx+RLIG6d0Z5jpj1ctBCh38nU4SNh2ftChTGRfvl2Een68YYys
0kigq5LrkH5repFgF8rxGkDIqBUH58sQn/McisZ51nxzUKTw4uc806wq1K4P+B5
t55Qz3fmXWn0wfv1bGonRugKaY2CcKhfCRbCOBJ5XlogC/Fw+ovzQK88gCGYUD+h
8rJnu4PtaRUXBkrCwKf2KcpdA9g2NICFslqqaCoEfGQIF9tpnzZ8WMCPcDNvR
JbwaGICCs/x1pVrzboNOoniqE7z0F9rgD/hV9Phpmlry3AknU5hB557VjINhIW
D61LXbbrV9Oykpod0/utsEGb32O4lc1NrrFHYULlurVsHkZny7JHSiy+MhQ06
sHV1aq2kwXV0PuaSOLObpq+RDLGq7N5pPHxIkZcLL51VixZiqjaXPbn0akPij08Z
HQ+sLzhZJ6mx5mEaQj/ZdvPO3q00WhJds5K9wl5r8FL6Ao7BM4+limr4WrxNm277
rMoD+QVMKnYaNFFsyYVKE4VUNPRBjZORxVHRVvCfj9mpBillqfTqggggRB7EVbwm
Xf6byLx89oelBmbfzd5k0ALDSz+W/7tsGKUzVGgLSvbM98vBkh8cJM8tkadhkfxe
JQX3PqFvj2MNOZeb95SFOQRLqCe+Ge+uCl1u1ShfT6e1TNJTFunb9iXFOCw==
-----END CERTIFICATE-----
```

## 2.7.4 修改 ECS 主机名 (hostname)

### 操作场景

ECS支持修改主机名功能，支持修改已创建的Linux操作系统ECS的静态主机名 (hostname)。

Linux操作系统ECS的静态主机名来源于创建ECS时，通过Cloud-init注入的用户自定义名称。ECS创建成功后，您可以根据业务需要，通过管理控制台在线修改ECS的名称和主机名。

修改ECS名称的详细操作，请参见[修改ECS名称](#)。离线修改ECS静态主机名的详细操作，请参见[怎样使修改的静态主机名永久生效?](#)

本文介绍如何为Linux操作系统ECS在线修改主机名。



## 约束与限制

- 该功能依赖云运维中心（Cloud Operations Center，简称COC），需开通并授权COC服务。  
对于IAM用户，需额外配置COC资源操作类权限，详细内容，请参见[配置ECS自助运维自定义策略](#)。
- 该功能依赖UniAgent。UniAgent是统一数据采集Agent，支持脚本下发和执行。若ECS未安装UniAgent，则无法修改主机名，详细内容，请参见[为ECS安装UniAgent](#)。
- 仅支持为Linux操作系统ECS修改主机名。
- 因系统存在缓存，使用VNC、CloudShell等远程登录工具登录的ECS，可能无法在修改完成后立即更新主机名，需退出并重新登录后才可更新。  
建议您使用命令退出ECS：  
`exit`

## 操作步骤

您可以为单台或多台ECS修改主机名，多台ECS修改后主机名相同。

### 为单台 ECS 修改主机名

- 登录管理控制台，进入[弹性云服务器](#)列表页面。
- 在待修改主机名ECS的“操作”列，单击“更多 > 修改主机名”。
- （可选）在“开通云运维中心并添加权限”页面，阅读服务声明并勾选后，单击“开通并授权”。  
若当前账号未开通并授权COC服务，则会显示该页面。
- 在“修改主机名”页面，根据界面提示信息，完成相关参数配置。

#### 须知

修改主机名功能依赖UniAgent，如果提示未安装UniAgent或者安装失败，请参考[为ECS安装UniAgent](#)进行安装，否则无法修改主机名。

图 2-167 修改主机名



表 2-53 修改主机名参数配置

| 参数             | 说明                                                                          |
|----------------|-----------------------------------------------------------------------------|
| 云服务器名称（可选）     | 可选配置，ECS的名称。您可以在修改主机名时同步修改ECS名称，修改后立即生效。<br>只能由中文字符、英文字母、数字及“_”、“-”、“.”组成。  |
| 主机名 (Hostname) | ECS的静态主机名hostname，修改后立即生效。<br>只能由英文字母、数字及“.”、“-”组成，但“.”和“-”不能连续使用或出现在开头和结尾。 |

5. 单击“确定”，完成ECS主机名的修改。

为多台 ECS 修改主机名

1. 登录管理控制台，进入弹性云服务器列表页面。
2. 在ECS列表中，勾选待修改主机名的多台ECS。
3. 单击列表上方的“更多 > 修改主机名”。
4. 在“修改主机名”页面，根据界面提示信息，完成相关参数配置。

须知

修改主机名功能依赖UniAgent，如果提示未安装UniAgent或者安装失败，请参考[为ECS安装UniAgent](#)进行安装，否则无法修改主机名。

批量操作多台ECS时，修改后的名称或主机名相同。

图 2-168 修改主机名

修改主机名

1 如果执行过程中遇到权限问题，请确认是否已授予对应权限。[查看权限](#)

1 批量修改多台云服务器时，修改后的名称或主机名相同。

以下 2 台云服务器 将执行修改主机名

| 名称   | ID        |
|------|-----------|
| ecs- | 82d00911- |
| ecs- | fac67167- |

总条数: 2 < 1 >

云服务器名称 (可选)

只能由中文字符、英文字母、数字及“\_”、“-”、“.”组成。

主机名 (Hostname) ?

只能由英文字母、数字及“.”、“-”组成，但“.”和“-”不能连续使用或出现在开头和结尾。

表 2-54 修改主机名参数配置

| 参数             | 说明                                                                          |
|----------------|-----------------------------------------------------------------------------|
| 云服务器名称（可选）     | 可选配置，ECS的名称。您可以在修改主机名时同步修改ECS名称，修改后立即生效。<br>只能由中文字符、英文字母、数字及“_”、“-”、“.”组成。  |
| 主机名 (Hostname) | ECS的静态主机名hostname，修改后立即生效。<br>只能由英文字母、数字及“.”、“-”组成，但“.”和“-”不能连续使用或出现在开头和结尾。 |

5. 单击“确定”，完成ECS主机名的修改。

## 后续操作

您可以登录云服务器执行以下命令，验证主机名的修改是否生效。

**hostname**

如果回显的内容是修改后的主机名（new\_hostname），则表示主机名修改成功。

## 2.7.5 修改 ECS 名称

### 操作场景

弹性云服务器创建成功后，您可以根据需求，修改云服务器的名称。

系统支持批量修改多台弹性云服务器的名称，修改完成后，这些弹性云服务器的名称相同。

### 修改单台弹性云服务器名称

1. 登录管理控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”。
4. 将鼠标移动至目标云服务器的“名称/ID”列。
5. 单击弹性云服务器名称右方的“”，根据界面提示，修改云服务器名称。  
允许重名：勾选后，允许修改后的名称与其他云服务器名称相同。如果未勾选，且设置的名称与其他云服务器名称相同，此时，系统将提示您该名称已被使用，您需要更换其他名称。
6. 单击，新名称生效。

### 批量修改弹性云服务器的名称

1. 登录管理控制台。
  2. 单击管理控制台左上角的 ，选择区域和项目。
  3. 单击“”，选择“计算 > 弹性云服务器”。
  4. 勾选待修改名称的弹性云服务器。
  5. 单击云服务器列表页上方的“更多 > 修改名称”。
  6. 设置新名称。
  7. 单击“确定”。
- 批量修改云服务器时，修改后的云服务器名称相同，如全部为ecs-test。

## 2.7.6 将 ECS 迁移至专属主机

### 操作场景

云平台支持弹性云服务器在专属主机与公共资源池之间迁移。

在控制台的“弹性云服务器”页面，您可以将公共资源池的弹性云服务器迁移至专属主机，成为专属主机上的弹性云服务器。

本章节介绍公共资源池的弹性云服务器迁移至专属主机的操作指导。

#### 说明

- 迁移云服务器需保证有可用的专属主机资源，否则无法进行迁移操作。
- 在控制台的“专属主机”页面还可以进行如下两个场景的迁移操作，具体请参见《专属主机用户指南》的“[专属主机上云服务器迁移](#)”章节：
  - 创建在专属主机上的弹性云服务器迁移至其他专属主机。
  - 创建在专属主机上的弹性云服务器迁移至公共资源池。

## 约束与限制

- 仅支持将按需计费的弹性云服务器迁移至专属主机。
- 关机状态的弹性云服务器才能执行迁移操作。
- 仅当有可用的专属主机资源时，迁移操作才能成功。
- 云备份或云服务器备份不受迁移影响。
- 迁移后云服务器ID保持不变。

## 操作步骤

1. 登录管理控制台。
2. 单击管理控制台左上角的，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”。
4. 在待迁移的弹性云服务器的“操作”列下，单击“更多 > 运维与监控 > 调整所属主机”。
5. 在“调整所属主机”页面中，选择对应的专属主机。

#### 说明

如果无可选择的专属主机，需先完成专属主机资源的创建，详细内容，请参见[购买专属主机](#)。

6. 单击“确定”，将公共资源池的弹性云服务器迁移至专属主机。

## 2.7.7 跨可用区迁移 ECS

### 操作场景

迁移中心MgC支持主机一站式跨可用区迁移，无需手动采集、分组和评估，一站式解决创建工作流前所有步骤。ECS可以使用主机一站式跨可用区迁移功能实现跨可用区迁移。

本章节介绍在控制台的“弹性云服务器”页面配置ECS跨可用迁移的操作指导。

### 前提条件

已完成“简单项目”创建，项目创建方法请参考[项目管理](#)。

约束与限制

- 不支持迁移系统盘超过1T的服务器。
- 不支持迁移处于“保留期”且为冻结状态的服务器。
- 每台主机只能被一个工作流迁移。
- 迁移工作流创建后，不能关闭或者重启源端主机，不能变更源端磁盘，否则会导致迁移失败，需要重新迁移。
- Linux主机迁移后目的端密码与源端服务器保持一致，Windows主机迁移后目的端密码无法保证与源端服务器一致，详情请参考[AZ迁移注意事项](#)。

更多约束限制请参考[跨AZ迁移约束与限制](#)。

操作步骤

- 登录管理控制台，进入[弹性云服务器](#)列表页面。
- 在待迁移的弹性云服务器的“操作”列下，单击“更多 > 运维与监控 > 跨可用区迁移”。
- 在弹出的“一站式跨可用区迁移”窗口，根据界面提示信息完成相关参数配置。

表 2-55 配置信息

| 参数    | 说明                  |
|-------|---------------------|
| 应用名称  | 用户自定义               |
| 区域    | 待迁移ECS所属区域          |
| 源端可用区 | 待迁移ECS所属可用区。        |
| 目的可用区 | 待迁移ECS需要迁移到的目的端可用区。 |

- 单击“开始执行”，启动主机信息采集，应用关联和迁移评估。

说明

一站式跨可用区迁移会自动采集当前账号所选区域下源端可用区中的所有主机信息，并将采集到的所有主机加入已创建的应用中，同时对应用中关联的所有主机进行迁移评估。

- 评估执行完成后，关闭“一站式跨可用区迁移”窗口。

说明

如果源端可用区中仅存在待迁移ECS，则在评估执行完成后，单击“一站式跨可用区迁移”窗口的“创建迁移工作流”，根据界面提示信息配置并启动迁移工作流，详细信息请参考[创建跨可用区迁移工作流](#)。后续步骤无需执行。

- 修改应用中待迁移的主机列表。
  - 在迁移中心左侧导航栏选择“调研 > 应用管理”，进入“应用管理”页面。
  - 在“应用列表”中，单击应用名称，进入“应用详情”页面。
  - 单击“主机”页签，在主机列表中，勾选不需要跨可用区迁移的主机，单击列表上方的“批量取消关联”。
  - 弹出“取消关联应用”页面，确认无误后单击“确定”。

7. 手动创建可用区迁移工作流。  
详细操作步骤，请参考[创建跨可用区迁移工作流](#)。

## 2.7.8 管理云服务器组

### 操作场景

云服务器组是对云服务器的一种逻辑划分，云服务器组中的弹性云服务器遵从同一策略。

当前云服务器组支持以下策略：

- **反亲和性**：同一云服务器组中的弹性云服务器分散地创建在不同的主机上，提高业务的可靠性。  
使用反亲和性策略可以将业务涉及到的云服务器分散部署在不同的物理服务器上，以此保证业务的高可用性和底层容灾能力。
- **故障域**：同一云服务器组中分布多个故障域，指定不同故障域可以实现云服务器的故障隔离，提高业务的可靠性。  
使用故障域策略可以将业务涉及到的云服务器分散部署在不同的故障域中，以此保证业务的高可用性和底层容灾能力。

云服务器组支持以下操作：

- [创建云服务器组](#)
- [添加云服务器到云服务器组](#)
  - 在创建弹性云服务器时，将弹性云服务器加入云服务器组。  
详细操作，请参考[自定义购买ECS](#)。
  - 在弹性云服务器创建成功后，添加到云服务器组。  
仅支持添加到反亲和性策略组，不支持添加到故障域策略组。
- [从云服务器组移出云服务器](#)
- [删除云服务器组](#)

### 约束与限制

- 同一个云服务器仅支持添加至同一种策略的一个云服务器组。
- “故障域”策略云服务器组仅在部分区域上线，使用时请以该区域实际支持能力为准。
- 云服务器置放层级：
  - 反亲和性策略云服务器组中，云服务器置放层级为物理机层级。
  - 故障域策略云服务器组中，云服务器置放层级为机架层级。
- “故障域”策略的云服务器组，不支持“添加云服务器”操作，仅支持在创建云服务器时选择“故障域策略”的云服务器组。  
详细操作，请参考[自定义购买ECS](#)。
- “反亲和性”策略的云服务器组，支持“添加云服务器”操作，您可以将“运行中”或“关机”状态的云服务器添加至云服务器组。
- “运行中”状态的云服务器加入云服务器组后，无需重启。
- “关机”状态的云服务器在加入云服务器组过程中，不可对云服务器进行开机操作。

- 若添加“运行中”状态的云服务器至云服务器组失败，可关机后重试。
- 添加云服务器到“反亲和性”云服务器组后，可能会重新分配主机。再次开机时可能会由于基础资源不足无法正常开机，请移出云服务器组后重试。
- 创建的云服务器组个数上限可调整，请联系客服扩大配额。
- 不同区域每个云服务器组最多支持添加的云服务器个数各不相同，请在云服务器组列表页查看可添加的云服务器个数。如图2-169所示。

图 2-169 查看可添加的云服务器数量



创建云服务器组

您可以申请创建一个云服务器组，同一云服务器组中的弹性云服务器遵从相同策略，云服务器组与云服务器组之间没有关联关系。

1. 登录管理控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”。
4. 在左侧导航树中，选择“弹性云服务器 > 云服务器组”。
5. 在“云服务器组”页面，单击“创建云服务器组”。
6. 输入云服务器组的名称。
7. 选择云服务器组的策略。
  - 反亲和性：同一云服务器组中的弹性云服务器分散地创建在不同的主机上，提高业务的可靠性。  
使用反亲和性策略可以将业务涉及到的云服务器分散部署在不同的物理服务器上，以此保证业务的高可用性和底层容灾能力。
  - 故障域：同一云服务器组中分布多个故障域，指定不同故障域可以实现云服务器的故障隔离，提高业务的可靠性。  
使用故障域策略可以将业务涉及到的云服务器分散部署在不同的故障域中，以此保证业务的高可用性和底层容灾能力。

说明

“故障域”策略仅在部分区域上线，使用时请以该区域实际支持能力为准。

8. 单击“确定”。

添加云服务器到云服务器组

为提升业务可靠性，您可以添加弹性云服务器到云服务器组，添加后，该弹性云服务器与云服务器组中的其他云服务器分散地创建在不同主机上。



## 说明

- 添加云服务器到云服务器组后，会重新分配该云服务器所在的主机，使其与云服务器组中的其他云服务器分散地创建在不同主机上。那么当弹性云服务器再次开机时，可能会出现由于资源不足引起的启动失败，请将云服务器移出云服务器组后重新启动。
- 弹性云服务器包含本地盘（如磁盘增强型、H2型、P1型、P2型）、NVMe SSD本地磁盘（如超高I/O型）、GPU卡（如G3型）、FPGA卡（如fp1型、fp1c型），则无法在创建后加入云服务器组，如需使用云服务器组功能，请在创建时选择云服务器组。

1. 登录管理控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”。
4. 在左侧导航树中，选择“弹性云服务器 > 云服务器组”。
5. 单击“操作”列下的“添加云服务器”。
6. 在“添加云服务器”页面，选择待添加的弹性云服务器。
7. （可选）根据界面提示，为弹性云服务器执行关机操作。

若“运行中”状态的云服务器添加至云服务器组失败，可执行本操作关机。

- a. 单击“操作”列的“关机”。
  - b. 选择“关机方式”。
    - 关机：正常关机。
    - 强制关机：该操作会导致云服务器中未保存的数据丢失，请谨慎操作。
  - c. 单击“是”，完成关机操作。
8. 单击“确定”，将弹性云服务器加入云服务器组。

## 从云服务器组移出云服务器

弹性云服务器从云服务器组移出后，与云服务器组中的其他云服务器不再遵从云服务器组策略。

1. 登录管理控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”。
4. 在左侧导航树中，选择“弹性云服务器 > 云服务器组”。
5. 展开云服务器组，查看云服务器组中包含的弹性云服务器。
6. 单击目标云服务器“操作”列下的“移出云服务器组”。
7. 单击“是”。

将弹性云服务器从云服务器组中移出。

## 删除云服务器组

删除云服务器组会解除组内云服务器的策略约束。

1. 登录管理控制台。

2. 单击管理控制台左上角的 ，选择区域和项目。
3. 单击 “”，选择“计算 > 弹性云服务器”。
4. 在左侧导航树中，选择“弹性云服务器 > 云服务器组”。
5. 单击待删除云服务器组“操作”列下的“删除”。
6. 单击“是”。

## 2.7.9 配置同一 VPC 内 ECS 通过主机名进行通信

对于同一VPC内的弹性云服务器，可以通过主机名称进行通信。此时，您需要配置主机名与IP地址之间的映射关系。较之通过IP地址进行通信，主机名方式进行通信更为方便。

### 约束限制

仅适用于Linux弹性云服务器。

### 操作步骤

假设VPC内共有2台弹性云服务器：ecs-01和ecs-02。通过如下操作，ecs-01和ecs-02可以通过主机名互相通信。

**步骤1** 分别登录ecs-01和ecs-02，获取2台弹性云服务器的私有IP地址。

1. 登录管理控制台。
2. 单击 “”，选择“计算 > 弹性云服务器”。
3. 在弹性云服务器列表页，通过“私有IP地址”栏，查看弹性云服务器的私有IP地址。

【示例】假设查询的私有IP地址如下：

ecs-01: 192.168.0.1

ecs-02: 192.168.0.2

**步骤2** 分别获取2台弹性云服务器的主机名。

1. 登录弹性云服务器。
2. 执行以下命令，查询弹性云服务器的主机名。

```
sudo hostname
```

【示例】假设查询的主机名如下：

ecs-01: hostname01

ecs-02: hostname02

**步骤3** 建立主机名与IP地址之间的映射关系，并添加同一VPC内其他弹性云服务器的信息。

1. 登录弹性云服务器ecs-01。
2. 执行以下命令，切换至root权限。

```
sudo su -
```

3. 执行以下命令，编辑hosts文件。

```
vi /etc/hosts
```

- 按“i”，进入编辑模式。
- 按照如下格式添加语句，建立映射关系。  
*私有IP地址 主机名*  
【示例】需添加的语句为：  
192.168.0.1 hostname01  
192.168.0.2 hostname02
- 按“Esc”退出编辑模式。
- 执行以下命令，保存并退出。  
**:wq**
- 登录ecs-02。
- 重复执行[步骤3.2](#)~[步骤3.7](#)。

#### 步骤4 测试验证能否通过主机名正常通信。

分别登录同一VPC内的弹性云服务器，执行以下命令，使用ping命令ping添加的主机，看ping包是否能正常送达。

**ping *hostname***

----结束

## 2.7.10 启、停弹性云服务器

在弹性云服务器的使用过程中，您可以进行开机、关机、重启或删除/退订等操作。

- 大量弹性云服务器同时开机或关机时，会加重主机的负载。如果需要同时对大量弹性云服务器执行开机或关机操作，建议分批进行，避免对其他弹性云服务器的业务造成影响。
- 重启/关机弹性云服务器时，如果弹性云服务器长时间处于“正在重启”/“正在关机”状态，可以执行强制重启/强制关机操作。强制重启/强制关机操作会导致弹性云服务器中未保存的数据丢失，请谨慎操作。

#### 说明

对于裸金属类型的规格实例（规格名称中包含physical），请勿通过操作系统的shutdown，poweroff，half等命令进行操作，可能会导致命令无效或关机后无法启动。

## 开机

- 登录管理控制台。
- 单击管理控制台左上角的，选择区域和项目。
- 选择“计算 > 弹性云服务器”。
- 在弹性云服务器列表中，勾选需要进行操作的弹性云服务器实例。
- 单击弹性云服务器列表左上角的“开机”。
- 参考界面提示信息，单击“确定”，完成弹性云服务器的“开机”操作。

#### 说明

如果弹性云服务器处于“开机中”中间状态超过30分钟，则说明出现异常，需要联系管理员处理。

关机

1. 登录管理控制台。
2. 单击管理控制台左上角的，选择区域和项目。
3. 选择“计算 > 弹性云服务器”。
4. 在弹性云服务器列表中，勾选需要进行操作的弹性云服务器实例。
5. 单击弹性云服务器列表左上角的“关机”。

图 2-170 关机



6. 在“关机”页面，您可以根据需要选择“关机方式”。  
在当前页面，您还可以查看按需计费的弹性云服务器关机计费策略，更多内容，请参见[关机计费策略](#)。

须知

“强制关机”方式会导致云服务器中未保存的数据丢失，请谨慎操作。

7. 单击“确定”，完成弹性云服务器的“关机”操作。

说明

如果弹性云服务器处于“关机中”中间状态超过30分钟，则说明出现异常，需要联系管理员处理。

重启

1. 登录管理控制台。
2. 单击管理控制台左上角的，选择区域和项目。

- 3. 选择“计算 > 弹性云服务器”。
- 4. 在弹性云服务器列表中，勾选需要进行操作的弹性云服务器实例。
- 5. 单击弹性云服务器列表左上角的“更多 > 重启”。

图 2-171 重启



须知

勾选“强制重启”会导致云服务器中未保存的数据丢失，请谨慎操作。

- 6. 单击“确定”，完成弹性云服务器的“重启”操作。

说明

如果弹性云服务器处于“重启中”或“强制重启中”中间状态超过30分钟，则说明出现异常，需要联系管理员处理。

删除/退订

- 1. 登录管理控制台。
- 2. 单击管理控制台左上角的，选择区域和项目。
- 3. 选择“计算 > 弹性云服务器”。
- 4. 在弹性云服务器列表中，勾选需要进行操作的弹性云服务器实例。
- 5. 单击弹性云服务器列表左上角的“更多 > 删除”或“更多 > 退订”。
  - 删除按需计费的弹性云服务器。

图 2-172 删除

删除

1 删除设置

2 资源明细

3 完成

以下1台云服务器，可直接删除

已开启云备份的云服务器在删除后，云备份会保留并继续计费，您可以前往云备份页面进行删除操作。

| 名称      | ID                |
|---------|-------------------|
| ecs-... | 07a25ce1-dc9e-... |

删除方式

☒ 立即删除

☐ 定时删除

是否同步删除关联资源

未勾选的弹性公网IP和数据盘不会随云服务器同步删除，会继续计费。

☐ 删除云服务器绑定的弹性公网IP地址

☐ 删除云服务器挂载的数据盘

取消

下一步

- i. 选择“删除方式”。
  - 立即删除：立即删除弹性云服务器。
  - 定时删除：在设置的“删除时间”删除弹性云服务器。
- 说明

仅部分区域支持删除支持方式，请参见[功能总览](#)。  
定时删除任务时间设置不可小于当前时间1小时。  
系统每5分钟执行一次定时删除任务，按照系统删除服务器的时间停止计费。
- ii. （可选）勾选“删除云服务器绑定的弹性公网IP地址”和“删除云服务器挂载的数据盘”，同步删除弹性云服务器绑定的资源。  
当“删除方式”选择“立即删除”时，该参数可见。
- iii. （可选）单击“下一步”，确认删除的资源明细。  
当“删除方式”选择“立即删除”时，该参数可见。
- iv. （可选）确认删除资源明细后，输入“DELETE”。  
当“删除方式”选择“立即删除”时，该参数可见。
- v. 单击“确定”，完成弹性云服务器的“删除”操作。
- 退订包年/包月的弹性云服务器。

图 2-173 退订

退订

确定要对以下1台云服务器进行退订操作吗？

| 名称      | 状态  | 备注 |
|---------|-----|----|
| ecs-... | 运行中 | -- |

取消

确定

- i. 单击“是”，跳转至费用中心的“退订资源”页面。
- ii. 根据界面提示，勾选需要退订的资源，并选择退订原因。
- iii. 确认退订信息无误后，勾选“资源退订后……”提示信息。
- iv. 单击“退订”，再次根据界面信息确认要退订的资源。
- v. 再次单击“退订”，完成包年/包月资源的退订操作。

#### 说明

如果弹性云服务器处于“正在删除”中间状态超过30分钟，则说明出现异常，需要联系管理员处理。

## 2.8 变更 ECS 规格（vCPU 和内存）

### 2.8.1 变更单台 ECS 规格

#### 操作场景

当您购买的弹性云服务器规格无法满足业务需要时，可参考本章节变更规格，升级 vCPU、内存。对于部分类型的弹性云服务器，您还可以在变更规格时，更换弹性云服务器的类型。

- “XEN实例”变更为“KVM实例”，需先手动配置弹性云服务器，安装对应的驱动，然后再变更规格。否则，规格变更后的弹性云服务器不可用（操作系统可能无法启动）。“XEN实例”变更为“KVM实例”操作指引如下。Linux操作系统优先推荐使用自动配置的方法变更规格。
  - [XEN实例变更为KVM实例（Windows）](#)
  - [XEN实例变更为KVM实例（Linux-自动配置）](#)
  - [XEN实例变更为KVM实例（Linux-手动配置）](#)
  - [XEN实例变更为KVM实例（Linux-批量自动配置）](#)
- “KVM实例”变更为“QingTian实例”，磁盘盘符及驱动依赖会发生变化，请先确认启动依赖项及驱动情况，然后再变更规格。否则，规格变更后的弹性云服务器不可用（操作系统可能无法启动），“KVM实例”变更为“QingTian实例”操作指引如下。
  - [KVM实例变更为QingTian实例（Windows）](#)
  - [KVM实例变更为QingTian实例（Linux）](#)
- 对于其他类型弹性云服务器的规格变更（例如“KVM实例”变更为“KVM实例”），请直接参见本节内容。

## 说明

- 弹性云服务器的实例包括：
  - XEN实例：S1、C1、C2、M1型弹性云服务器。
  - KVM实例：参考[规格清单](#)，查询对应规格的虚拟化类型。
  - QingTian实例：C7型弹性云服务器、M7型弹性云服务器、C6（支持KVM和QingTian虚拟化类型）型弹性云服务器。
- 不同弹性云服务器实例的变更原则：
  - 支持将“KVM实例”变更为“QingTian实例”。
  - 不支持将“QingTian实例”变更为“KVM实例”。
  - 不支持将“XEN实例”变更为“QingTian实例”。
- “XEN实例”变更为“KVM实例”必须先安装对应的驱动，然后再变更规格。否则，规格变更后的弹性云服务器不可用（如操作系统无法启动等问题）。
- Linux操作系统的“XEN实例”变更为“KVM实例”时，优先推荐使用[XEN实例变更为KVM实例（Linux-自动配置）](#)。

## 变更须知

- 变更规格过程中，弹性云服务器需要关机，建议您选择业务空闲时间进行操作。
- 变更规格过程中，不要对弹性云服务器做任何操作，例如关机、重启等，否则会导致变更规格失败。
- 变更弹性云服务器规格时，用户不能选择已售罄的CPU和内存资源。
- 弹性云服务器规格（CPU或内存）变小，会影响弹性云服务器的性能。
- 对于部分类型的弹性云服务器，暂不支持规格变更操作。[实例类型](#)章节列举了提供的云服务器类型，并对每种云服务器类型的功能、使用进行介绍，具体请以各类型云服务器的“使用须知”为准。
- 当云硬盘状态为“正在扩容”时，不支持变更所挂载的弹性云服务器规格。
- Windows操作系统的弹性云服务器，执行变更规格操作前建议您参考[磁盘脱机怎么办？](#)修改Windows操作系统SAN策略，避免变更规格后磁盘处于脱机状态。
- Windows 2016操作系统的弹性云服务器，执行变更操作前建议您参考[为什么Windows 2016操作系统的云服务器实例变更到C7规格后蓝屏？](#)修改注册表信息，避免变更规格后出现蓝屏。
- 使用了收费镜像的包年/包月模式的弹性云服务器，无法进行规格降配，即不支持变更到费用更低的规格。

## 费用说明

变更规格会引起费用的变化，具体费用说明请参见[变更资源费用说明](#)。

## 变更前准备

变更规格后，可能会出现网卡漂移现象，请在变更规格前做如下操作：

## 说明

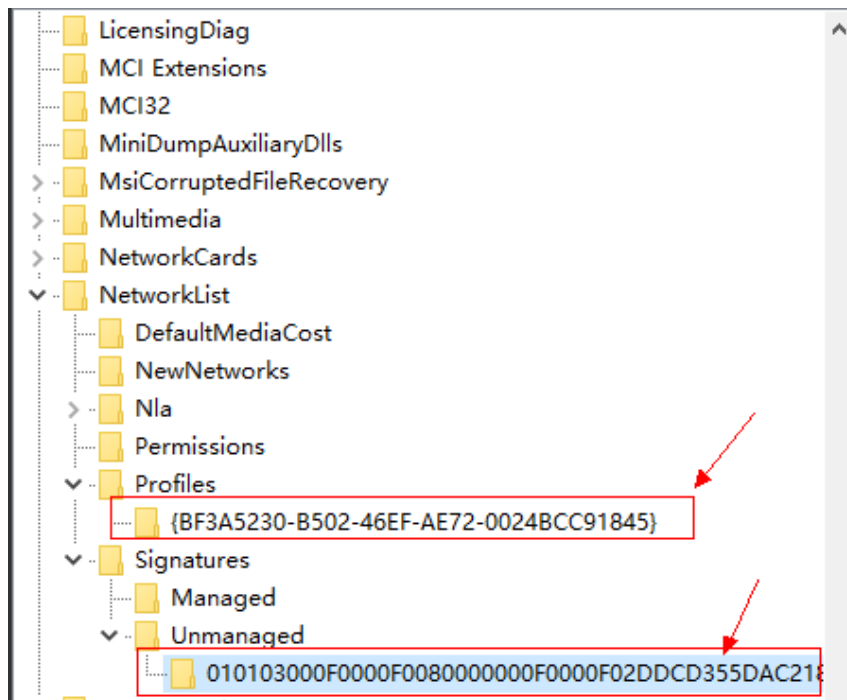
出现网卡漂移的现象，是由于创建云服务器使用的镜像的操作系统中打开了网卡保留规则，才导致该云服务器变更规格后出现网卡漂移。

关于网卡漂移的更多信息，请参见[弹性云服务器变更规格后网卡漂移怎么办？](#)。



- Linux系统：  
在云服务器中执行以下命令，删除网络规则目录下，文件名同时包含**persistent**和**net**的规则文件  
**rm -fr /etc/udev/rules.d/\*net\*persistent\*.rules**  
**rm -fr /etc/udev/rules.d/\*persistent\*net\*.rules**
- Windows系统：  
在云服务器中删除如下注册表下的目录。  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion  
\NetworkList\Profiles  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion  
\NetworkList\Signatures\Unmanaged

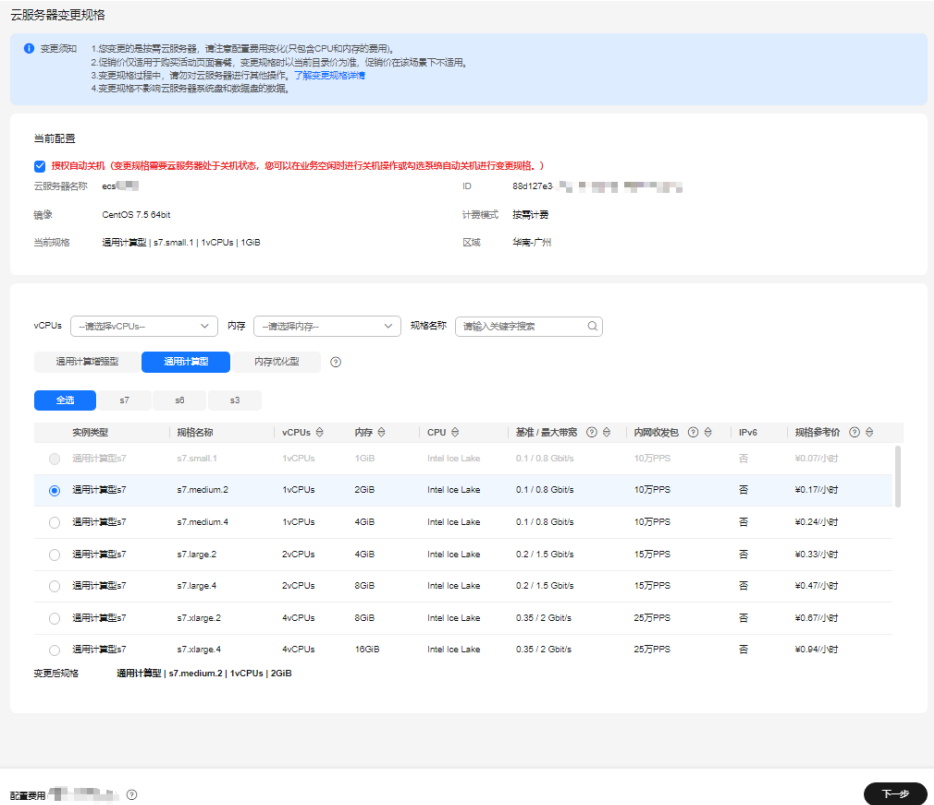
图 2-174 注册表



## 步骤 1：变更规格

1. 登录管理控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”。
4. 单击“操作”列下的“更多 > 变更规格”。
- 系统进入“云服务器变更规格”页面。
5. 根据界面提示，选择变更后的弹性云服务器类型、vCPU和内存。
- 变更规格前请先将云服务器关机，或根据页面提示勾选“授权自动关机”。

图 2-175 变更规格



6. （可选）选择“专属主机”。
- 对于在专属主机上创建的弹性云服务器，系统支持更换云服务器所在的专属主机。
- 请展开下拉列表，选择更换的专属主机。如果下拉列表中无可用的专属主机，说明所剩资源不足，不能用于创建变更规格后的弹性云服务器。
7. （可选）勾选“指定CPU选项”。
- 当需要为云服务器实例开启或关闭超线程时，勾选“指定CPU选项”。
- 关于超线程的详细介绍，请参见[开启/关闭ECS超线程](#)。
8. （可选）设置“每核心线程数”。
- 当勾选“指定CPU选项”时，显示该参数。在“每核心线程数”下拉框进行设置。
- 1：关闭超线程
  - 2：开启超线程，默认开启
9. 单击“下一步”。
10. （可选）根据界面提示，检查并修改磁盘标识方式为UUID。
- 当变更的目标规格为QingTian规格时，显示该提示界面。
- 更多内容，请参见[KVM实例变更为QingTian实例（Linux）](#)和[KVM实例变更为QingTian实例（Windows）](#)。
11. 确认变更后的配置无误后，阅读并勾选同意服务协议，单击“提交申请”。
12. 查询规格是否变更成功。
- 申请变更规格后，可以通过“异常任务”栏查看规格是否变更成功。

- a. 查看控制台是否显示“异常任务”栏，查看操作请参见[查看ECS失败任务](#)。
  - 是，执行12.b。
  - 否，变更规格成功。
- b. 打开“异常任务”，根据弹性云服务器的“名称/ID”、“操作时间”和“任务”，确认列表中是否有刚刚执行的变更规格任务。
  - 是，变更规格失败，失败原因请参见[后续处理](#)。
  - 否，变更规格成功。

## 步骤 2：检查磁盘挂载状态

变更规格时，可能会发生磁盘挂载失败的情况，因此，变更规格后，需检查磁盘挂载状态是否正常。如果正常，则变更成功。

- Windows弹性云服务器  
详细操作请参考[Windows云服务器变更规格后数据盘脱机怎么办？](#)
- Linux弹性云服务器  
详细操作请参考[Linux云服务器变更规格后数据盘脱机怎么办？](#)

## 后续处理

如果变更规格失败，请到云审计页面查看失败原因。具体操作如下：

1. 登录管理控制台。
2. 选择“管理与监管 > 云审计服务”。
3. 在左侧导航栏，选择“云审计 > 事件列表”。
4. 在“事件名称”栏，根据“资源ID”查找到名称为“resizeServer”的规格变更失败事件。  
其中，“资源ID”为规格变更失败的弹性云服务器ID。
5. 单击“操作”列下的“查看事件”，查看失败原因。  
如果无法根据日志解决问题，可联系客服。

## 2.8.2 批量变更多台 ECS 规格

### 操作场景

当您购买的多台弹性云服务器的规格无法满足业务需要时，可以参考本章节批量变更规格，升级vCPU、内存。

不同计费模式弹性云服务器的批量变更规格操作不同，本文将分别进行介绍：

- [操作步骤（按需计费）](#)
- [操作步骤（包年/包月）](#)

### 约束与限制

- 变更规格过程中，弹性云服务器需要关机，建议您选择业务空闲时间进行操作。

- 变更规格过程中，不要对弹性云服务器做任何操作，例如关机、重启等，否则会导致变更规格失败。
- 批量变更规格操作仅支持对相同可用区、相同计费模式以及相同规格的弹性云服务器实例进行变更。
- 变更规格时，不能选择已售罄的CPU和内存资源。
- 弹性云服务器规格（CPU或内存）变小，会影响弹性云服务器的性能。
- 对于部分类型的弹性云服务器，暂不支持规格变更操作。[实例类型](#)章节列举了提供的云服务器类型，并对每种云服务器类型的功能、使用进行介绍，具体请以各类型云服务器的“使用须知”为准。
- 当云硬盘状态为“正在扩容”时，不支持变更所挂载的弹性云服务器规格。
- Windows操作系统的弹性云服务器，执行变更规格操作前建议您参考[磁盘脱机怎么办？](#)修改Windows操作系统SAN策略，避免变更规格后磁盘处于脱机状态。
- Windows 2016操作系统的弹性云服务器，执行变更操作前建议您参考[为什么Windows 2016操作系统的云服务器实例变更到C7规格后蓝屏？](#)修改注册表信息，避免变更规格后出现蓝屏。

## 费用说明

变更规格会引起费用的变化，具体费用说明请参见[变更资源费用说明](#)。

## 变更前准备

变更规格后，可能会出现网卡漂移现象，请在变更规格前做如下操作：

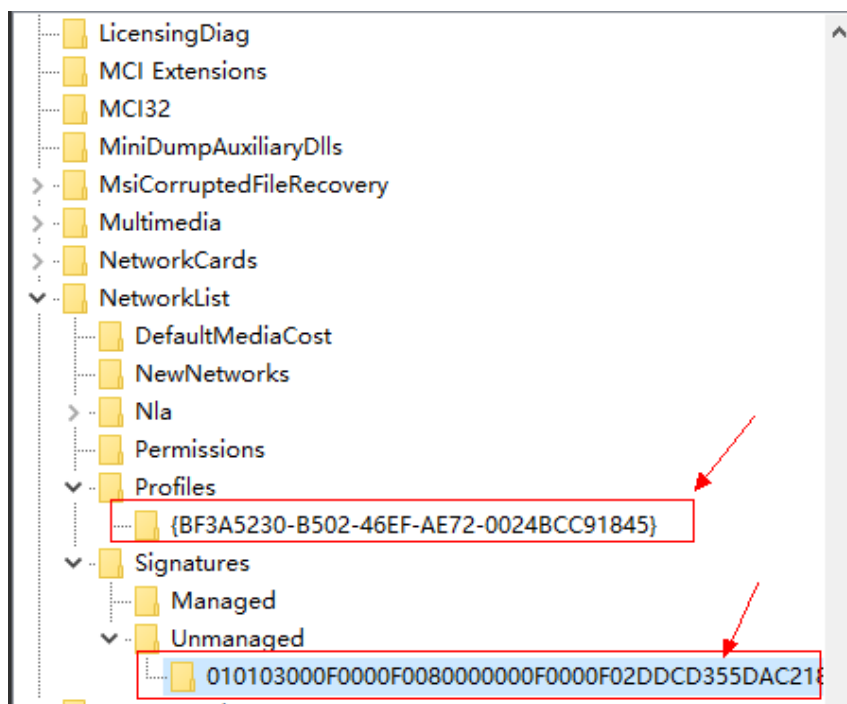
### 说明

出现网卡漂移的现象，是由于创建云服务器使用的镜像的操作系统中打开了网卡保留规则，才导致该云服务器变更规格后出现网卡漂移。

关于网卡漂移的更多信息，请参见[弹性云服务器变更规格后网卡漂移怎么办？](#)。

- Linux系统：  
在云服务器中执行以下命令，删除网络规则目录下，文件名同时包含**persistent**和**net**的规则文件  
**rm -fr /etc/udev/rules.d/\*net\*persistent\*.rules**  
**rm -fr /etc/udev/rules.d/\*persistent\*net\*.rules**
- Windows系统：  
在云服务器中删除如下注册表下的目录。  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged

图 2-176 注册表

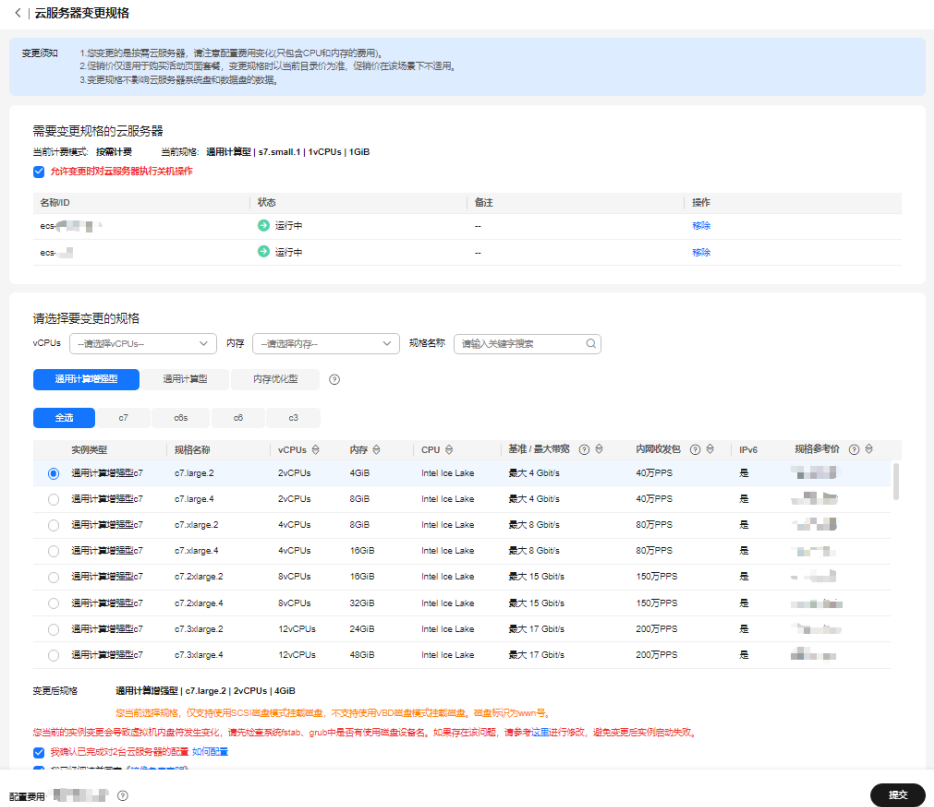


## 操作步骤（按需计费）

### 批量变更规格

1. 登录管理控制台。
  2. 单击管理控制台左上角的 ，选择区域和项目。
  3. 单击“”，选择“计算 > 弹性云服务器”。
  4. 勾选待变更的弹性云服务器实例，单击列表上方的“更多 > 变更规格 > 按需云服务器规格变更”。
- 系统进入“云服务器变更规格”页面。
5. 根据界面提示，选择变更后的弹性云服务器类型、vCPU和内存。
- 变更规格前请先将云服务器关机，或根据页面提示勾选“立即关机”。

图 2-177 批量变更规格（按需计费）



6. （可选）根据界面提示，检查并修改云服务器系统的fstab、grub，修改完成后勾选“我确认已完成对弹性云服务器的配置”。
7. 确认变更后的配置无误后，阅读并勾选同意服务协议，单击“提交”。
8. 查询规格是否变更成功。  
申请变更规格后，可以通过“异常任务”栏查看规格是否变更成功。

a. 查看控制台是否显示“异常任务”栏，查看操作请参见[查看ECS失败任务](#)。

是，执行8.b。

否，变更规格成功。

b. 打开“异常任务”，根据弹性云服务器的“名称/ID”、“操作时间”和“任务”，确认列表中是否有刚刚执行的变更规格任务。

是，变更规格失败，失败原因请参见[后续处理](#)。

否，变更规格成功。

检查磁盘挂载状态

变更规格时，可能会发生磁盘挂载失败的情况，因此，变更规格后，需检查磁盘挂载状态是否正常。如果正常，则变更成功。

Windows弹性云服务器

详细操作请参考[Windows云服务器变更规格后数据盘脱机怎么办？](#)

Linux弹性云服务器

详细操作请参考[Linux云服务器变更规格后数据盘脱机怎么办？](#)

文档版本 01 (2025-06-13)

版权所有 © 华为云计算技术有限公司

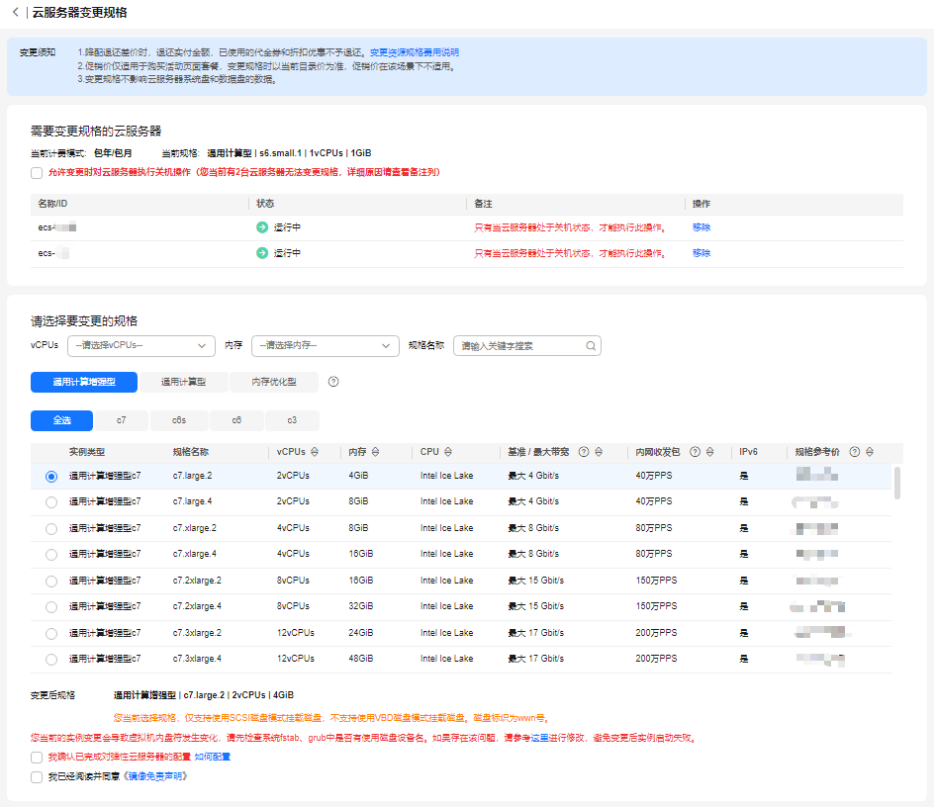
222

操作步骤（包年/包月）

批量变更规格

1. 登录管理控制台。
2. 单击管理控制台左上角的，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”。
4. 勾选待变更的弹性云服务器实例，单击列表上方的“更多 > 变更规格 > 包年/包月云服务器规格变更”。
- 系统进入“云服务器变更规格”页面。
5. 根据界面提示，选择变更后的弹性云服务器类型、vCPU和内存。
- 变更规格前请先将云服务器关机，或根据页面提示勾选“立即关机”。

图 2-178 批量变更规格（包年/包月）



6. （可选）根据界面提示，检查并修改云服务器系统的fstab、grub，修改完成后勾选“我确认已完成对弹性云服务器的配置”。
7. 确认变更后的配置无误后，阅读并勾选同意服务协议，单击“提交申请”。
8. 查询规格是否变更成功。
- 申请变更规格后，可以通过“异常任务”栏查看规格是否变更成功。
- a. 查看控制台是否显示“异常任务”栏，查看操作请参见查看ECS失败任务。
- 是，执行8.b。
  - 否，变更规格成功。



- b. 打开“异常任务”，根据弹性云服务器的“名称/ID”、“操作时间”和“任务”，确认列表中是否有刚刚执行的变更规格任务。
  - 是，变更规格失败，失败原因请参见[后续处理](#)。
  - 否，变更规格成功。

### 检查磁盘挂载状态

变更规格时，可能会发生磁盘挂载失败的情况，因此，变更规格后，需检查磁盘挂载状态是否正常。如果正常，则变更成功。

- Windows弹性云服务器  
详细操作请参考[Windows云服务器变更规格后数据盘脱机怎么办？](#)
- Linux弹性云服务器  
详细操作请参考[Linux云服务器变更规格后数据盘脱机怎么办？](#)

## 后续处理

如果变更规格失败，请到云审计页面查看失败原因。具体操作如下：

1. 登录管理控制台。
2. 选择“> 云审计服务”。
3. 在左侧导航栏，选择“云审计 > 事件列表”。
4. 在“事件名称”栏，根据“资源ID”查找到名称为“resizeServer”的规格变更失败事件。  
其中，“资源ID”为规格变更失败的弹性云服务器ID。
5. 单击“操作”列下的“查看事件”，查看失败原因。  
如果无法根据日志解决问题，可联系客服。

## 2.8.3 通过性能助手变更 ECS 规格

### 操作场景

弹性云服务器支持性能助手功能，实时检测云服务器的CPU负载情况。当云服务器的CPU负载超过阈值时，会提示您调整配置，并提供推荐规格。

触发“调整配置”提醒的阈值为：云服务器在最近72小时内，开机时间超过36小时，且“CPU使用率”的中位数超过75%。

关于监控指标“CPU使用率”的详细描述，请参见[弹性云服务器支持的基础监控指标](#)。

本章节介绍当云服务器CPU偏高、超过阈值时，系统提示调整配置时的操作指导。

### 变更须知

- 当云服务器状态为“已冻结”时，不支持变更规格。
- 变更规格过程中，弹性云服务器需要关机，建议您选择业务空闲时间进行操作。
- 变更弹性云服务器规格时，用户不能选择已售罄的CPU和内存资源。
- 弹性云服务器规格（CPU或内存）变小，会影响弹性云服务器的性能。



- 对于部分类型的弹性云服务器，暂不支持规格变更操作。[实例类型](#)章节列举了提供的云服务器类型，并对每种云服务器类型的功能、使用进行介绍，具体请以各类型云服务器的“使用须知”为准。

费用说明

变更规格会引起费用的变化，具体费用说明请参见[变更资源费用说明](#)。

操作步骤

- 登录管理控制台。
- 单击管理控制台左上角的，选择区域和项目。
- 单击“”，选择“计算 > 弹性云服务器”。
- 查看弹性云服务器列表，若云服务器CPU负载偏高，会出现如下提示。

图 2-179 云服务器列表上方提示信息

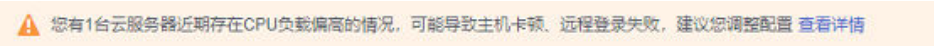


图 2-180 云服务器列表“监控”列提示信息



- 在云服务器列表上方提示信息中，单击“查看详情”，显示“调整配置建议”页面，包含所有CPU负载偏高，需要调整配置的云服务器。

图 2-181 调整配置建议



- 在待调整配置的云服务器“操作”列，单击“调整配置”，进入“云服务器变更规格”页面。

说明

您也可以在云服务器列表页面，单击如图2-180所示的“”，直接进入该云服务器的“云服务器变更规格”页面。

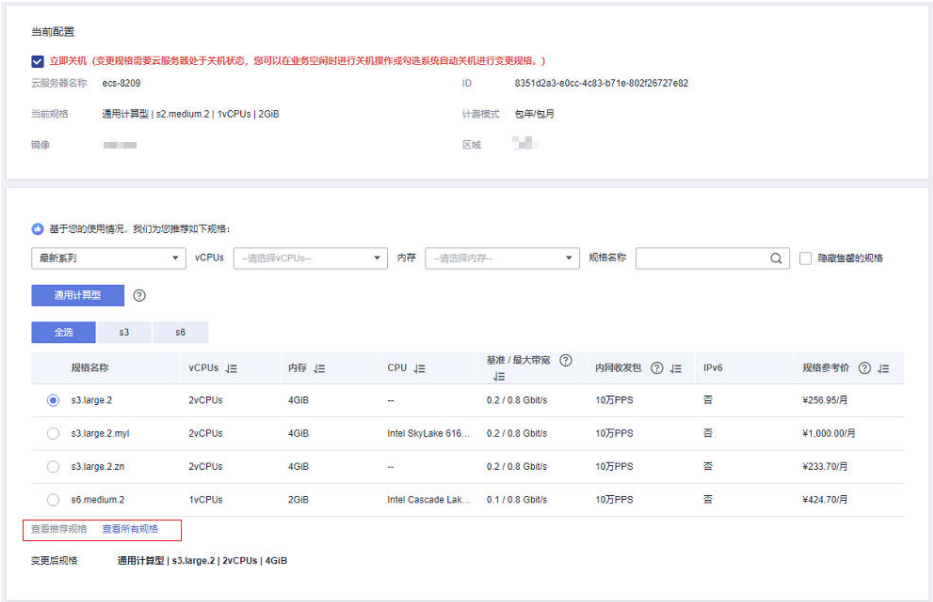
7. 设置变更规格相关参数。
- a. 勾选“立即关机”。

b. 在推荐规格的规格列表中，选择待变更的目标规格。
- 若推荐规格不满足需要，您可以单击“查看所有规格”，切换至完整规格列表页面进行选择。

说明

弹性云服务器规格（CPU或内存）变小，会影响弹性云服务器的性能。

图 2-182 云服务器变更规格



- c. 单击“下一步”。

d. 确认变更后的配置无误后，阅读并勾选“我已阅读《 镜像免责声明 》”，单击“提交订单”。

e. 支付订单，完成云服务器规格的变更。
8. 返回云服务器列表，查询规格是否变更成功。
- a. 在云服务器列表上方的提示信息中单击“查看详情”。

b. 在“调整配置建议”页面，若云服务器“操作”列显示“已调整”，表示云服务器变更规格完成。

2.8.4 XEN 实例变更为 KVM 实例（ Windows ）

操作场景

XEN实例变更为KVM实例前，需要确保Windows弹性云服务器已安装了PV driver和UVP VMTools。

本节指导您安装PV driver和UVP VMTools，将XEN实例变更为KVM实例。

#### 说明

- 弹性云服务器的实例包括：
  - XEN实例：S1、C1、C2、M1型弹性云服务器。
  - KVM实例：参考[规格清单](#)，查询对应规格的虚拟化类型。
  - QingTian实例：C7型弹性云服务器、M7型弹性云服务器、C6（支持KVM和QingTian虚拟化类型）型弹性云服务器。
- 不同弹性云服务器实例的变更原则：
  - 支持将“KVM实例”变更为“QingTian实例”。
  - 不支持将“QingTian实例”变更为“KVM实例”。
  - 不支持将“XEN实例”变更为“QingTian实例”。
- “XEN实例”变更为“KVM实例”必须先安装对应的驱动，然后再变更规格。否则，规格变更后的弹性云服务器不可用（如操作系统无法启动等问题）。
- Linux操作系统的“XEN实例”变更为“KVM实例”时，优先推荐使用[XEN实例变更为KVM实例（Linux-自动配置）](#)。

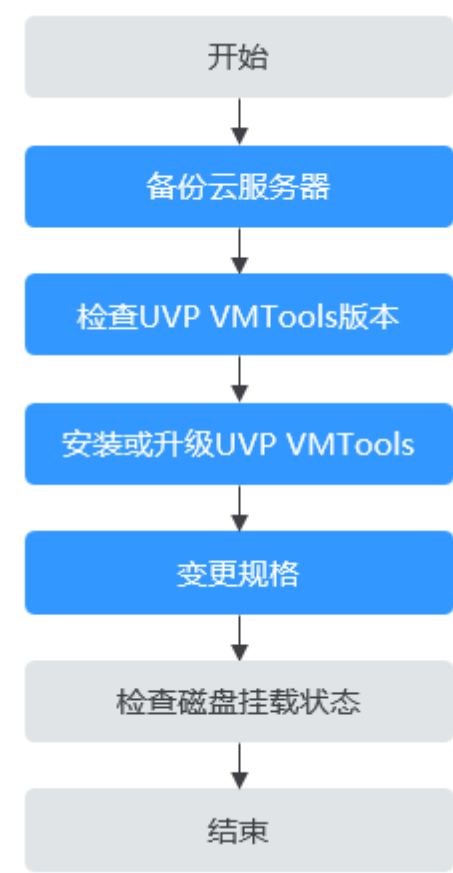
## 约束与限制

- 变更规格过程中，弹性云服务器需要关机，建议您选择业务空闲时间进行操作。
- Windows操作系统云服务器如果存在跨区卷，不支持变更规格，否则可能会导致数据丢失。
- 对于XEN实例，当挂载的VBD磁盘超过24块时，不支持将规格变更为KVM实例。
- 系统支持将“XEN实例”变更为“KVM实例”，不支持将“KVM实例”变更为“XEN实例”。

## 操作流程

XEN实例变更为KVM实例的操作流程如[图2-183](#)所示。

图 2-183 Windows 云服务器变更流程



具体的变更操作如[表2-56](#)所示。

表 2-56 XEN 实例变更为 KVM 实例

| 序号  | 任务                                   |
|-----|--------------------------------------|
| 步骤1 | <a href="#">步骤1：备份云服务器</a>           |
| 步骤2 | <a href="#">步骤2：检查UVP VMTools版本</a>  |
| 步骤3 | <a href="#">步骤3：安装或升级UVP VMTools</a> |
| 步骤4 | <a href="#">步骤4：变更规格</a>             |
| 步骤5 | <a href="#">（可选）步骤5：检查磁盘挂载状态</a>     |

步骤 1：备份云服务器

如果未安装驱动就执行变更规格的操作，云服务器可能无法正常使用，造成您的数据丢失。因此，建议您先备份云服务器，防止数据丢失。

1. 自检云服务器。
- 备份前请对云服务器执行关机、开机操作，确保云服务器重启后业务可以正常运行。

## 2. 备份云服务器。

其中，云服务器备份涉及存储费用；快照分为存量快照及标准快照，存量快照公测不计费，标准快照计费，请按需选择。

- 方式一：创建云服务器备份。

创建云服务器备份的操作，请参见[云服务器备份操作步骤](#)。

- 方式二：创建系统盘快照和数据盘快照。

创建快照的操作，请参见《云硬盘用户指南》的“[创建快照](#)”章节。

### 说明

云服务器的备份和快照用于恢复数据，当变更规格失败回退后，可通过备份或快照进行数据恢复：

- 通过云服务器备份恢复数据，详细操作请参见[使用云服务器备份恢复数据](#)。
- 通过快照回滚数据，详细操作请参见[使用快照回滚数据至云硬盘](#)。

变更规格完成后，如已确认业务恢复正常，请在对应服务控制台页面删除云服务器备份或快照。

## 步骤 2：检查 UVP VMTools 版本

变更规格前请先检查 UVP VMTools 版本。

1. 登录弹性云服务器。
2. 下载驱动检查脚本

下载驱动检查脚本，用管理员权限执行脚本，等待检查结果。

请根据云服务器所在区域选择脚本的下载地址：

- 华东-上海二：[https://cn-east-2-server-resize.obs.cn-east-2.myhuaweicloud.com/windows/server\\_resize/check\\_kvm\\_drivers.vbs](https://cn-east-2-server-resize.obs.cn-east-2.myhuaweicloud.com/windows/server_resize/check_kvm_drivers.vbs)
- 华北-北京一：[https://cn-north-1-server-resize.obs.cn-north-1.myhuaweicloud.com/windows/server\\_resize/check\\_kvm\\_drivers.vbs](https://cn-north-1-server-resize.obs.cn-north-1.myhuaweicloud.com/windows/server_resize/check_kvm_drivers.vbs)
- 华南-广州：[https://cn-south-1-server-resize.obs.cn-south-1.myhuaweicloud.com/windows/server\\_resize/check\\_kvm\\_drivers.vbs](https://cn-south-1-server-resize.obs.cn-south-1.myhuaweicloud.com/windows/server_resize/check_kvm_drivers.vbs)

驱动检查脚本在确认驱动安装成功后会自动为云服务器设置标签，标记驱动安装成功，没有设置标签的云服务器无法执行变更规格的操作。

- 检查结果为“Check version success!”说明驱动版本符合要求，且为云服务器设置标签标记驱动安装成功。您可以执行[步骤4：变更规格](#)。
- 检查结果为“Check version success but set metadata failed! Please run this script again later.”说明驱动版本符合要求，但为云服务器设置标签失败，请稍后重试。
- 检查结果为“Check version failed! Please install drivers at first.”说明驱动版本不符合要求，请参见[步骤3：安装或升级 UVP VMTools](#)安装或升级 UVP VMTools。

## 步骤 3：安装或升级 UVP VMTools

安装或升级 UVP VMTools 时，如果云服务器中已安装 PV Driver，会对其版本进行校验，为了避免在云服务器上安装 UVP VMTools 失败，需确保 PV Driver 版本满足要求。本小节介绍检查安装 PV Driver、UVP VMTools 的操作步骤。

⚠ 注意

安装PV Driver或UVP VMTools前请确保云服务器满足以下条件：

- 云服务器的系统盘的剩余空间必须大于2GB。
- 为了避免在云服务器上安装驱动失败，安装前请先卸载第三方虚拟化平台的工具（例如：Citrix Xen Tools、VMware Tools），相关卸载方法请参考对应的工具的官方文档。
- 禁用防病毒软件或入侵检测软件，您可以在驱动安装完成后，再启用这些软件。

1. 安装前请先检查PV Driver版本是否满足UVP VMTools依赖。  
进入目录“C:\Program Files (x86)\Xen PV Drivers\bin”，打开文件“version.ini”，查看PV driver版本号。

pvdriverVersion=5.0.104.010

- 如果存在目录，且驱动版本高于5.0，表示PV driver已安装且满足版本要求，请执行6安装UVP VMTools。
- 反之，表示PV driver未正常安装或版本不满足要求，请执行以下步骤卸载旧版本PV driver，安装新版本的PV driver。

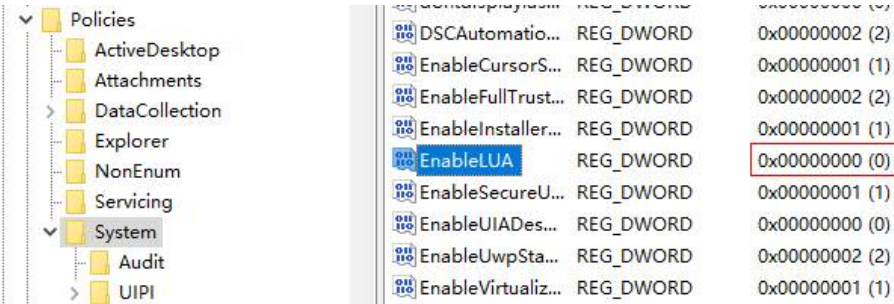
2. 记录当前云服务器的UAC（User Account Control）配置。

📖 说明

PV Driver版本低于5.0时，为实现静默升级功能（防止升级过程中弹窗过多），安装PV Driver时在注册表中加入了Disable LUA操作，卸载PV Driver时在注册表中加入了Enable LUA操作（5.0及以上版本已优化解决此问题）。为避免对您的业务造成影响，如果PV Driver版本低于5.0，请在卸载前先记录UAC配置，并在安装新版本PV Driver后检查并恢复注册表中Enable LUA配置。了解更多UAC配置请参考[微软官方文档](#)。

- a. 打开“运行”窗口，输入“regedit”，打开“注册表编辑器”。
- b. 记录HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA 键值。

图 2-184 EnableLUA



3. 卸载旧版本PV driver。
- a. 在云服务器云主机操作系统界面，选择“开始 > 控制面板”。
- b. 单击“卸载程序”。
- c. 按照提示，卸载“GPL PV Drivers for Windows x.x.x.xx”。
- d. 在控制台重启云服务器。
4. 安装新版本PV driver。
- a. 下载PV Driver的安装包。



PV Driver下载地址：<https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/pvdriver-windows.zip>

- b. 解压PV driver软件包。
- c. 双击“pvdriver-windows.iso”。
- d. 运行“Setup.exe”，根据界面提示安装PV Driver。  
请耐心等待驱动安装完成，请勿重复单击“Setup.exe”。
- e. 根据提示重启云服务器，使PV driver生效。
5. 检查并恢复UAC配置。
  - a. 打开“运行”窗口，输入“regedit”，打开“注册表编辑器”。
  - b. 查看HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA 键值，与卸载PV Driver前记录的键值比较，如果不同请将键值修改为2中记录的值。
6. 安装或升级UVP VMTools。
  - a. 下载UVP VMTools的安装包。  
UVP VMTools下载地址：<https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/vmtools-windows.zip>
  - b. 解压UVP VMTools的安装包。
  - c. 双击“vmtools-windows.iso”。
  - d. 运行“Setup.exe”，根据界面提示安装UVP VMTools。  
安装程序会自动匹配当前操作系统版本，并识别新安装或升级场景。  
请耐心等待驱动安装完成，请勿重复单击“Setup.exe”
  - e. 根据提示重启云服务器，使UVP VMTools驱动生效。
  - f. 驱动安装完成并重启云服务器后，需检查驱动是否安装成功。检查方法请参考[步骤2：检查UVP VMTools版本](#)。

## 步骤 4：变更规格

1. 登录控制台。
2. 单击控制台左上角的，选择区域和项目。
3. 单击“≡”，选择“计算 > 弹性云服务器”。
4. 在弹性云服务器列表，查询待变更弹性云服务器状态。  
如果不是关机状态，单击“操作”列下的“更多 > 关机”。
5. 单击“操作”列下的“更多 > 变更规格”。  
系统进入“云服务器变更规格”页面。
6. 根据界面提示，选择变更后的云服务器类型、vCPU和内存。
7. （可选）选择“专属主机”。  
对于在专属主机上创建的弹性云服务器，系统支持更换云服务器所在的专属主机。  
此时，您可以单击下拉列表，选择更换专属主机。如果下拉列表中无可用的专属主机，说明专属主机所剩资源不足，不能用于创建变更规格后的弹性云服务器。
8. 勾选复选框“我确认已完成对弹性云服务器的配置”，确认已完成[步骤3：安装或升级UVP VMTools](#)。

9. 单击“下一步”。
10. 确认变更后的配置无误后，阅读并勾选同意服务协议，单击“提交申请”。

#### 说明

- 单击“提交申请”后云平台自动为您制作系统盘快照。变更规格完成后，如已确认业务恢复正常，请在快照页面手动删除快照。
- 如果变更规格失败后，弹性云服务器无法使用，可能会需要重装操作系统来恢复云服务器，请注意重装操作系统会清除系统盘数据，但不影响数据盘的数据。

### （可选）步骤 5：检查磁盘挂载状态

XEN实例变更为KVM实例时，可能会发生磁盘脱机，因此，变更规格后，需检查磁盘挂载状态是否正常。如果正常，则变更成功。

- Windows弹性云服务器  
详细操作请参考[Windows云服务器变更规格后数据盘脱机怎么办？](#)

## 后续处理

如果控制台上云服务器列表页，显示弹性云服务器已变更规格成功，但是远程登录云服务器后，操作系统无法启动，此时，请联系客服进行恢复，或重装操作系统进行恢复。重装操作系统的操作指导，请参见[重装操作系统](#)。

#### 说明

重装操作系统会清除系统盘数据，但不影响数据盘的数据。

变更规格完成后，如已确认业务恢复正常，请在快照页面手动删除快照。

## 2.8.5 XEN 实例变更为 KVM 实例（Linux-自动配置）

### 操作场景

Linux操作系统XEN实例变更为KVM实例前，必须已完成必要的驱动安装和配置。

本节操作指导您使用自动化脚本的方式为Linux云服务器安装驱动、配置磁盘自动挂载等，并将XEN实例变更为KVM实例。

#### 说明

- XEN实例：S1、C1、C2、M1型弹性云服务器。
- KVM实例：参考[规格清单](#)，查询对应规格的虚拟化类型。
- 为了同时支持XEN虚拟化和KVM虚拟化，Linux弹性云服务器的正常运行需依赖于xen-pv驱动、virtio驱动等。XEN实例变更为KVM实例前，需要确保Linux弹性云服务器已完成相关配置，包括安装驱动、配置磁盘自动挂载等。

### 约束与限制

- 变更规格过程中，弹性云服务器需要关机，建议您选择业务空闲时间进行操作。
- Linux操作系统云服务器如果存在由多个物理卷组成的LVM逻辑卷或组建了RAID磁盘阵列，均不支持变更规格，否则可能会导致数据丢失。
- 对于XEN实例，当挂载的VBD磁盘超过24块时，不支持将规格变更为KVM实例。

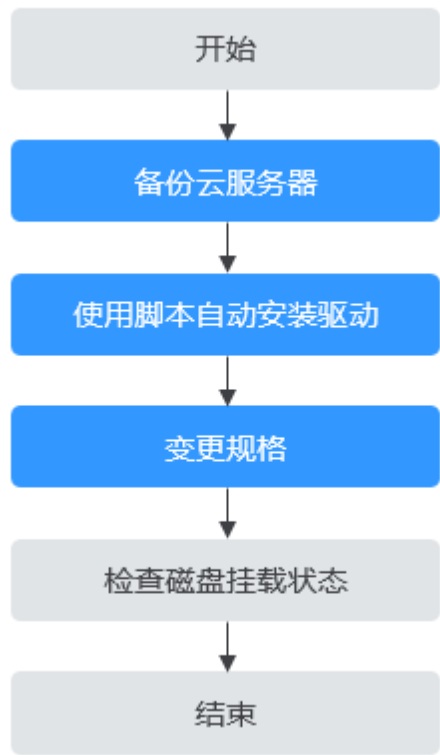


- 系统支持将“XEN实例”变更为“KVM实例”，不支持将“KVM实例”变更为“XEN实例”。

操作流程

XEN实例变更为KVM实例的操作流程如图2-185所示。

图 2-185 Linux 云服务器变更流程（自动配置）



具体的变更操作如表2-57所示。

表 2-57 XEN 实例变更为 KVM 实例（自动配置）

| 序号  | 任务               |
|-----|------------------|
| 步骤1 | 步骤1：备份云服务器       |
| 步骤2 | 步骤2：使用脚本自动安装驱动   |
| 步骤3 | 步骤3：变更规格         |
| 步骤4 | （可选）步骤4：检查磁盘挂载状态 |

步骤 1：备份云服务器

如果未安装驱动就执行变更规格的操作，云服务器可能无法正常使用，造成您的数据丢失。因此，建议您先备份云服务器，防止数据丢失。

1. 自检云服务器。  
备份前请对云服务器执行关机、开机操作，确保云服务器重启后业务可以正常运行。
2. 备份云服务器。  
其中，云服务器备份涉及存储费用；快照分为存量快照及标准快照，存量快照公测不计费，标准快照计费，请按需选择。
  - 方式一：创建云服务器备份。  
创建云服务器备份的操作，请参见[云服务器备份操作步骤](#)。
  - 方式二：创建系统盘快照和数据盘快照。  
创建快照的操作，请参见《云硬盘用户指南》的“[创建快照](#)”章节。

#### 说明

云服务器的备份和快照用于恢复数据，当变更规格失败回退后，可通过备份或快照进行数据恢复：

- 通过云服务器备份恢复数据，详细操作请参见[使用云服务器备份恢复数据](#)。
- 通过快照回滚数据，详细操作请参见[使用快照回滚数据至云硬盘](#)。

变更规格完成后，如已确认业务恢复正常，请在对应服务控制台页面删除云服务器备份或快照。

## 步骤 2：使用脚本自动安装驱动

对于支持使用脚本方式配置的弹性云服务器，请参见本部分内容。部分操作系统的弹性云服务器暂不支持使用自动化脚本方式进行配置，请直接参见[XEN实例变更为KVM实例（Linux-手动配置）](#)。

1. 登录弹性云服务器。
2. 执行以下命令，将驱动安装脚本下载到root目录下。  
**curl URL > ~/resize\_ecs\_modify\_linux.sh**  
其中，URL为规格变更优化脚本的下载地址。  
请根据云服务器所在区域选择优化脚本的下载地址：
  - 华东-上海二：[https://cn-east-2-server-resize.obs.cn-east-2.myhuaweicloud.com/linux/server\\_resize/resize\\_ecs\\_modify\\_linux.sh](https://cn-east-2-server-resize.obs.cn-east-2.myhuaweicloud.com/linux/server_resize/resize_ecs_modify_linux.sh)
  - 华北-北京一：[https://cn-north-1-server-resize.obs.cn-north-1.myhuaweicloud.com/linux/server\\_resize/resize\\_ecs\\_modify\\_linux.sh](https://cn-north-1-server-resize.obs.cn-north-1.myhuaweicloud.com/linux/server_resize/resize_ecs_modify_linux.sh)
  - 华南-广州：[https://cn-south-1-server-resize.obs.cn-south-1.myhuaweicloud.com/linux/server\\_resize/resize\\_ecs\\_modify\\_linux.sh](https://cn-south-1-server-resize.obs.cn-south-1.myhuaweicloud.com/linux/server_resize/resize_ecs_modify_linux.sh)
3. 执行以下命令，运行脚本，该脚本会自动检查并安装原生xen-pv驱动、virtio驱动。  
**bash resize\_ecs\_modify\_linux.sh**

图 2-186 运行脚本

```
susellsp3:/home # bash resize_ecs_modify_linux.sh
2018-08-21 11:04:23 Info:*****BEGIN Modify*****
2018-08-21 11:04:23 Info:get linux system type and version...
2018-08-21 11:04:23 Info:system type: susell
2018-08-21 11:04:23 Info:search grub file...
2018-08-21 11:04:23 Info:find grub file: /boot/grub/menu.lst
2018-08-21 11:04:23 Info:search initrd file list...
2018-08-21 11:04:23 Info:find initrd file: /boot/initrd-3.0.76-0.11-default
2018-08-21 11:04:23 Info:begin to modify grub file...
2018-08-21 11:04:23 Info:modify grub file: /boot/grub/menu.lst
2018-08-21 11:04:23 Info:backup file: /boot/grub/menu.lst
2018-08-21 11:04:23 Info:modify grub file success!
2018-08-21 11:04:23 Info:backup file: /boot/grub/menu.lst
2018-08-21 11:04:23 Info:add xen_platform_pci.dev.unplug=all in /boot/grub/menu.lst
2018-08-21 11:04:23 Info:begin to modify fstab file...
2018-08-21 11:04:23 Info:modify fstab file: /etc/fstab
2018-08-21 11:04:23 Info:backup file: /etc/fstab
2018-08-21 11:04:23 Info:modify fstab file success!
2018-08-21 11:04:23 Info:check xen/ide driver is already exist in initrd** or not
```

## 4. 请耐心等待脚本运行结束。

该脚本在确认驱动安装成功后会自动为云服务器设置标签，标记驱动安装成功，没有设置标签的云服务器无法执行变更规格的操作。

如果回显提示“{镜像名称} already contain xen and virtio driver”，表示检查并安装驱动成功。

- 回显提示“Success to set kvm meta!”或“this server already has kvm meta.”，表示设置标签成功，请继续执行**步骤3：变更规格**。
- 回显提示“Failed to set metadata, please try again”，表示设置标签失败，可稍后重试执行脚本。

如果安装失败请参考[XEN实例变更为KVM实例（Linux-手动配置）](#)手动配置或者联系客服寻求技术支持。

图 2-187 运行成功

```
161.548762l device-mapper: uevent: version 1.0.3
161.551753l device-mapper: ioctl: 4.37.1-iocli (2018-04-03) initialised: dm-devel@redhat.com
generating grub configuration file ...
found linux image: /boot/vmlinuz-3.10.0-1062.12.1.el7.x86_64
found initrd image: /boot/initramfs-3.10.0-1062.12.1.el7.x86_64.img
found linux image: /boot/vmlinuz-3.10.0-957.el7.x86_64
found initrd image: /boot/initramfs-3.10.0-957.el7.x86_64.img
found linux image: /boot/vmlinuz-0-rescue-8f5b018f6eb344989f6cfec5ad0839ef
found initrd image: /boot/initramfs-0-rescue-8f5b018f6eb344989f6cfec5ad0839ef.img
162.148361l SELinux: XFS with ACLs, security attributes, no debug enabled
162.189514l xor: automatically using best checksumming function:
162.202066l avx : 22448.000 MB/sec
162.233066l raid6: sse2x1 gen() 7382 MB/s
162.277075l raid6: sse2x2 gen() 8589 MB/s
162.297084l raid6: sse2x4 gen() 10273 MB/s
162.318073l raid6: avx2x1 gen() 13410 MB/s
162.337070l raid6: avx2x2 gen() 16503 MB/s
162.356066l raid6: avx2x4 gen() 18976 MB/s
162.358393l raid6: using algorithm avx2x4 gen() (18976 MB/s)
162.361600l raid6: using avx2x2 recovery algorithm
162.431572l Btrfs loaded, crc32c=crc32c-intel
162.446525l fuse init (API version 7.23)
done
2020-09-24 15:12:13 Info:check xen/ide driver is already exist in /boot/initramfs-0-rescue-8f5b018f6eb344989f6cfec5ad0839ef.img or not
2020-09-24 15:12:23 Info:xen driver:yes
2020-09-24 15:12:23 Info:ide driver:no
2020-09-24 15:12:23 Info:check virtio driver is already exist in /boot/initramfs-0-rescue-8f5b018f6eb344989f6cfec5ad0839ef.img or not
2020-09-24 15:12:41 Info:virtio driver:yes
2020-09-24 15:12:41 Info:check xen/ide driver is already exist in /boot/initramfs-3.10.0-1062.12.1.el7.x86_64.img or not
2020-09-24 15:12:45 Info:xen driver:yes
2020-09-24 15:12:45 Info:ide driver:no
2020-09-24 15:12:45 Info:check virtio driver is already exist in /boot/initramfs-3.10.0-1062.12.1.el7.x86_64.img or not
2020-09-24 15:12:52 Info:virtio driver:yes
2020-09-24 15:12:52 Info:check xen/ide driver is already exist in /boot/initramfs-3.10.0-957.el7.x86_64.img or not
2020-09-24 15:12:55 Info:xen driver:yes
2020-09-24 15:12:55 Info:ide driver:no
2020-09-24 15:12:55 Info:check virtio driver is already exist in /boot/initramfs-3.10.0-957.el7.x86_64.img or not
2020-09-24 15:13:03 Info:virtio driver:yes
2020-09-24 15:13:03 Info:centos7 already contain xen and virtio driver
% Total % Received % Xferd Average Speed Time Time Time Current
 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
2020-09-24 15:13:03 Info:Success to set kvm meta!
```

### 📖 说明

- 请务必确保云服务器配置成功，否则，可能会导致变更规格后的弹性云服务器不可用。如果运行失败，请参考[XEN实例变更为KVM实例（Linux-手动配置）](#)手动配置。
- 脚本安装失败常见问题请参考：
  - [CentOS 5操作系统云服务器执行驱动安装脚本失败怎么办？](#)
  - [Linux云服务器变更规格时执行驱动安装脚本失败怎么办？](#)

## 步骤 3：变更规格

1. 登录控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”。
4. 在弹性云服务器列表，查询待变更弹性云服务器状态。  
如果不是关机状态，单击“操作”列下的“更多 > 关机”。
5. 单击“操作”列下的“更多 > 变更规格”。  
系统进入“云服务器变更规格”页面。
6. 根据界面提示，选择变更后的云服务器类型、vCPU和内存。
7. （可选）选择“专属主机”。  
对于在专属主机上创建的弹性云服务器，系统支持更换云服务器所在的专属主机。  
此时，您可以单击下拉列表，选择更换专属主机。如果下拉列表中无可用的专属主机，说明专属主机所剩资源不足，不能用于创建变更规格后的弹性云服务器。
8. 勾选复选框“我确认已完成对弹性云服务器的配置”，确认已完成“配置弹性云服务器”操作。
9. 单击“下一步”。
10. 确认变更后的配置无误后，阅读并勾选同意服务协议，单击“提交申请”。

### 📖 说明

- 单击“提交申请”后云平台自动为您制作系统盘快照。变更规格完成后，如已确认业务恢复正常，请在快照页面手动删除快照。
- 如果变更规格失败后，弹性云服务器无法使用，可能会需要重装操作系统来恢复云服务器，请注意重装操作系统会清除系统盘数据，但不影响数据盘的数据。

## （可选）步骤 4：检查磁盘挂载状态

XEN实例变更为KVM实例时，可能会发生磁盘挂载失败的情况，因此，变更规格后，需检查磁盘挂载状态是否正常。如果正常，则变更成功。

- Linux弹性云服务器  
详细操作请参考[Linux云服务器变更规格后数据盘脱机怎么办？](#)

## 后续处理

如果控制台上云服务器列表页，显示弹性云服务器已变更规格成功，但是远程登录云服务器后，操作系统无法启动，此时，请联系客服进行恢复，或重装操作系统进行恢复。重装操作系统的操作指导，请参见[重装操作系统](#)。

#### 说明

重装操作系统会清除系统盘数据，但不影响数据盘的数据。

变更规格完成后，如已确认业务恢复正常，请在快照页面手动删除快照。

## 2.8.6 XEN 实例变更为 KVM 实例（Linux-手动配置）

### 操作场景

Linux操作系统XEN实例变更为KVM实例前，必须完成驱动的安装和配置。

本节操作指导您手动安装Linux云服务器驱动、配置磁盘自动挂载等，并将XEN实例变更为KVM实例。

如需使用自动化脚本安装驱动的方法请参考[XEN实例变更为KVM实例（Linux-自动配置）](#)。

#### 说明

- XEN实例：S1、C1、C2、M1型弹性云服务器。
- KVM实例：参考[规格清单](#)，查询对应规格的虚拟化类型。
- 为了同时支持XEN虚拟化和KVM虚拟化，Linux弹性云服务器的正常运行需依赖于xen-pv驱动、virtio驱动等。XEN实例变更为KVM实例前，需要确保Linux弹性云服务器已完成相关配置，包括安装驱动、配置磁盘自动挂载等。

### 约束与限制

- 变更规格过程中，弹性云服务器需要关机，建议您选择业务空闲时间进行操作。
- Linux操作系统云服务器如果存在由多个物理卷组成的LVM逻辑卷或组建了RAID磁盘阵列，均不支持变更规格，否则可能会导致数据丢失。
- 对于XEN实例，当挂载的VBD磁盘超过24块时，不支持将规格变更为KVM实例。
- 系统支持将“XEN实例”变更为“KVM实例”，不支持将“KVM实例”变更为“XEN实例”。

### 操作流程

XEN实例变更为KVM实例的操作流程如[图2-188](#)所示。

图 2-188 Linux 云服务器变更流程（手动配置）

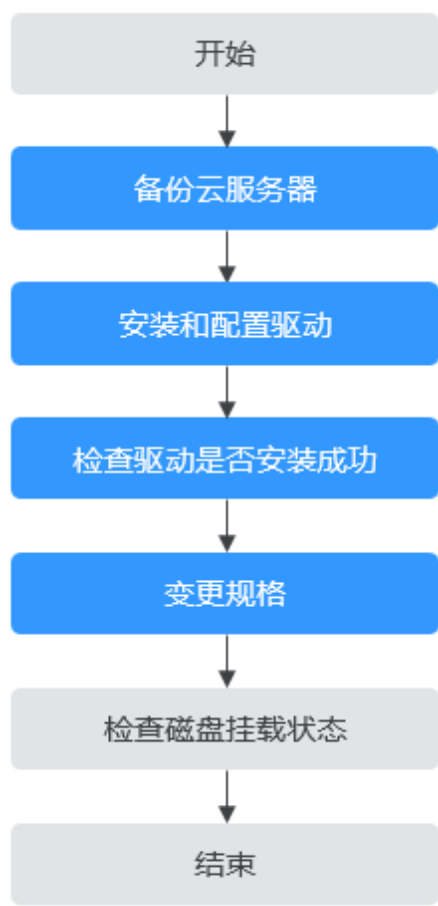


表 2-58 XEN 实例变更为 KVM 实例（手动配置）

| 序号  | 任务               |
|-----|------------------|
| 步骤1 | 步骤1：备份云服务器       |
| 步骤2 | 步骤2：安装驱动         |
| 步骤3 | 步骤3：检查云服务器配置是否成功 |
| 步骤4 | 步骤4：变更规格         |
| 步骤5 | （可选）步骤5：检查磁盘挂载状态 |

步骤 1：备份云服务器

如果未安装驱动就执行变更规格的操作，云服务器可能无法正常使用，造成您的数据丢失。因此，建议您先备份云服务器，防止数据丢失。

1. 自检云服务器。
- 备份前请对云服务器执行关机、开机操作，确保云服务器重启后业务可以正常运行。

## 2. 备份云服务器。

其中，云服务器备份涉及存储费用；快照分为存量快照及标准快照，存量快照公测不计费，标准快照计费，请按需选择。

- 方式一：创建云服务器备份。

创建云服务器备份的操作，请参见[云服务器备份操作步骤](#)。

- 方式二：创建系统盘快照和数据盘快照。

创建快照的操作，请参见《云硬盘用户指南》的“[创建快照](#)”章节。

### 说明

云服务器的备份和快照用于恢复数据，当变更规格失败回退后，可通过备份或快照进行数据恢复：

- 通过云服务器备份恢复数据，详细操作请参见[使用云服务器备份恢复数据](#)。
- 通过快照回滚数据，详细操作请参见[使用快照回滚数据至云硬盘](#)。

变更规格完成后，如已确认业务恢复正常，请在对应服务控制台页面删除云服务器备份或快照。

## 步骤 2：安装驱动

对于不支持使用脚本方式配置的弹性云服务器，请参见本部分内容，手动配置云服务器。

1. 登录弹性云服务器。
2. 卸载云服务器中已安装的Tools。  
卸载操作请参见[在Linux系统中卸载Tools](#)。
3. 修改grub的UUID。  
具体操作请参见[修改grub文件磁盘标识方式为UUID](#)。
4. 修改fstab的UUID。  
具体操作请参见[修改fstab文件磁盘标识方式为UUID](#)。
5. 安装原生的XEN和KVM驱动。  
安装方法请参见[安装原生的XEN和KVM驱动](#)。

## 步骤 3：检查云服务器配置是否成功

根据[步骤2：安装驱动](#)修改grub文件、安装所需驱动后，需检查修改是否生效、驱动是否安装成功。

### 说明

手动方式配置弹性云服务器时请务必执行以下操作检查云服务器配置是否成功。

1. 登录弹性云服务器。
2. 执行以下命令，检查root分区是否以UUID的形式表示。

**cat /boot/grub/grub.cfg**

- 是，表示已修改grub文件的磁盘标识方式为UUID。
- 否，修改失败，请参见[步骤2：安装驱动](#)重新修改。

```
.....menuentry 'Ubuntu Linux, with Linux 3.13.0-24-generic' --class ubuntu --class gnu-linux --class
gnu --class os --unrestricted $menuentry_id_option 'gnulinux-3.13.0-24-generic-advanced-
ec51d860-34bf-4374-ad46-a0c3e337fd34' {
 recordfail
 load_video
```



```
gfxmode $linux_gfx_mode
insmod gzio
insmod part_msdos
insmod ext2
if [x$feature_platform_search_hint = xy]; then
search --no-floppy --fs-uuid --set=root ec51d860-34bf-4374-ad46-a0c3e337fd34
else
search --no-floppy --fs-uuid --set=root ec51d860-34bf-4374-ad46-a0c3e337fd34
fi
echo 'Loading Linux 3.13.0-24-generic ...'
linux /boot/vmlinuz-3.13.0-24-generic root=UUID=ec51d860-34bf-4374-ad46-a0c3e337fd34 ro
echo 'Loading initial ramdisk ...'
initrd /boot/initrd.img-3.13.0-24-generic
}
```

### 说明

对于不同操作系统，grub文件的具体路径存在差异，请以具体的操作系统为准。例如：“/boot/grub/menu.lst”、“/boot/grub/grub.cfg”、“/boot/grub2/grub.cfg”、“/boot/grub/grub.conf”。

3. 执行以下命令，检查磁盘的标识方式是否为UUID。

**cat /etc/fstab**

- 是，表示已修改fstab文件的磁盘标识方式为UUID。
- 否，修改失败，请参见[步骤2：安装驱动](#)重新修改。

```
[root@***** ~]# cat /etc/fstab
UUID=4eb40294-4c6f-4384-bbb6-b8795bbb1130 / xfs defaults 0 0
UUID=2de37c6b-2648-43b4-a4f5-40162154e135 swap swap defaults 0 0
```

4. 检查是否已安装原生的XEN和KVM驱动。

- 如果引导的虚拟文件系统是initramfs，执行以下命令：

```
lsinitrd /boot/initramfs-`uname -r`.img | grep `uname -r` | grep xen
lsinitrd /boot/initramfs-`uname -r`.img | grep `uname -r` | grep virtio
```

- 如果引导的虚拟文件系统是initrd，执行如下命令：

```
lsinitrd /boot/initrd-`uname -r` | grep `uname -r` | grep xen
lsinitrd /boot/initrd-`uname -r` | grep `uname -r` | grep virtio
```

如果安装成功，回显将显示已安装的原生XEN和KVM驱动名称。

```
[root@CTU10000xxxx home]# lsinitrd /boot/initramfs-`uname -r`.img | grep `uname -r` | grep xen
-rwxr--r-- 1 root root 54888 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/
block/xen-blkfront.ko
-rwxr--r-- 1 root root 45664 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/
drivers/net/xen-netfront.ko

[root@CTU10000xxxx home]# lsinitrd /boot/initramfs-`uname -r`.img | grep `uname -r` | grep virtio
-rwxr--r-- 1 root root 23448 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/
block/virtio_blk.ko
-rwxr--r-- 1 root root 50704 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/
drivers/net/virtio_net.ko
-rwxr--r-- 1 root root 28424 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/
scsi/virtio_scsi.ko
drwxr-xr-x 2 root root 0 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/
virtio
-rwxr--r-- 1 root root 14544 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/
virtio/virtio.ko
-rwxr--r-- 1 root root 21040 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/
virtio/virtio_pci.ko
-rwxr--r-- 1 root root 18016 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/
virtio/virtio_ring.ko
```

5. 执行以下命令更新云服务器的系统标签。



```
curl 'http://169.254.169.254/openstack/latest/support_hypervisor' -X POST
-H "Accept: application/json" -d '{"support_hypervisor":["all"]}' -w %
{http_code}
```

回显显示200说明云服务器的系统标签已添加成功。

图 2-189 设置云服务器的系统标签

```
[root@test ~]# curl 'http://169.254.169.254/openstack/latest/support_hypervisor'
-X POST -H "Accept: application/json" -d '{"support_hypervisor":["all"]}' -w %
{http_code}
200[root@test ~]#
```

#### 说明

请务必确保云服务器配置成功，否则，可能会导致变更规格后的弹性云服务器不可用。

## 步骤 4：变更规格

1. 登录控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”。
4. 在弹性云服务器列表，查询待变更弹性云服务器状态。  
如果不是关机状态，单击“操作”列下的“更多 > 关机”。
5. 单击“操作”列下的“更多 > 变更规格”。
6. 根据界面提示，选择变更后的云服务器类型、vCPU和内存。
7. （可选）选择“专属主机”。

对于在专属主机上创建的弹性云服务器，系统支持更换云服务器所在的专属主机。

此时，您可以单击下拉列表，选择更换专属主机。如果下拉列表中无可用的专属主机，说明专属主机所剩资源不足，不能用于创建变更规格后的弹性云服务器。

8. 勾选复选框“我确认已完成对弹性云服务器的配置”，确认已完成“配置弹性云服务器”操作。
9. 单击“下一步”。
10. 确认变更后的配置无误后，阅读并勾选同意服务协议，单击“提交申请”。

#### 说明

- 单击“提交申请”后云平台自动为您制作系统盘快照。变更规格完成后，如已确认业务恢复正常，请在快照页面手动删除快照。
- 如果变更规格失败后，弹性云服务器无法使用，可能会需要重装操作系统来恢复云服务器，请注意重装操作系统会清除系统盘数据，但不影响数据盘的数据。

## （可选）步骤 5：检查磁盘挂载状态

XEN实例变更为KVM实例时，可能会发生磁盘挂载失败的情况，因此，变更规格后，需检查磁盘挂载状态是否正常。如果正常，则变更成功。

- Linux弹性云服务器  
详细操作请参考[Linux云服务器变更规格后数据盘脱机怎么办？](#)

## 后续处理

如果控制台上云服务器列表页，显示弹性云服务器已变更规格成功，但是远程登录云服务器后，操作系统无法启动，此时，请联系客服进行恢复，或重装操作系统进行恢复。重装操作系统的操作指导，请参见[重装操作系统](#)。

### 说明

重装操作系统会清除系统盘数据，但不影响数据盘的数据。

变更规格完成后，如已确认业务恢复正常，请在快照页面手动删除快照。

## 2.8.7 XEN 实例变更为 KVM 实例（Linux-批量自动配置）

### 操作场景

Linux操作系统XEN实例变更为KVM实例前，必须已完成必要的驱动安装和配置。

当您需要变更的Linux操作系统的XEN实例比较多时候，推荐您使用本节的批量自动配置的方法安装驱动，通过自动化脚本的方式批量为Linux云服务器安装驱动、配置磁盘自动挂载。在驱动安装完成后使用控制台提供的“变更规格”功能将XEN实例变更为KVM实例。

### 说明

- XEN实例：S1、C1、C2、M1型弹性云服务器。
- KVM实例：参考[规格清单](#)，查询对应规格的虚拟化类型。
- 为了同时支持XEN虚拟化和KVM虚拟化，Linux弹性云服务器的正常运行需依赖于xen-pv驱动、virtio驱动等。XEN实例变更为KVM实例前，需要确保Linux弹性云服务器已完成相关配置，包括安装驱动、配置磁盘自动挂载等。

### 约束与限制

- 批量安装驱动仅支持Linux操作系统。
- 变更规格过程中，弹性云服务器需要关机，建议您选择业务空闲时间进行操作。
- 需要选取一台操作系统为CentOS 7且已绑定弹性公网IP的云服务器作为执行机，且与待批量安装驱动的弹性云服务器之间网络需要互通。

### 说明

若已配置yum内部源，可不需要绑定弹性公网IP。

- 需要提前准备待批量安装驱动的云服务器的IP地址、root用户的密码信息或者私钥文件。
- 仅支持对使用同一密钥对的云服务器执行批量安装驱动和配置的操作。

### 操作流程

XEN实例变更为KVM实例的操作流程如[图2-190](#)所示。

图 2-190 Linux 云服务器变更流程（批量自动配置）

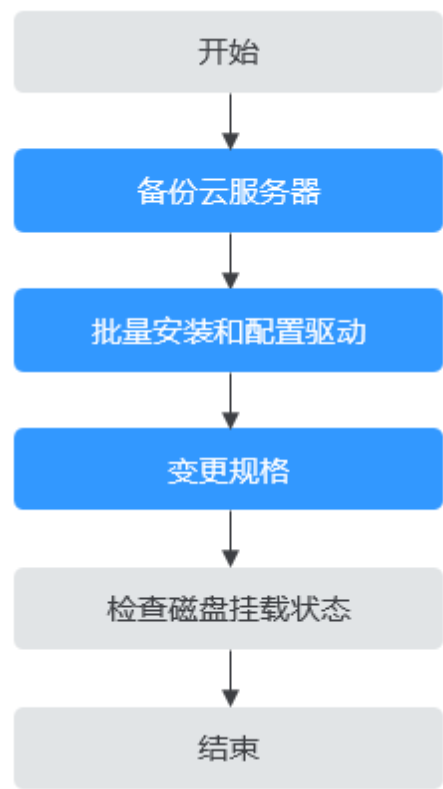


表 2-59 XEN 实例变更为 KVM 实例（批量自动配置）

| 序号  | 任务               |
|-----|------------------|
| 步骤1 | 步骤1：备份云服务器       |
| 步骤2 | 步骤2：批量安装和配置驱动    |
| 步骤3 | 步骤3：变更规格         |
| 步骤4 | （可选）步骤4：检查磁盘挂载状态 |

步骤 1：备份云服务器

如果未安装驱动就执行变更规格的操作，云服务器可能无法正常使用，造成您的数据丢失。因此，建议您先备份云服务器，防止数据丢失。

1. 自检云服务器。  
备份前请对云服务器执行关机、开机操作，确保云服务器重启后业务可以正常运行。
2. 备份云服务器。  
其中，云服务器备份涉及存储费用；快照分为存量快照及标准快照，存量快照公测不计费，标准快照计费，请按需选择。
  - 方式一：创建云服务器备份。  
创建云服务器备份的操作，请参见[云服务器备份操作步骤](#)。

- 方式二：创建系统盘快照和数据盘快照。  
创建快照的操作，请参见《云硬盘用户指南》的“[创建快照](#)”章节。

#### 说明

云服务器的备份和快照用于恢复数据，当变更规格失败回退后，可通过备份或快照进行数据恢复：

- 通过云服务器备份恢复数据，详细操作请参见[使用云服务器备份恢复数据](#)。
- 通过快照回滚数据，详细操作请参见[使用快照回滚数据至云硬盘](#)。

变更规格完成后，如已确认业务恢复正常，请在对应服务控制台页面删除云服务器备份或快照。

## 步骤 2：批量安装和配置驱动

对于支持使用脚本方式批量配置的弹性云服务器，请参见本节操作内容。

不支持使用自动化脚本方式进行配置的云服务器，请直接参见[XEN实例变更为KVM实例（Linux-手动配置）](#)。

1. 登录已准备好的执行机，执行机需满足的条件请参考[约束与限制](#)。
2. 执行以下命令，安装批量脚本运行所需要的依赖。

```
yum install ansible -y
```

3. 执行以下命令，将驱动安装脚本下载到root目录下。

```
curl URL > ~/resize_ecs_modify_linux.sh
```

其中，URL为驱动安装脚本的下载地址。

请根据云服务器所在区域选择脚本的下载地址：

- 华东-上海二：[https://cn-east-2-server-resize.obs.cn-east-2.myhuaweicloud.com/linux/server\\_resize/resize\\_ecs\\_modify\\_linux.sh](https://cn-east-2-server-resize.obs.cn-east-2.myhuaweicloud.com/linux/server_resize/resize_ecs_modify_linux.sh)
- 华北-北京一：[https://cn-north-1-server-resize.obs.cn-north-1.myhuaweicloud.com/linux/server\\_resize/resize\\_ecs\\_modify\\_linux.sh](https://cn-north-1-server-resize.obs.cn-north-1.myhuaweicloud.com/linux/server_resize/resize_ecs_modify_linux.sh)
- 华南-广州：[https://cn-south-1-server-resize.obs.cn-south-1.myhuaweicloud.com/linux/server\\_resize/resize\\_ecs\\_modify\\_linux.sh](https://cn-south-1-server-resize.obs.cn-south-1.myhuaweicloud.com/linux/server_resize/resize_ecs_modify_linux.sh)

4. 执行以下命令，将批量操作脚本下载到root目录下。

```
curl URL > ~/batch_resize_ecs_modify_linux.py
```

其中，URL为批量操作的执行脚本。

请根据云服务器所在区域选择脚本的下载地址：

- 华东-上海二：[https://cn-east-2-server-resize.obs.cn-east-2.myhuaweicloud.com/linux/server\\_resize/batch\\_resize\\_ecs\\_modify\\_linux.py](https://cn-east-2-server-resize.obs.cn-east-2.myhuaweicloud.com/linux/server_resize/batch_resize_ecs_modify_linux.py)
- 华北-北京一：[https://cn-north-1-server-resize.obs.cn-north-1.myhuaweicloud.com/linux/server\\_resize/batch\\_resize\\_ecs\\_modify\\_linux.py](https://cn-north-1-server-resize.obs.cn-north-1.myhuaweicloud.com/linux/server_resize/batch_resize_ecs_modify_linux.py)
- 华南-广州：[https://cn-south-1-server-resize.obs.cn-south-1.myhuaweicloud.com/linux/server\\_resize/batch\\_resize\\_ecs\\_modify\\_linux.py](https://cn-south-1-server-resize.obs.cn-south-1.myhuaweicloud.com/linux/server_resize/batch_resize_ecs_modify_linux.py)

5. 执行以下命令，新建并编辑host\_list.txt，按i进入编辑模式。

**vi host\_list.txt****⚠ 注意**

请将驱动安装脚本、批量操作执行脚本、host\_list.txt文件放在一个目录下。

6. 将需要自动安装驱动的云服务器的相关信息填写到host\_list.txt文件中。  
文件填写格式与登录待切换弹性云服务器的方式需要匹配。
  - 使用密钥对方式鉴权的云服务器，填写方式如下：

**⚠ 注意**

- 使用密钥对方式鉴权的云服务器，请将创建弹性云服务器时保存的私钥文件，上传至与host\_list.txt同一个文件夹下。
- 使用密钥对方式鉴权的云服务器，请确保私钥文件的权限为400。

**chmod 400 私钥文件**

每行仅需填写云服务器IP地址。

示例：

```
192.168.1.10
192.168.1.11
```

- 使用密码方式登录的云服务器，填写方式如下：  
请严格按照每行ip,root用户密码，中间以英文逗号隔开的格式填写。

示例：

```
192.168.1.10,*****
192.168.1.11,*****
```

确认输入完毕后，按Esc退出编辑模式，输入:wq保存退出。

7. 运行批量执行操作脚本“batch\_resize\_ecs\_modify\_linux.py”，该脚本会批量对配置好的云服务器进行自动检查并安装原生xen-pv驱动、virtio驱动。
  - a. 执行以下命令，对配置好的云服务器安装驱动。

- 密钥对鉴权方式的服务器

如果私钥文件与批量操作执行脚本在一个目录下，则直接指定私钥文件名称即可。

**python batch\_resize\_ecs\_modify\_linux.py {私钥文件路径/私钥文件名称}**

图 2-191 运行脚本

```
[root@allinone-centos ~]# python batch_resize_ecs_modify_linux.py id_rsa
2020-10-22 10:51:56 Start copying the scripts to all hosts.
2020-10-22 10:52:03 Start executing scripts on all hosts, it will take a while..
```

- 密码方式鉴权的服务器。

**python batch\_resize\_ecs\_modify\_linux.py**

图 2-192 运行脚本

```
[root@allinone-centos ~]# python batch_resize_ecs_modify_linux.py
2020-10-22 10:53:44 Start copying the scripts to all hosts.
2020-10-22 10:53:52 Start executing scripts on all hosts, it will take a while..
```

8. 查看运行结果。
- 请耐心等待脚本运行结束，脚本在确认驱动安装成功后会自动为云服务器设置标签，标记驱动安装成功，没有设置标签的云服务器无法执行变更规格的操作。
- 运行结果如图2-193所示。表2-60，列举了常见的运行结果和说明。

图 2-193 运行成功

```
2020-10-22 10:56:04 Please check the execution result.
status ip msg
[SUCCESS] 172.28.0.6 Success to set kvm meta
[SUCCESS] 172.28.0.8 Success to set kvm meta
[SUCCESS] 172.28.0.9 Success to set kvm meta
Total: 3 Success: 3 Failed: 0
You can check the logs/exec_origin.log for details.
```

如果安装失败请参考[XEN实例变更为KVM实例（Linux-手动配置）](#)手动配置或者联系客服寻求技术支持。

表 2-60 运行结果对照表

| 回显信息                                                                       | 说明                                                                          |
|----------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| Total: {数量} Success: {数量} Failed: 0                                        | 全部弹性云主机完成检查并安装驱动成功。                                                         |
| Total: {数量} Success: {数量} Failed: {数量}                                     | Failed数量不为零，表示部分弹性云主机检查或者安装驱动失败，可按照提示查看日志(logs/exec_origin.log)对应主机执行失败的原因。 |
| Please check the format of host_list.txt                                   | host_list.txt文件填写不符合要求，需要重新按照步骤6要求进行填写。                                     |
| [Error] resize_ecs_modify_linux.sh not found.                              | 步骤6中的驱动安装脚本尚未下载，需要重新操作下载。                                                   |
| Host(s) is unreachable, please check the network or password of user root. | 当前云服务器无法访问以上弹性云服务器，需要确认网络是否互通，或者host_list.txt文件中配置的root用户密码是否正确。            |
| [Error] host_list.txt not found.                                           | host_list.txt文件尚未创建，需要按照步骤6进行操作。                                            |
| [Error] key-file {私钥文件} not found.                                         | 指定的私钥文件不存在，请确定私钥文件存在后，重新按照步骤6操作。或者使用密码方式登录，重新按照操作流程步骤6进行操作。                 |
| Please confirm that the ansible has been installed.                        | 步骤2中的运行所需依赖尚未安装，需要执行命令进行安装。                                                 |



 说明

- 驱动安装成功后，请妥善处理host\_list.txt中的弹性虚拟机密码以及私钥文件，防止出现环境密码、私钥文件泄露。
- 请务必确保云服务器配置成功，否则，可能会导致变更规格后的弹性云服务器不可用。如果运行失败或者，请参考[XEN实例变更为KVM实例（Linux-手动配置）](#)。
- 脚本安装失败常见问题请参考：
  - [CentOS5操作系统云服务器执行驱动安装脚本失败怎么办？](#)
  - [Linux云服务器变更规格时执行驱动安装脚本失败怎么办？](#)

## 步骤 3：变更规格

- 在管理控制台变更规格
  - a. 登录控制台。
  - b. 单击控制台左上角的 ，选择区域和项目。
  - c. 单击“”，选择“计算 > 弹性云服务器”。
  - d. 在弹性云服务器列表，查询待变更弹性云服务器状态。  
如果不是关机状态，单击“操作”列下的“更多 > 关机”。
  - e. 单击“操作”列下的“更多 > 变更规格”。  
系统进入“云服务器变更规格”页面。
  - f. 根据界面提示，选择变更后的云服务器类型、vCPU和内存。
  - g. （可选）选择“专属主机”。  
对于在专属主机上创建的弹性云服务器，系统支持更换云服务器所在的专属主机。  
此时，您可以单击下拉列表，选择更换专属主机。如果下拉列表中无可用的专属主机，说明专属主机所剩资源不足，不能用于创建变更规格后的弹性云服务器。
  - h. 勾选复选框“我确认已完成对弹性云服务器的配置”，确认已完成[步骤2：批量安装和配置驱动](#)。
  - i. 单击“下一步”。
  - j. 确认变更后的配置无误后，阅读并勾选同意服务协议，单击“提交申请”。

 说明

- 单击“提交申请”后云平台自动为您制作系统盘快照。变更规格完成后，如已确认业务恢复正常，请在快照页面手动删除快照。
- 如果变更规格失败后，弹性云服务器无法使用，可能会需要重装操作系统来恢复云服务器，请注意重装操作系统会清除系统盘数据，但不影响数据盘的数据。
- 使用API变更规格
  - [变更云服务器规格](#)
  - [变更云服务器规格（按需）](#)

## （可选）步骤 4：检查磁盘挂载状态

XEN实例变更为KVM实例时，可能会发生磁盘脱机，因此，变更规格后，需检查磁盘挂载状态是否正常。如果正常，则变更成功。

- Linux弹性云服务器  
详细操作请参考[Linux云服务器变更规格后数据盘脱机怎么办?](#)

## 后续处理

如果控制台上云服务器列表页，显示弹性云服务器已变更规格成功，但是远程登录云服务器后，操作系统无法启动，此时，请联系客服进行恢复，或重装操作系统进行恢复。重装操作系统的操作指导，请参见[重装操作系统](#)。

### 说明

重装操作系统会清除系统盘数据，但不影响数据盘的数据。

变更规格完成后，如已确认业务恢复正常，请在快照页面手动删除快照。

## 2.8.8 KVM 实例变更为 QingTian 实例（Windows）

### 操作场景

本节介绍将Windows操作系统的KVM实例变更为QingTian架构实例的操作步骤。

### 说明

- KVM实例：参考[规格清单](#)，虚拟化类型为KVM的规格实例。
- QingTian架构实例：参考[规格清单](#)，虚拟化类型为QingTian的规格实例。

### 约束与限制

- 变更规格过程中，弹性云服务器需要关机，建议您选择业务空闲时间进行操作。
- 变更规格时不支持修改网络类型。
- QingTian实例仅支持使用SCSI磁盘模式挂载磁盘，不支持使用VBD磁盘模式挂载磁盘。即磁盘标识为wwn。
- 支持将“KVM实例”变更为“QingTian实例”，不支持将“QingTian实例”变更为“KVM实例”。
- 不支持“XEN”实例变更为“QingTian实例”。

### 操作流程

KVM实例变更为QingTian实例的操作流程如[图2-194](#)所示。



图 2-194 Windows 云服务器变更流程

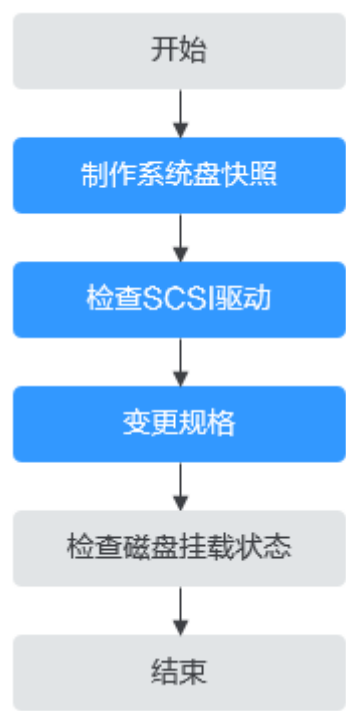


表 2-61 KVM 实例变更为 QingTian 实例

| 序号  | 任务                |
|-----|-------------------|
| 步骤1 | 步骤1：备份云服务器        |
| 步骤2 | 步骤2：检查SCSI驱动      |
| 步骤3 | 步骤3：变更规格          |
| 步骤4 | (可选) 步骤4：检查磁盘挂载状态 |

步骤 1：备份云服务器

如果未安装驱动就执行变更规格的操作，云服务器可能无法正常使用，造成您的数据丢失。因此，建议您先备份云服务器，防止数据丢失。

1. 自检云服务器。  
备份前请对云服务器执行关机、开机操作，确保云服务器重启后业务可以正常运行。
2. 备份云服务器。  
其中，云服务器备份涉及存储费用；快照分为存量快照及标准快照，存量快照公测不计费，标准快照计费，请按需选择。
  - 方式一：创建云服务器备份。  
创建云服务器备份的操作，请参见[云服务器备份操作步骤](#)。
  - 方式二：创建系统盘快照和数据盘快照。  
创建快照的操作，请参见《云硬盘用户指南》的“[创建快照](#)”章节。

说明

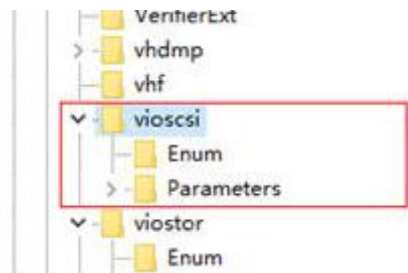
云服务器的备份和快照用于恢复数据，当变更规格失败回退后，可通过备份或快照进行数据恢复：

- 通过云服务器备份恢复数据，详细操作请参见[使用云服务器备份恢复数据](#)。
  - 通过快照回滚数据，详细操作请参见[使用快照回滚数据至云硬盘](#)。
- 变更规格完成后，如已确认业务恢复正常，请在对应服务控制台页面删除云服务器备份或快照。

步骤 2：检查 SCSI 驱动

- 登录弹性云服务器。
  - 打开“运行”对话框，输入“regedit”进入注册表编辑器。
  - 在注册表中找到以下路径：Computer\HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Services\vioscsi
- 查看该目录下是否存在“StartOverride”项。
- 若注册表该路径下只有“Enum”和“Parameters”项，则无需修改。

图 2-195 注册表

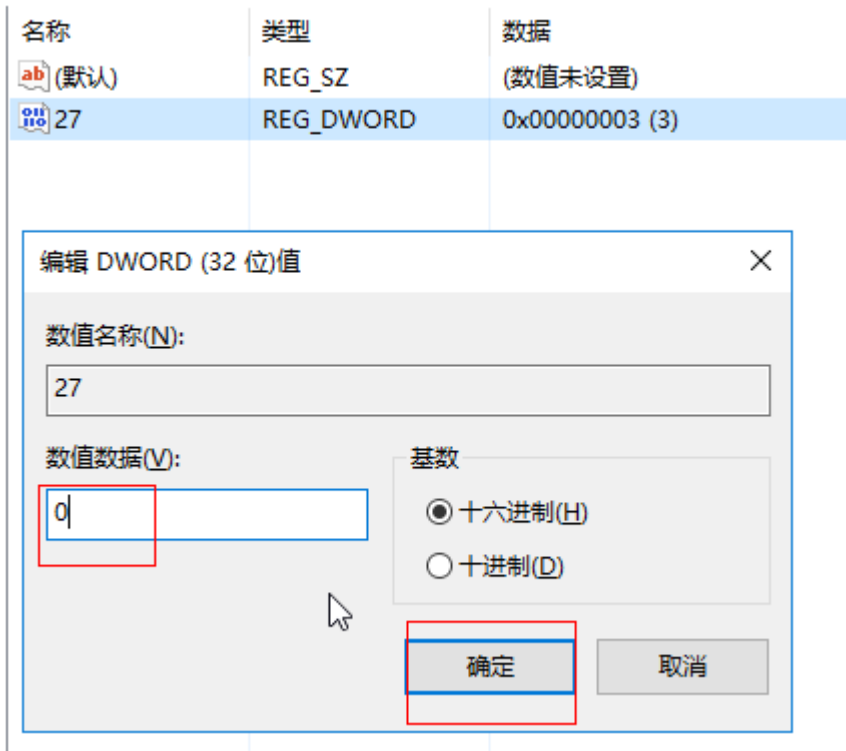


- 若注册表该路径下存在“StartOverride”项，请执行步骤4。
- 修改“StartOverride”项中类型为“REG\_DWORD”，数据为“3”的字段修改为“0”。

图 2-196 “StartOverride”项



图 2-197 修改“REG\_DWORD”数据



5. 将弹性云服务器关机。

步骤 3：变更规格

1. 登录控制台。
2. 单击控制台左上角的 ，选择区域和项目。
3. 单击“

文档版本 01 (2025-06-13)

版权所有 © 华为云计算技术有限公司

251

### 📖 说明

- 单击“提交申请”后云平台自动为您制作系统盘快照。变更规格完成后，如已确认业务恢复正常，请在快照页面手动删除快照。
- 如果变更规格失败后，弹性云服务器无法使用，可能会需要重装操作系统来恢复云服务器，请注意重装操作系统会清除系统盘数据，但不影响数据盘的数据。

## （可选）步骤 4：检查磁盘挂载状态

KVM 实例变更为QingTian实例时，可能会发生磁盘挂载失败的情况，因此，变更规格后，需检查磁盘挂载状态是否正常。如果正常，则变更成功。

- Windows弹性云服务器

详细操作请参考[Windows云服务器变更规格后数据盘脱机怎么办？](#)

## 后续处理

如果控制台上云服务器列表页，显示弹性云服务器已变更规格成功，但是远程登录云服务器后，操作系统无法启动。此时，请联系客服进行恢复，或重装操作系统。重装系统的操作指导，请参见[重装操作系统](#)。

### 📖 说明

重装操作系统会清除系统盘数据，但不影响数据盘的数据。

变更规格完成后，如已确认业务恢复正常，请在快照页面手动删除快照。

## 2.8.9 KVM 实例变更为 QingTian 实例（Linux）

### 操作场景

本节介绍将Linux操作系统的KVM实例变更为QingTian架构实例的操作步骤。

### 📖 说明

- KVM实例：参考[规格清单](#)，查询对应规格的虚拟化类型。
- QingTian架构实例：参考[规格清单](#)，虚拟化类型为QingTian的规格实例。

## 约束与限制

- 变更规格过程中，弹性云服务器需要关机，建议您选择业务空闲时间进行操作。
- 变更规格时不支持修改网络类型。
- Linux操作系统云服务器的系统盘和数据盘如果存在由多个物理卷组成的LVM逻辑卷或组建了RAID磁盘阵列，均不支持变更规格，否则可能会导致数据丢失。
- QingTian实例仅支持使用SCSI磁盘模式挂载磁盘，不支持使用VBD磁盘模式挂载磁盘。即磁盘标识为wwn。
- 支持将“KVM实例”变更为“QingTian实例”，不支持将“QingTian实例”变更为“KVM实例”。
- 不支持“XEN”实例变更为“QingTian实例”。

操作流程

KVM实例变更为QingTian实例的操作流程如图2-198所示。

图 2-198 Linux 云服务器变更流程

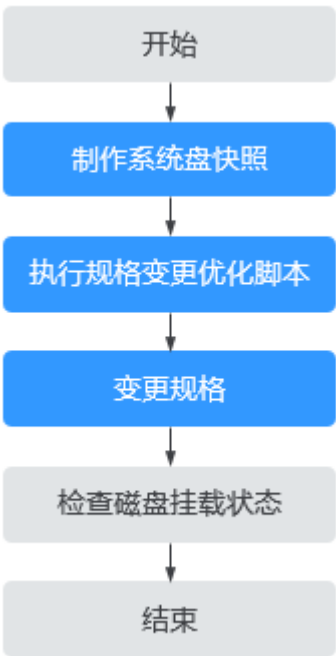


表 2-62 KVM 实例变更为 QingTian 实例

| 序号  | 任务                |
|-----|-------------------|
| 步骤1 | 步骤1：备份云服务器        |
| 步骤2 | 步骤2：执行规格变更优化脚本    |
| 步骤3 | 步骤3：变更规格          |
| 步骤4 | (可选) 步骤4：检查磁盘挂载状态 |

步骤 1：备份云服务器

如果未安装驱动就执行变更规格的操作，云服务器可能无法正常使用，造成您的数据丢失。因此，建议您先备份云服务器，防止数据丢失。

1. 自检云服务器。  
备份前请对云服务器执行关机、开机操作，确保云服务器重启后业务可以正常运行。
2. 备份云服务器。  
其中，云服务器备份涉及存储费用；快照分为存量快照及标准快照，存量快照公测不计费，标准快照计费，请按需选择。
  - 方式一：创建云服务器备份。

创建云服务器备份的操作，请参见[云服务器备份操作步骤](#)。

- 方式二：创建系统盘快照和数据盘快照。

创建快照的操作，请参见《云硬盘用户指南》的“[创建快照](#)”章节。

#### 📖 说明

云服务器的备份和快照用于恢复数据，当变更规格失败回退后，可通过备份或快照进行数据恢复：

- 通过云服务器备份恢复数据，详细操作请参见[使用云服务器备份恢复数据](#)。
- 通过快照回滚数据，详细操作请参见[使用快照回滚数据至云硬盘](#)。

变更规格完成后，如已确认业务恢复正常，请在对应服务控制台页面删除云服务器备份或快照。

## 步骤 2：执行规格变更优化脚本

1. 远程登录弹性云服务器。
2. 执行以下命令，将规格变更优化下载到root目录下。

```
curl URL > ~/offload_check_blockdevice.sh
```

其中，URL为规格变更优化脚本的下载地址。

下载地址：

- 华东-上海一：[https://sdi-resize-check-cn-east-3.obs.cn-east-3.myhuaweicloud.com:443/offload\\_check\\_blockdevice.sh](https://sdi-resize-check-cn-east-3.obs.cn-east-3.myhuaweicloud.com:443/offload_check_blockdevice.sh)
- 华北-北京四：[https://sdi-resize-check-cn-north-4.obs.cn-north-4.myhuaweicloud.com:443/offload\\_check\\_blockdevice.sh](https://sdi-resize-check-cn-north-4.obs.cn-north-4.myhuaweicloud.com:443/offload_check_blockdevice.sh)
- 华南-广州：[https://sdi-resize-check-cn-south-1.obs.cn-south-1.myhuaweicloud.com:443/offload\\_check\\_blockdevice.sh](https://sdi-resize-check-cn-south-1.obs.cn-south-1.myhuaweicloud.com:443/offload_check_blockdevice.sh)
- 乌兰察布一：[https://sdi-resize-check-cn-north-9.obs.cn-north-9.myhuaweicloud.com:443/offload\\_check\\_blockdevice.sh](https://sdi-resize-check-cn-north-9.obs.cn-north-9.myhuaweicloud.com:443/offload_check_blockdevice.sh)
- 西南-贵阳一：[https://sdi-resize-check-cn-southwest-2.obs.cn-southwest-2.myhuaweicloud.com:443/offload\\_check\\_blockdevice.sh](https://sdi-resize-check-cn-southwest-2.obs.cn-southwest-2.myhuaweicloud.com:443/offload_check_blockdevice.sh)

#### 📖 说明

若回显异常，请检查云服务器是否绑定弹性公网IP。除上述区域外，绑定弹性公网IP后才能获取脚本。

3. 执行以下命令，运行规格变更优化脚本，该脚本会自动检查云服务器是否可以变更为QingTian实例。

```
bash offload_check_blockdevice.sh
```

图 2-199 运行脚本

```
[root@ecs-10e8 ~]# bash offload_check_blockdevice.sh
2023-06-27 09:36:52 Info: -----
2023-06-27 09:36:52 Info: Begin to check and correct grub and fstab file
2023-06-27 09:36:52 Info: OK fstab file looks fine and does not contain any device names.
2023-06-27 09:36:52 Info: Search grub file...
2023-06-27 09:36:52 Info: Find grub file: /boot/grub2/grub.cfg
2023-06-27 09:36:52 Info: Check grub file: /boot/grub2/grub.cfg
2023-06-27 09:36:52 Info: OK /boot/grub2/grub.cfg file looks fine and does not contain any device names.
2023-06-27 09:36:52 Info: -----
[root@ecs-10e8 ~]#
```

请耐心等待脚本运行结束。如果回显提示“fstab file looks fine”，表示规格变更优化脚本执行成功，云服务器可以变更为QingTian实例。

### 说明

请务必确保云服务器配置成功，否则，可能会导致变更规格后的弹性云服务器不可用。

## 步骤 3：变更规格

1. 登录控制台。
2. 单击“”，选择“计算 > 弹性云服务器”。
3. 在弹性云服务器列表，查询待变更弹性云服务器状态。  
如果不是关机状态，单击“操作”列下的“更多 > 关机”。
4. 单击“操作”列下的“更多 > 变更规格”。  
系统进入“云服务器变更规格”页面。
5. 根据界面提示，选择变更后的云服务器类型、vCPU和内存。
6. （可选）选择“专属主机”。  
对于在专属主机上创建的弹性云服务器，系统支持更换云服务器所在的专属主机。  
此时，您可以单击下拉列表，选择更换专属主机。如果下拉列表中无可用的专属主机，说明专属主机所剩资源不足，不能用于创建变更规格后的弹性云服务器。
7. 勾选复选框“我确认已完成对弹性云服务器的配置”，确认已完成“配置弹性云服务器”操作。
8. 单击“下一步”。
9. 确认变更后的配置无误后，阅读并勾选同意服务协议，单击“提交申请”。

### 说明

- 单击“提交申请”后云平台自动为您制作系统盘快照。变更规格完成后，如已确认业务恢复正常，请在快照页面手动删除快照。
- 如果变更规格失败后，弹性云服务器无法使用，可能会需要重装操作系统来恢复云服务器，请注意重装操作系统会清除系统盘数据，但不影响数据盘的数据。

## （可选）步骤 4：检查磁盘挂载状态

KVM实例变更为QingTian实例时，可能会发生磁盘挂载失败的情况，因此，变更规格后，需检查磁盘挂载状态是否正常。如果正常，则变更成功。

- Linux弹性云服务器  
详细操作请参考[Linux云服务器变更规格后数据盘脱机怎么办？](#)

## 后续处理

如果控制台上云服务器列表页，显示弹性云服务器已变更规格成功，但是远程登录云服务器后，操作系统无法启动。此时，请联系客服进行恢复，或重装操作系统。重装系统的操作指导，请参见[重装操作系统](#)。

### 说明

重装操作系统会清除系统盘数据，但不影响数据盘的数据。

变更规格完成后，如已确认业务恢复正常，请在快照页面手动删除快照。



## 2.9 变更 ECS 操作系统

### 2.9.1 重装操作系统

#### 操作场景

弹性云服务器操作系统无法正常启动时，或云服务器系统运行正常，但需要对系统进行优化，使其在最优状态下工作时，用户可以使用重装弹性云服务器的操作系统功能。

#### 重装须知

- 重装操作系统后弹性云服务器IP地址和MAC地址不发生改变。
- 重装操作系统会清除系统盘数据，包括系统盘上的系统分区和所有其他分区，请做好数据备份。
- 重装操作系统不影响数据盘数据。
- 重装操作系统后的几分钟，系统正在注入密码或密钥信息，在此期间请勿对云服务器执行其他操作，避免密码或密钥信息注入失败导致云服务器无法登录。
- Windows操作系统云服务器，如果重装操作系统时设置了新密码，本地保存的RDP文件已失效，请重新下载RDP文件登录云服务器。

#### 约束与限制

- 云硬盘的配额需大于0。
- 如果是通过私有镜像创建的弹性云服务器，请确保原有镜像仍存在。
- 如果原有云服务器计费方式为按需模式，请确认账户余额充足。
- 如果原有云服务器计费方式为包年/包月模式，请确保在有效期内。
- H2型弹性云服务器不支持操作系统的重装功能。

#### 前提条件

- 待重装操作系统的弹性云服务器挂载有系统盘。

#### 操作步骤

1. 登录管理控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”。
4. 在待重装操作系统的弹性云服务器的“操作”列下，单击“更多 > 镜像 > 重装操作系统”。  
重装操作系统前请先将云服务器关机，或根据页面提示勾选“立即关机（重装操作系统前需先将云服务器关机）”。
5. 设置登录方式。  
如果待重装操作系统的弹性云服务器是使用密钥登录方式创建的，此时可以更换使用新密钥。



图 2-200 重装操作系统



6. 单击“确定”。
7. 在“重装操作系统”页面，确认重装的操作系统规格无误后，阅读并勾选协相关协议或声明，单击“提交申请”。
- 提交申请后，弹性云服务器的状态变为“重装中”，当该状态消失后，表示重装结束。

说明

重装操作系统过程中，会创建一台临时弹性云服务器，重装操作系统结束后会自动删除。在重装操作系统过程中请不要对该弹性云服务器进行任何操作。

后续处理

如果操作系统重装失败，页面会提示重装操作系统失败。云服务平台支持重试功能，用户可重新执行3-7，重装弹性云服务器的操作系统。

重试后，如果仍未成功，可直接联系客服，客服会在后台进行人工恢复。

2.9.2 切换操作系统

操作场景

切换操作系统是为您的弹性云服务器重新切换一个系统盘。切换完成后弹性云服务器的系统盘ID会发生改变，并删除原有系统盘。

如果弹性云服务器当前使用的操作系统不能满足业务需求（如软件要求的操作系统版本较高），您可以选择切换弹性云服务器的操作系统。

云服务平台支持不同镜像类型（包括公共镜像、私有镜像、共享镜像以及市场镜像）与不同操作系统之间的互相切换。您可以将现有的操作系统切换为不同镜像类型的操作系统。

## 约束与限制

- 切换操作系统操作预计需等待1~4分钟。切换操作系统过程中，弹性云服务器会显示任务状态为“切换操作系统中”。
- 切换操作系统完成后的几分钟，系统正在注入密码或密钥信息，在此期间请勿对云服务器执行其他操作，避免密码或密钥信息注入失败导致云服务器无法登录。
- 待切换操作系统的弹性云服务器需挂载有系统盘。
- “包年/包月”方式购买的弹性云服务器切换操作系统时，由于所选镜像不同，当前云服务器的系统盘容量可能不足，不支持切换后的镜像使用。此时，需先卸载系统盘并进行扩容，然后再重新切换操作系统。
- “包年/包月”方式购买的弹性云服务器切换操作系统时，支持如下场景：
  - 支持Linux操作系统之间互相切换。
  - 支持Linux操作系统与由伊登公司提供的Windows标准操作系统互相切换。
  - 支持由伊登公司提供的Windows标准操作系统不同版本之间互相切换。

### 说明

- “包年/包月”方式购买的弹性云服务器，除了由伊登公司提供的Windows标准操作系统之外，仅支持由免费的操作系统切换至免费的操作系统。
- 使用源镜像为市场镜像（除了由伊登公司提供的Windows标准操作系统）的私有镜像创建，且购买方式为“包年/包月”的云服务器不支持切换操作系统。
- 仅中国大陆区域的“包年/包月”方式购买的弹性云服务器支持“Linux操作系统与由伊登公司提供的Windows标准操作系统互相切换”和“由伊登公司提供的Windows标准操作系统不同版本之间互相切换”这两个场景。  
支持的区域包括：华北-北京一、华北-北京四、华北-乌兰察布一、华东-上海一、华东-上海二、华南-广州、华南-广州-友好用户环境、华南-深圳、西南-贵阳一。
- 云硬盘的配额需大于0。
- 不支持更换系统盘的磁盘类型。
- H2型弹性云服务器不支持操作系统的切换功能。
- 不支持使用ISO文件创建的ISO镜像切换操作系统，必须完成操作系统和驱动安装将ISO镜像做成系统盘镜像后才能使用。
- 不支持BIOS启动方式与UEFI启动方式的操作系统互相切换。
- 不支持x86架构的弹性云服务器切换为鲲鹏架构类型的操作系统，也不支持鲲鹏架构的弹性云服务器切换到x86架构类型的操作系统。

## 切换须知

切换操作系统后，弹性云服务器的原操作系统和系统盘均不再保留，您的业务运行环境也需要在新的操作系统中重新部署，可能造成较长时间的业务中断，因此，在进行操作前，请仔细阅读切换须知并谨慎操作。

表 2-63 切换须知

| 资源及环境            | 切换操作系统后影响                                                                                                                                                                                                                                                                                                |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 操作系统             | 不保留原操作系统。<br>当进行不同操作系统间的切换时： <ul style="list-style-type: none"><li>Windows系统切换为Linux系统：需安装读写Windows系统的NTFS分区工具，例如NTFS-3G等。</li><li>Linux系统切换为Windows系统：需安装可以识别ext3、ext4等分区的识别软件，例如Ext2Read、Ext2Fsd等。</li></ul> <b>说明</b><br>当Linux系统中存在LVM分区时，切换为Windows系统后可能会导致LVM逻辑分区无法识别。因此，不建议您将Linux系统更换为Windows系统。 |
| 实例规格             | 不变。                                                                                                                                                                                                                                                                                                      |
| 系统盘              | <ul style="list-style-type: none"><li>由于所选镜像不同，系统盘的容量可能会增大。</li><li>系统盘磁盘类型不变，系统盘ID变化。</li><li>删除原系统盘，并清除系统盘数据，包括系统盘上的所有分区数据和创建的所有快照。<br/>请提前做好数据备份。详细内容，请参考<a href="#">备份弹性云服务器</a>。</li></ul>                                                                                                          |
| 数据盘              | 不影响数据盘数据。                                                                                                                                                                                                                                                                                                |
| IP地址和MAC地址       | 不变。                                                                                                                                                                                                                                                                                                      |
| 个性化设置（如DNS、主机名等） | 个性化设置会被重置，需重新配置。 <ul style="list-style-type: none"><li>重新配置云服务器DNS信息请参考：<a href="#">怎样配置弹性云服务器的DNS和NTP信息？</a></li><li>重新配置主机名请参考：<a href="#">怎样使修改的静态主机名永久生效？</a></li></ul>                                                                                                                              |
| 运行状态             | 自动开机。                                                                                                                                                                                                                                                                                                    |
| 本地保存的RDP文件       | 对于Windows操作系统的云服务器，如果切换操作系统时设置了新密码，则本地保存的RDP文件会失效，需重新下载RDP文件登录云服务器。                                                                                                                                                                                                                                      |
| 业务运行环境           | 需要在新的系统中重新部署。                                                                                                                                                                                                                                                                                            |

计费规则

- 切换操作系统功能不收费。按需计费的云服务器切换成功后，系统将按照新的配置费用（系统盘、规格、市场镜像）进行计费。
- “按需付费”方式购买的弹性云服务器切换操作系统后，由于所选镜像不同，系统盘的容量可能会增大，由此将带来费用的变更，具体收费请参见[产品价格详情](#)。

前提条件

- 完成云服务器的数据备份。  
详细内容，请参见[备份弹性云服务器](#)。

- 若在切换操作系统过程中，要将云服务器的登录鉴权方式由密码改为密钥，请提前创建密钥文件。  
详细内容，请参见（推荐）[通过管理控制台创建密钥对](#)。
- 如果您使用私有镜像切换操作系统请参考《[镜像服务用户指南](#)》提前完成私有镜像的制作。
  - 如果需要指定弹性云服务器的镜像，请提前使用指定弹性云服务器创建私有镜像。
  - 如果需要使用本地的镜像文件，请提前将镜像文件导入并注册为云平台的私有镜像。
  - 如果需要使用其他区域的私有镜像，请提前复制镜像。
  - 如果需要使用其他账号的私有镜像，请提前完成镜像共享。

## 操作步骤

1. 登录管理控制台。
  2. 单击管理控制台左上角的 ，选择区域和项目。
  3. 单击“”，选择“计算 > 弹性云服务器”。
  4. 在待切换操作系统的弹性云服务器的“操作”列下，单击“更多 > 镜像 > 切换操作系统”。
- 切换操作系统前请先将云服务器关机，或根据页面提示勾选“立即关机（切换操作系统前需先将云服务器关机）”。
5. 根据需求选择需要切换的弹性云服务器镜像。

### 说明

对于“包年/包月”方式购买的弹性云服务器，如果当前操作系统的系统盘容量小于目标操作系统的系统盘容量时，您需要先卸载系统盘，并进行扩容，然后再挂载至原弹性云服务器执行切换操作。

扩容系统盘的操作指导，请参见“[扩容云硬盘](#)”章节。

图 2-201 切换操作系统

切换操作系统

切换操作系统提供以用户选择的镜像进行重装系统的功能。

1、切换操作系统不影响数据盘数据，但是系统盘的所有分区数据和创建的所有快照会被删除，请做好数据备份。

2、部分操作系统不支持挂载SCSI磁盘，切换操作系统后，可能会导致原弹性云服务器上挂载的SCSI磁盘不可用。[查看支持列表](#)

3、切换操作系统成功后，云服务器会自动开机；当前操作系统内的个性化设置（如DNS、主机名等）将被重置，需重新配置。

[收起说明](#)

当前配置

| 云服务器名称   | IP地址                | 规格                  | 镜像                        | 系统盘   |
|----------|---------------------|---------------------|---------------------------|-------|
| ecs-7004 | 192.168.0.93 (私有IP) | 1vCPUs   1GiB   ... | CentOS 7.5 64bit (64-bit) | 40GiB |

☐ 立即关机 (切换操作系统前需先将云服务器关机)

镜像

公共镜像私有镜像共享镜像市场镜像

-请选择操作系统-

-请选择操作系统版本-

登录凭证

密码密钥对

密码

请输入密码

可使用云服务器原密码或重新设置密码。请输入并牢记密码。

确认密码

请再次输入密码

取消确定

6. 设置登录方式。
- 如果待切换操作系统的弹性云服务器是使用密钥登录方式创建的，此时可以更换使用新密钥。
- 使用私有镜像切换操作系统时，可以选择使用私有镜像密码。
7. 单击“确定”。
8. 在“确认切换云服务器操作系统”页面，确认切换的操作系统规格无误后，阅读并勾选相关协议或声明，单击“确定”。
- 提交切换操作系统的申请后，弹性云服务器的状态变为“切换操作系统中”，当该状态消失后，表示切换结束。

说明

切换操作系统过程中，会创建一台临时弹性云服务器，切换操作系统结束后会自动删除。

后续处理

- 如果切换操作系统前后都是Linux系统，且数据盘设置了开机自动挂载分区。切换操作系统后，数据盘分区挂载信息会丢失，请更新/etc/fstab配置。
  - 在/etc/fstab写入切换后的分区信息。

建议您先备份/etc/fstab文件。

详细操作请参考[初始化Linux数据盘（fdisk）](#)，设置开机自动挂载磁盘分区。
  - 挂载分区。挂载分区后即可开始使用数据盘。

**mount 磁盘分区 挂载目录**
  - 执行以下命令，查看挂载结果。

**df -TH**

- 如果操作系统切换失败，云服务平台支持重试功能，用户可重新执行3-8，切换弹性云服务器的操作系统。
- 重试后，如果仍未成功，可直接联系客服，客服会在后台进行人工恢复。

## 2.10 查看 ECS 信息

### 2.10.1 查看 ECS 创建状态

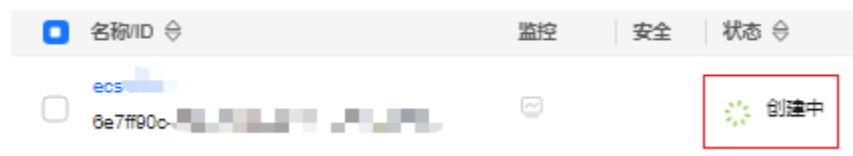
#### 操作场景

用户申请创建弹性云服务器后，可以查看任务的创建状态。本节介绍如何查看弹性云服务器的创建状态。

#### 操作步骤

1. 登录管理控制台。
2. 单击管理控制台左上角的，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”。
4. 用户执行购买弹性云服务器操作后，在列表的“状态”列，可查看该任务的“创建中”状态。

图 2-202 申请状态



#### 说明

- 创建云服务器存在以下状态：
  - 创建中：指系统正在处理创建云服务器的请求。
  - 创建失败：指未能成功处理的请求。对于创建失败的任务，系统会自动回退，同时在界面上直观的展示错误码，例如“（Ecs.0013）EIP配额不足”。
  - 运行中：成功处理创建云服务器的请求，是弹性云服务正常运行的状态。在这个状态的云服务器可以运行您的业务。
- 如果用户发现申请状态栏显示创建弹性云服务器的任务失败，而弹性云服务器列表中显示该弹性云服务器已创建成功，关于此问题请参见[为什么创建弹性云服务器的任务失败，但是在云服务器列表中显示创建成功](#)。

### 2.10.2 查看 ECS 失败任务

#### 操作场景

“失败信息”栏记录了系统处理中发生异常，导致处理失败的任务，包括该任务的“名称”、“状态”等信息。当有处理失败的操作时，控制台将显示该内容。本节介绍如何查看“失败信息”。

失败信息事件类型

“失败信息”栏记录的失败信息事件类型如表2-64所示。

表 2-64 失败信息事件类型

| 事件类型 | 说明                                                                                               |
|------|--------------------------------------------------------------------------------------------------|
| 创建失败 | 指未能成功处理的请求。对于创建失败的任务，系统会自动回退，同时在界面上直观的展示错误码，例如“（ Ecs.0013 ）EIP配额不足”。                             |
| 操作失败 | <ul style="list-style-type: none"><li>变更规格<br/>用户申请变更规格后，如果规格变更失败，则“失败信息”栏将显示本次变更规格操作。</li></ul> |

操作步骤

1. 登录管理控制台。
2. 单击管理控制台左上角的，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”。
4. 常用操作“开机/关机/重启/更多”的右侧即为“失败信息”。

图 2-203 失败任务



5. 单击“失败信息”栏对应的数字，即可查看系统处理失败的任务详情。其中：
  - 创建失败：您可以从创建失败的列表中查看创建中和创建失败的任务。
  - 操作失败：您可以从操作失败列表中查看处理异常的任务，包括异常任务的具体操作、错误码等，便于定位系统处理异常的原因，及时予以恢复。

2.10.3 查看 ECS 详细信息（列表视图）

操作场景

在您申请了弹性云服务器后，可以通过管理控制台查看和管理您的弹性云服务器。本节介绍如何查看弹性云服务器的详细配置，包括弹性云服务器名称、镜像信息、系统盘、数据盘、虚拟私有云、网卡、安全组、弹性公网IP地址和带宽等信息。

如需查看弹性云服务器的私有IP地址，请直接在弹性云服务器列表页进行查看。



操作步骤

1. 登录管理控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”。
- 系统进入弹性云服务器列表页，您可以在本页面查看您已购买的弹性云服务器，以及弹性云服务器的规格、镜像、IP地址等基本信息。
- 您可以设置列表可显示的弹性云服务器信息：
- a. 在列表搜索框右侧，单击 ，进入“设置”页面。
- b. 在“自定义显示列”勾选想要显示在弹性云服务器列表的信息。

图 2-204 自定义列表显示项

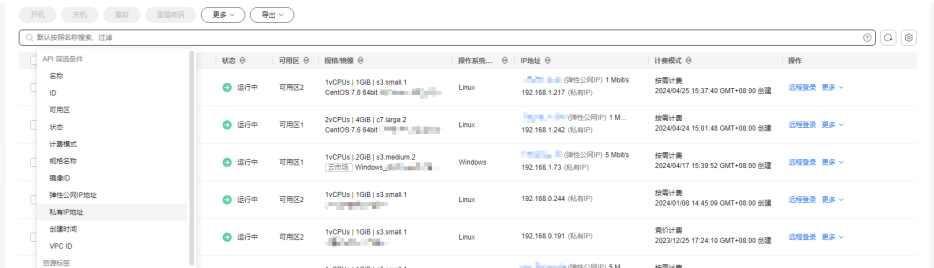


 说明

- 切换区域后，弹性云服务器列表展示信息设置会保留。
4. 在弹性云服务器列表中的上方，输入弹性云服务器名称、云服务器ID、IP地址等属性类型，并按回车键进行搜索。
- 搜索云服务器的更多内容，请参见或[搜索ECS](#)。



图 2-205 搜索弹性云服务器



5. 单击待查询弹性云服务器的名称。  
系统跳转至该弹性云服务器详情页面。
6. 查看弹性云服务器的详细信息。  
您可以选择“云硬盘/弹性网卡/安全组/弹性公网IP/监控/标签”页签，为弹性云服务器进行[更改安全组](#)、[绑定弹性网卡](#)、[绑定弹性公网IP](#)、[添加标签](#)等操作。

2.10.4 查看 ECS 详细信息（精简视图）

操作场景

精简视图提供了云服务器资源概况和状态的可视化统计结果，帮助您直观的了解云服务器资源。在精简视图中，您可以快速获取弹性云服务器基本信息、登录信息、配置信息、监控信息。

怎样切换至精简视图？

精简视图提供了云服务器资源概况和状态的可视化统计结果，直观的了解云服务器资源。

请按以下步骤切换至精简视图：

1. 登录管理控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”。
- 系统进入弹性云服务器列表页。
4. 在列表页切换进入精简视图。
- a. 在列表搜索框右侧，单击 ，进入“设置”页面。
- b. “视图切换”设置为“精简视图”。

在精简视图下用户可查看弹性云服务器的详细配置，包括弹性云服务器名称、登录信息指引、云服务器详情、云服务器监控数据。

在精简视图查看云服务器资源信息

在精简视图中，您可以快速获取弹性云服务器基本信息、登录信息、配置信息、监控信息。

表 2-65 云服务器资源信息

| 信息分类   | 描述                                                                                                                                                                               |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 基本信息   | 基本信息包括云服务器名称、状态、云服务器ID、计费模式，同时提供关机、重启、变更计费模式等操作入口。 <ul style="list-style-type: none"><li>按需资源：按需资源费用较高，需要长期使用可以选择对按需资源进行转包年/包月。</li><li>包年/包月资源：控制台会提示您资源到期时间，并提供续费链接。</li></ul> |
| 登录信息   | <ul style="list-style-type: none"><li>远程登录：通过管理控制台远程登录入口。</li><li>客户端登录：提供客户端登录云服务器的必要信息，包括弹性公网IP、登录用户名、登录操作指引。</li></ul>                                                        |
| 配置信息   | 云服务器的配置信息包括云服务器规格、镜像、系统盘信息、数据盘信息，私有IP地址、弹性公网IP地址、安全组等信息，同时提供变更规格、切换操作系统等操作入口。                                                                                                    |
| 监控信息   | 云服务器运行相关的信息，包括CPU和网络使用情况。您可以选择页面左上方的时间范围按钮，查看该云服务资源“近1小时”、“近3小时”、“近12小时”、“近24小时”、“近7天”、“近30天”的监控原始数据曲线图。                                                                         |
| 监控信息总览 | 精简视图中监控视图总览从性能、安全、成本三方面帮助您监控云服务器健康程度。当监控指标异常时，提供异常信息及解决方案。                                                                                                                       |

2.10.5 导出 ECS 列表信息

操作场景

您可以将当前账号下拥有的所有弹性云服务器信息，以.xlsx文件的形式导出至本地。该文件记录了弹性云服务器的如下信息：

- 基本信息：名称、区域、可用区、状态、规格、镜像、计费模式等信息。
- 网络信息：私有IP地址、弹性公网IP、VPC、子网、安全组等信息。
- 磁盘信息：磁盘数量、磁盘属性、磁盘容量等信息。

操作步骤

1. 登录管理控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”。
4. 在弹性云服务器列表页左上角，单击“导出”，导出列表。

图 2-206 导出弹性云服务器列表



系统会将您账号下，当前区域的所有弹性云服务器信息自动导出，并下载至本地。

#### 说明

- 您可以在[云服务器控制台](#)导航栏的最下端，单击“切换新版/切换旧版”进行新版和旧版控制台的切换。
  - 如需导出部分弹性云服务器的信息，请勾选对应的弹性云服务器，然后再进行导出操作。
5. 在本地计算机桌面的默认下载地址文件夹，可以获取到导出的弹性云服务器列表信息。

## 2.10.6 搜索 ECS（旧版）

### 操作场景

购买弹性云服务器后，可以通过管理控制台提供的搜索功能快速检索当前区域的云服务器资源。本节操作介绍搜索云服务器的操作步骤。当前支持使用名称、云服务器ID、可用区、状态、规格名称、镜像ID、弹性公网IP地址、私有IP地址、创建时间、计费模式、VPC ID、企业项目、标签以上属性进行搜索。单击搜索框右侧的可以设置系统的默认搜索属性。

### 搜索语法

弹性云服务器支持多种类型的搜索，详细的说明和示例请参考[表2-66](#)。

#### 说明

- 部分属性支持系统自动匹配属性搜索，但必须输入完整的属性值。
- 选择属性搜索时，以下属性仅支持精确搜索，需输入完整的属性值：云服务器ID、镜像ID、弹性公网IP地址、VPC ID。
- 多值搜索时私有IP地址也必须使用精确搜索，需输入完整的属性值。
- 私有IP地址的网段需在以下范围内：10.0.0.0/8-24，172.16.0.0/12-24，192.168.0.0/16-24。
- 按标签过滤时可选择键或键值对搜索。支持设置多个标签，如果键不同，则标签按“与”的关系搜索。如果键相同，值不同，则标签按“与”的关系搜索。
- 未选择属性的时候标签不支持多值搜索。
- 私有IP和弹性公网IP不能同时搜索。

表 2-66 搜索语法

| 搜索类型              | 支持的属性                                              | 输入格式            | 示例                                                                                                                 | 说明                                                                                               |
|-------------------|----------------------------------------------------|-----------------|--------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| 属性值<br>自动匹配<br>属性 | 云服务器ID、规格名称、私有IP地址、弹性公网IP地址、标签（标签不支持输入多值。）         | 完整的属性值          | 云服务器ID：<br>4a79dfec-f0d8-4181-9bef-495b8b7220e1，<br>规格名称：<br>s2.xlarge.4<br>私有IP地址：<br>192.168.9.231<br>标签：<br>a=b | 使用关键字搜索时，不需要选择属性，仅输入完整的属性值，系统自动匹配属性类型进行搜索。<br><br>多个取值使用“,”分隔。否则后输入的取值会替换之前输入的取值。多个属性值之间为“或”的关系。 |
| 单属性               | 控制台支持的所有属性                                         | 属性：属性值          | 状态：运行中                                                                                                             | 选择属性后，输入/选择对应的属性信息。<br><br>以下属性仅支持精确搜索，需输入完整的属性值：云服务器ID、弹性公网IP地址、镜像ID、VPC ID。                    |
| 多属性               | 控制台支持的所有属性                                         | 属性：取值<br>&属性：取值 | 状态：运行中<br>名称：ecs-c                                                                                                 | 支持选择多个不同的属性，搜索时多个属性为“与”的关系。<br><br>以下属性仅支持精确搜索，需输入完整的属性值：云服务器ID、弹性公网IP地址、镜像ID、VPC ID。            |
| 单属性、多值            | 状态、云服务器ID、规格名称、私有IP地址、弹性公网IP地址、计费模式、标签（标签不支持输入多值。） | 属性：取值1 取值2      | 规格名称：s2,s3<br>私有IP地址：<br>192.168.0.19,192.168.111.111                                                              | 选择一个属性后，输入多个取值，多个取值之间为“或”的关系。<br><br>以下属性仅支持精确搜索，需输入完整的属性值：云服务器ID、私有IP地址、弹性公网IP地址。               |

| 搜索类型   | 支持的属性                                              | 输入格式                 | 示例                | 说明                                                                                                       |
|--------|----------------------------------------------------|----------------------|-------------------|----------------------------------------------------------------------------------------------------------|
| 多属性、多值 | 状态、云服务器ID、规格名称、私有IP地址、弹性公网IP地址、计费模式、标签（标签不支持输入多值。） | 属性：取值<br>&属性：取值1 取值2 | 状态：运行中&规格名称：s2,s3 | 选择多个“属性：取值,取值”的搜索方式，属性之间为“与”的关系。同一属性的多个取值之间为“或”的关系。<br><br>以下属性仅支持精确搜索，需输入完整的属性值：云服务器ID、私有IP地址、弹性公网IP地址。 |

操作步骤

1. 登录管理控制台。
2. 单击“”，选择“计算 > 弹性云服务器”。系统进入弹性云服务器列表页。
3. 在搜索的输入框中，设置搜索条件。

图 2-207 搜索弹性云服务器



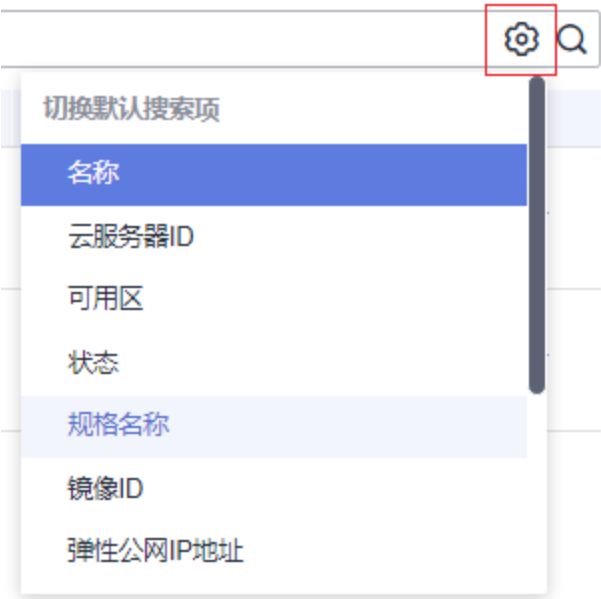
您可以根据需要，选择并设置合适的搜索条件。

- 在搜索框直接输入属性值，系统自动识别属性并搜索。
- 设置默认搜索项进行搜索。
  - i. 在搜索框右侧，单击，在搜索项列表中选择要设置的默认搜索项。

说明

切换区域后，搜索栏中设置的默认搜索项信息会保留。

图 2-208 切换默认搜索项



- ii. 根据提示输入搜索关键字，并单击  进行搜索。
- 设置搜索属性类型进行搜索。
  - i. 单击搜索框，在列表中选择搜索的属性类型。

图 2-209 设置搜索属性类型



- ii. 根据提示信息，在搜索栏中输入或选择搜索条件，例如云服务器ID、云服务器状态、规格名称等，并单击  进行搜索。

## 示例 1：使用属性值搜索，系统自动匹配属性

输入完整的属性值后，系统自动识别属性并搜索。多个取值使用“,”分隔，否则后输入的取值会替换之前输入的取值。多个属性值之间为“或”的关系。

- 单值搜索：

在云服务器列表页搜索的输入框中输入完整云服务器ID，单击  进行搜索。

图 2-210 输入完整的云服务器 ID

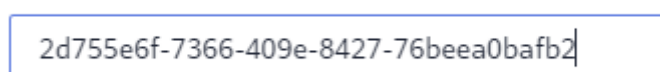
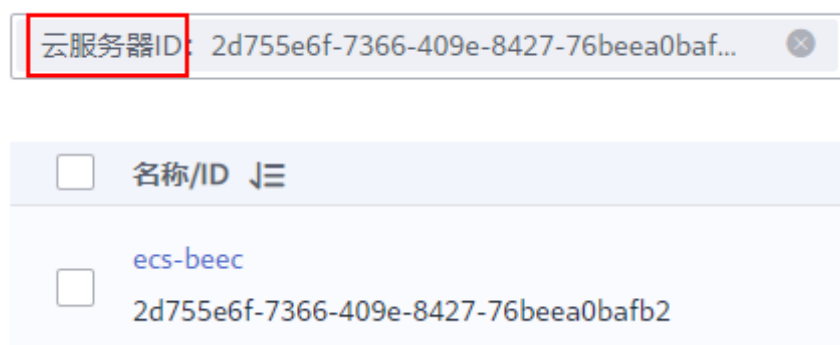


图 2-211 系统自动匹配属性



- 多值搜索：

在云服务器列表页搜索的输入框中输入完整的规格名称，单击  进行搜索。

图 2-212 输入多个完整的规格名称



图 2-213 系统自动匹配属性并搜



## 示例 2：单属性搜索

选择属性后，输入/选择对应的属性信息。

以下属性仅支持精确搜索，需输入完整的属性值：云服务器ID、镜像ID、弹性公网IP地址、VPC ID。

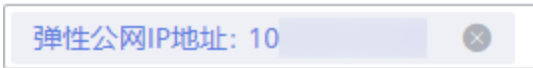
- 模糊搜索：使用私有IP地址搜索
  - a. 在云服务器列表页搜索的输入框中选择“私有IP地址”。
  - b. 根据提示，输入私有IP地址，单击 进行搜索。“私有IP地址”支持模糊搜索，例如输入“192.168.0”，可以搜索到所有使用192.168.0网段的云服务器。

图 2-214 按私有 IP 地址搜索云服务器



- 精确搜索：使用弹性公网IP地址搜索
  - a. 在云服务器列表页搜索的输入框中选择“弹性公网IP地址”。
  - b. 根据提示，输入完整弹性公网IP地址，单击 进行搜索。

图 2-215 按弹性公网 IP 地址搜索云服务器



示例 3：多属性搜索

支持选择多个不同的属性，搜索时多个属性为“与”的关系。

以下属性仅支持精确搜索，需输入完整的属性值：云服务器ID、弹性公网IP地址、镜像ID、VPC ID。

本例同时使用“云服务器名称”和“私有IP地址”进行搜索。

- 在云服务器列表页搜索的输入框中选择“云服务器名称”并输入取值。单击 进行搜索。本例云服务器名称使用模糊搜索。
- 添加筛选属性条件，选择“私有IP地址”，根据提示输入私有IP地址，单击 进行搜索。本例私有IP地址使用模糊搜索。

图 2-216 按私有 IP 地址搜索云服务器

| 名称: ecs-f                                              |    | 私有IP地址: 192.168.12 |     | 添加筛选条件                      |                    |  |
|--------------------------------------------------------|----|--------------------|-----|-----------------------------|--------------------|--|
| <input type="checkbox"/> 名称/ID                         | 监控 | 可用区                | 状态  | 规格/镜像                       | IP地址               |  |
| <input type="checkbox"/> ecs-f6d8d189a-068b-4f07...    |    | 可用区2               | 关机  | 1vCPUs   2GiB   s2.medium.2 | 192.168.128.121... |  |
| <input type="checkbox"/> ecs-f6b33e20a97a-e108-437c... |    | 可用区2               | 运行中 | 1vCPUs   2GiB   s2.medium.2 | 192.168.125.168... |  |

示例 4：单属性、多值搜索

仅以下属性支持单属性、多值搜索：状态、云服务器ID、规格名称、私有IP地址、弹性公网IP地址、计费模式、标签。



其中以下属性仅支持精确搜索，需输入完整的属性值：云服务器ID、私有IP地址、弹性公网IP地址。

选择一个属性后，输入多个取值，多个取值之间为“或”的关系。

- 模糊搜索
  - 在云服务器列表页搜索的输入框中选择“规格名称”。
  - 根据提示输入多个规格名称，使用“,”分隔，单击 进行搜索。

图 2-217 按规格名称搜索云服务器



- 精确搜索
  - 在云服务器列表页搜索的输入框中选择“私有IP地址”。
  - 根据提示输入多个完整的私有IP地址，使用“,”分隔，单击 进行搜索。

图 2-218 按私有 IP 地址搜索云服务器



示例 5：多属性、多值搜索

仅以下属性支持多属性、多值搜索：状态、云服务器ID、规格名称、私有IP地址、弹性公网IP地址、计费模式、标签。

其中以下属性仅支持精确搜索，需输入完整的属性值：云服务器ID、私有IP地址、弹性公网IP地址。

选择多个“属性：取值,取值”的搜索方式，属性之间为“与”的关系。同一属性的多个取值之间为“或”的关系。

- 模糊搜索
  - 在云服务器列表页搜索的输入框中选择“状态”，并选择“运行中”、“关机”，单击 进行搜索。
  - 添加筛选属条件，选择“规格名称”，输入多个规格名称，使用“,”分隔，单击 进行搜索。

图 2-219 按状态和规格名称搜索云服务器



- 精确搜索
  - a. 在云服务器列表页搜索的输入框中选择“状态”，并选择“运行中”、“关机”，单击 进行搜索。
  - b. 添加筛选属条件，选择“私有IP地址”，根据提示输入多个完整的私有IP地址，使用“,” 分隔，单击 进行搜索。

图 2-220 按状态和私有 IP 地址搜索云服务器



示例 6：按标签搜索

按标签过滤时可选择键或键值对搜索。

支持设置多个标签，如果键不同，则标签按“与”的关系搜索。

如果键相同，值不同，则标签按“与”的关系搜索。

- 单个标签搜索

在云服务器列表页搜索的输入框中选择“标签”，选择标签键值对，单击“确认”进行搜索。

图 2-221 按标签搜索云服务器



- 多个标签搜索

在云服务器列表页搜索的输入框中选择“标签”，选择多个标签键值对，单击“确认”进行搜索。

按“与”的关系搜索，搜索同时具备这两个标签的云服务器。

图 2-222 按标签搜索云服务器



## 2.10.7 搜索 ECS

### 操作场景

购买弹性云服务器后，可以通过管理控制台提供的搜索功能快速检索当前区域的云服务器资源。本节操作介绍搜索云服务器的操作步骤。当前支持使用名称、ID、可用区、状态、规格名称、镜像ID、弹性公网IP地址、私有IP地址(IPv4/IPv6)、创建时间、计费模式、VPC ID、企业项目、资源标签等属性进行搜索。

### 搜索语法

弹性云服务器支持多种类型的搜索，详细的说明和示例请参考[表2-67](#)。

#### 说明

- 部分属性支持系统自动匹配属性搜索，但必须输入完整的属性值。
- 选择属性搜索时，以下属性仅支持精确搜索，需输入完整的属性值：ID、镜像ID、弹性公网IP地址、VPC ID、企业项目。
- 多值搜索时私有IP地址也必须使用精确搜索，需输入完整的属性值。
- 私有IP地址的网段需在以下范围内：10.0.0.0/8-24，172.16.0.0/12-24，192.168.0.0/16-24。
- 按标签过滤时可选择键或键值对搜索。支持设置多个标签，如果键不同，则标签按“与”的关系搜索。如果键相同，值不同，则标签按“与”的关系搜索。
- 未选择属性的时候标签不支持多值搜索。
- 私有IP和弹性公网IP不能同时搜索。

表 2-67 搜索语法

| 搜索类型              | 支持的属性                            | 格式     | 示例                                                                                              | 说明                                                                                               |
|-------------------|----------------------------------|--------|-------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| 属性值<br>自动匹配<br>属性 | ID<br>规格名称<br>弹性公网IP地址<br>私有IP地址 | 完整的属性值 | ID:<br>4a79dfec-f0d8-4181-9bef-495b8b7220e1<br>规格名称:<br>s2.xlarge.4<br>私有IP地址:<br>192.168.9.231 | 使用关键字搜索时，不需要选择属性，仅输入完整的属性值，系统自动匹配属性类型进行搜索。<br><br>多个取值使用“,”分隔。否则后输入的取值会替换之前输入的取值。多个属性值之间为“或”的关系。 |

| 搜索类型        | 支持的属性                  | 格式               | 示例                                                                                                 | 说明                                                                            |
|-------------|------------------------|------------------|----------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| 属性值<br>模糊搜索 | 名称<br>私有IP地址<br>规格名称   | 属性：不完整的属性值       | 名称：<br>ecs-c<br>规格名称：s7n<br>私有IP地址：<br>192.168.0                                                   | 选择属性后，输入对应的属性信息。                                                              |
| 单属性         | 控制台支持的所有属性             | 属性：属性值           | 私有IP地址：<br>192.168.9<br>9.231                                                                      | 选择属性后，输入或选择对应的属性信息。<br>以下属性仅支持精确搜索，需输入完整的属性值：ID、弹性公网IP地址、镜像ID、VPC ID。         |
| 多属性         | 控制台支持的所有属性             | 属性1：取值<br>属性2：取值 | 私有IP地址：<br>192.168.9<br>9.231 名称：<br>ecs-c                                                         | 支持选择多个不同的属性，搜索时多个属性为“与”的关系。<br>以下属性仅支持精确搜索，需输入完整的属性值：ID、弹性公网IP地址、镜像ID、VPC ID。 |
| 单属性、多值      | ID<br>规格名称<br>弹性公网IP地址 | 属性：取值1,取值2       | ID：<br>624eda28-6bd9-402a-934b-26c8969f7169,bf6c0281-f749-42d7-b732-23ac69d80ebe<br>规格名称：<br>s2,s3 | 选择一个属性后，输入多个取值，多个取值之间为“或”的关系。<br>以下属性仅支持精确搜索，需输入完整的属性值：ID。                    |
|             | 状态<br>计费模式             | 属性：取值1<br>属性：取值2 | 状态：运行中<br>状态：关闭                                                                                    | 选择一个属性后，勾选多个取值，多个取值之间为“或”的关系。                                                 |

| 搜索类型   | 支持的属性                           | 格式                         | 示例                                                                                          | 说明                                                                                                                                                                     |
|--------|---------------------------------|----------------------------|---------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 多属性、多值 | ID、规格名称、状态、弹性公网IP地址、私有IP地址、计费模式 | 属性1：取值1,取值2<br>属性2：取值1,取值2 | ID：<br>624eda28-6bd9-402a-934b-26c8969f7169,bf6c0281-f749-42d7-b732-23ac69d80ebe 规格名称：s2,s3 | 选择多属性、多值搜索时： <ul style="list-style-type: none"><li>多个属性之间为“与”的关系。</li><li>同一属性的多个取值之间为“或”的关系。</li></ul> 以下属性仅支持精确搜索，需输入完整的属性值：ID。<br>以下属性的多个值之间支持使用“ ”分隔或直接勾选：状态、计费模式。 |

操作步骤

1. 登录管理控制台。
2. 单击“”，选择“计算 > 弹性云服务器”。
- 系统进入弹性云服务器列表页。
3. 在搜索的输入框中，设置搜索条件。
- 您可以根据需要，选择并设置合适搜索条件。
- 在搜索框直接输入属性值，系统自动识别属性并搜索。

- 设置搜索属性类型进行搜索。

i. 单击搜索框，在列表中选择搜索的属性类型。

图 2-223 设置搜索属性类型



- ii. 根据提示，在搜索栏中选择属性值直接搜索，或者输入属性值后单击回车键进行搜索。

## 4. （可选）在搜索栏中修改搜索条件。

完成ECS实例搜索后，如果需要按照其他的属性类型或值重新搜索，可修改搜索条件。

- 单击搜索栏中需要修改的搜索条件。
- 在“属性类型”下拉框中输入或选择搜索属性，在“值”下拉框中输入或选择搜索值。
- 单击“确定”，系统将按照新的搜索条件重新搜索ECS实例。

## 示例 1：使用属性值搜索，系统自动匹配属性

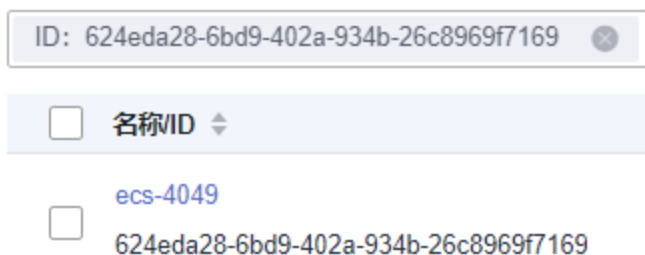
输入完整的属性值后，系统自动识别属性并搜索。多个取值使用“,”分隔，否则后输入的取值会替换之前输入的取值。多个属性值之间为“或”的关系。

- 单值搜索：  
在云服务器列表页搜索的输入框中输入完整ID，按回车键进行搜索。

图 2-224 输入完整的 ID



图 2-225 系统自动匹配属性



- 多值搜索：  
在云服务器列表页搜索的输入框中输入完整的规格名称，按回车键进行搜索。

图 2-226 输入多个完整的规格名称



图 2-227 系统自动匹配属性并搜索



## 示例 2：单属性搜索

选择属性后，输入/选择对应的属性信息。

以下属性仅支持精确搜索，需输入完整的属性值：ID、弹性公网IP地址、镜像ID、VPC ID。

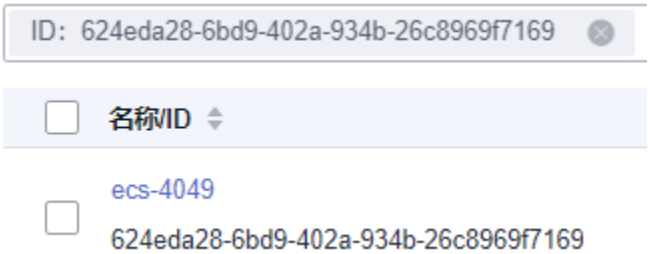
- 模糊搜索：使用私有IP地址搜索
  - 在云服务器列表页搜索的输入框中选择“私有IP地址”。
  - 根据提示，输入私有IP地址，按回车键进行搜索。“私有IP地址”支持模糊搜索，例如输入“192.168.0”，可以搜索到所有使用192.168.0网段的云服务器。

图 2-228 按私有 IP 地址搜索云服务器



- 精确搜索：使用ID搜索
  - 在云服务器列表页搜索的输入框中选择“ID”。
  - 根据提示，输入完整的ID，按回车键进行搜索。

图 2-229 按 ID 搜索云服务器



示例 3：多属性搜索

支持选择多个不同的属性，搜索时多个属性为“与”的关系。

以下属性仅支持精确搜索，需输入完整的属性值：ID、弹性公网IP地址、镜像ID、VPC ID。

本例同时使用“名称”和“私有IP地址”进行搜索。

- 在云服务器列表页搜索的输入框中选择“名称”并输入取值。按回车键进行搜索。本例名称使用模糊搜索。
- 添加筛选属性条件，选择“私有IP地址”，根据提示输入私有IP地址，按回车键进行搜索。本例私有IP地址使用模糊搜索。

图 2-230 按名称和私有 IP 地址搜索云服务器

|                          |                               |                    |      |        |                             |                    |
|--------------------------|-------------------------------|--------------------|------|--------|-----------------------------|--------------------|
| 名称: ecs-f                |                               | 私有IP地址: 192.168.12 |      | 添加筛选条件 |                             |                    |
| <input type="checkbox"/> | 名称/ID                         | 监控                 | 可用区  | 状态     | 规格/镜像                       | IP地址               |
| <input type="checkbox"/> | ecs-f6d8d189a-068b-4f07...    |                    | 可用区2 | 关机     | 1vCPUs   2GiB   s2.medium.2 | 192.168.128.121... |
| <input type="checkbox"/> | ecs-f6b33e20a97a-e108-437c... |                    | 可用区2 | 运行中    | 1vCPUs   2GiB   s2.medium.2 | 192.168.125.168... |

示例 4：单属性、多值搜索

仅以下属性支持单属性、多值搜索：状态、ID、规格名称、私有IP地址、弹性公网IP地址、计费模式、标签。

其中以下属性仅支持精确搜索，需输入完整的属性值：ID、私有IP地址、弹性公网IP地址。

选择一个属性后，输入多个取值，多个取值之间为“或”的关系。

- 模糊搜索
  - 在云服务器列表页搜索的输入框中选择“规格名称”。
  - 根据提示输入多个规格名称，使用“,”分隔，按回车键进行搜索。

图 2-231 按规格名称搜索云服务器



- 精确搜索
  - 在云服务器列表页搜索的输入框中选择“私有IP地址”。
  - 根据提示输入多个完整的私有IP地址，使用“,”分隔，按回车键进行搜索。

图 2-232 按私有 IP 地址搜索云服务器



示例 5：多属性、多值搜索

仅以下属性支持多属性、多值搜索：ID、规格名称、状态、弹性公网IP地址、计费模式。

选择多属性、多值搜索：

- 多个属性之间为“与”的关系。
- 同一属性的多个取值之间为“或”的关系。

以下属性仅支持精确搜索，需输入完整的属性值：ID。

- 模糊搜索
  - 在云服务器列表页搜索的输入框中选择“状态”，并选择“运行中”、“关机”，按回车键进行搜索。
  - 添加筛选属条件，选择“规格名称”，输入多个规格名称，使用“,”分隔，按回车键进行搜索。

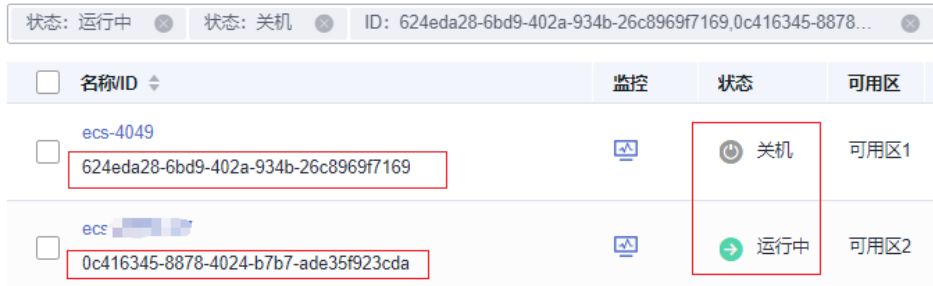
图 2-233 按状态和规格名称搜索云服务器





- 精确搜索
  - a. 在云服务器列表页搜索的输入框中选择“状态”，并选择“运行中”、“关机”，按回车键进行搜索。
  - b. 添加筛选属条件，选择“ID”，根据提示输入多个完整的ID，使用“,”分隔，按回车键进行搜索。

图 2-234 按状态和 ID 搜索云服务器

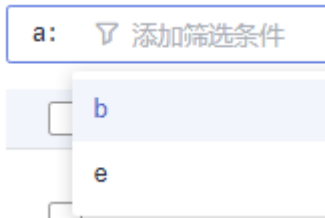


示例 6：按标签搜索

按标签过滤时可选择键或键值对搜索。  
支持设置多个标签，如果键不同，则标签按“与”的关系搜索。  
如果键相同，值不同，则标签按“与”的关系搜索。

- 单个标签搜索  
在云服务器列表页搜索的输入框中选择“标签”，选择标签键值对后自动搜索。

图 2-235 按标签搜索云服务器



- 多个标签搜索  
在云服务器列表页搜索的输入框中选择“标签”，选择多个标签键值对后自动搜索。  
按“与”的关系搜索，搜索同时具备这两个标签的云服务器。

图 2-236 按标签搜索云服务器



示例 7：修改搜索条件

搜索完成后，您可以修改搜索条件，按照其他的属性类型或值重新搜索。本示例将其  
中一个搜索条件由“名称: ecs-test1”变更为“可用区: 可用区1”。

1. 单击搜索栏中需要修改的搜索条件“名称：ecs-test1”。

图 2-237 选择搜索条件



2. 在“属性类型”下拉框中选择“可用区”，在“值”下拉框中选择“可用区1”。

图 2-238 修改搜索属性



3. 单击“确定”，系统将搜索“可用区1”中状态为“运行中”的ECS实例。

图 2-239 搜索 ECS 实例



# 3 回收站管理（公测）

## 3.1 回收站概述

### 什么是回收站

回收站是一种弹性云服务器（Elastic Cloud Server，ECS）回收机制。当您主动删除按需计费的ECS或主动退订未到期的包年/包月ECS时，如果希望ECS可以保留一段时间，您可以使用回收站功能，防止因误删除/退订ECS造成的业务损失。

#### 说明

回收站目前在公测阶段，如需使用，请[提交工单](#)申请公测。

### 约束与限制

- 对于IAM用户，如要使用回收站功能，需要具有如下IAM权限：
  - 查询回收站：ecs:recycleBin:get
  - 更新回收站（开启或关闭操作）：ecs:recycleBin:update
  - 更新回收站策略：ecs:recycleBin:updatePolicy

您可以通过IAM用户对应的账号为IAM用户授予上述权限，详细操作，请参见[ECS自定义策略](#)。

- 在以下场景中，删除或退订的ECS不支持放入回收站。
  - 账号处于欠费、受限或冻结的异常状态。
  - ECS处于“故障”状态。
  - ECS距离创建时间的天数小于配置的创建时长。
  - ECS处于保留期。
  - ECS保留期到期后被系统释放。
  - 已设置“定时删除时间”的ECS不支持放入回收站。
  - 竞价计费型ECS，释放时不放入回收站。
- 回收站对ECS的资源配额约束：
  - ECS进入回收站后，会占用ECS的资源配额。
  - 专属主机上的ECS进入回收站后，会占用专属主机上的资源配额。

说明

当ECS配额不足时，请及时对回收站中的ECS进行清理。

- 当ECS作为高阶服务的计算资源使用时，如果满足回收站条件，ECS会进入回收站。这可能会导致高阶服务清理资源失败，请清理回收站中的ECS后，再进行重试。

计费说明

- 按需计费或包年/包月ECS进入回收站后，均转为按需计费。ECS进入回收站后关机，其计费原则如表3-1所示。（详细计费标准，请参见[计费模式概述](#)）：

表 3-1 关机计费策略

| 实例类型 | 实例说明                                                                                               | 资源计费项                | 关机是否计费 | 关机后资源处理                                                                                                                                                                     |
|------|----------------------------------------------------------------------------------------------------|----------------------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 普通实例 | 普通实例包括： <ul style="list-style-type: none"><li>非裸金属实例</li><li>不含本地盘的实例</li><li>不含FPGA卡的实例</li></ul> | 云服务器（计算资源，包括vCPU和内存） | 不计费    | <ul style="list-style-type: none"><li>公共资源池创建的实例，基础资源（vCPU、内存）不再保留。当再次启动云服务器时，可能由于资源不足无法正常开机，请耐心等待，稍后再试。</li><li>基于专属资源或边缘可用区创建的实例，基础资源（vCPU、内存）仍会保留。</li></ul>             |
|      |                                                                                                    | 镜像                   | 不计费    | 资源保留，不计费，不进行处理。                                                                                                                                                             |
|      |                                                                                                    | GPU                  | 不计费    | 不含本地盘的“GPU加速型”实例，关机后GPU资源不再保留。                                                                                                                                              |
|      |                                                                                                    | 云硬盘（系统盘和数据盘）         | 计费     | 不受关机影响，仍然按资源计费原则正常计费。                                                                                                                                                       |
|      |                                                                                                    | 带宽                   | 计费     | 不受关机影响，固定带宽仍然按资源计费原则正常计费。 <ul style="list-style-type: none"><li>弹性公网IP的带宽费用：按需计费(按带宽计费)弹性公网IP的带宽费用。</li><li>共享带宽的费用。</li></ul> 以上计费项目的详细说明，请参见 <a href="#">弹性公网IP计费说明</a> 。 |

| 实例类型 | 实例说明                                                                                                                                   | 资源计费项                | 关机是否计费 | 关机后资源处理                                      |
|------|----------------------------------------------------------------------------------------------------------------------------------------|----------------------|--------|----------------------------------------------|
| 特殊实例 | 特殊实例包括： <ul style="list-style-type: none"><li>裸金属实例</li><li>含本地盘的实例如磁盘增强型、超高I/O型、H2型、P1型、P2型等。</li><li>含FPGA卡的实例如Fp1型、Fp1c型。</li></ul> | 云服务器（计算资源，包括vCPU和内容） | 计费     | 不受关机影响，仍然按资源计费原则正常计费。<br>如需停止计费，需删除实例及其绑定资源。 |
|      |                                                                                                                                        | 镜像                   | 计费     |                                              |
|      |                                                                                                                                        | GPU                  | 计费     |                                              |
|      |                                                                                                                                        | 云硬盘（系统盘和数据盘）         | 计费     |                                              |
|      |                                                                                                                                        | 带宽                   | 计费     |                                              |

- 已在回收站中的ECS，当账户欠费时会进入宽限期、保留期，受宽限期和保留期的影响，在未达到自定义保存时长时，ECS也可能会被系统提前删除。了解宽限期保留期的具体时长请参见[宽限期保留期](#)。
- 回收站中的ECS恢复后均遵循按需计费模式。若要使用包年/包月，您可以将ECS按需计费变更为包年/包月，具体方法请参见[按需转包年/包月](#)。

操作流程

ECS回收站的操作流程如[图3-1](#)所示。

图 3-1 云服务器回收站操作流程



回收站策略配置建议

在使用ECS的回收站功能时，需要配置回收站策略，详细操作，请参见[配置回收站策略](#)。

回收站策略包括：

- 创建时长：用于决定您的ECS创建多少天后，删除或退订时会放入回收站。
- 停留时长：控制ECS进入回收站后的保留时长。

 说明

停留时长仅对设置后放入回收站中的云服务器生效。

ECS与EVS均支持回收站功能，且均支持独立配置回收站策略。在配置ECS的“创建时长”时，建议与EVS保持一致，避免二者出现因生命周期不同导致的问题。

在部分特殊场景，可能需要将ECS和EVS的回收站策略配置为不同值，此时，具体的回收站策略如表3-2所示。

以一个创建了8天的ECS（含系统盘和数据盘）为例，删除或退订资源时，处理结果如下：

表 3-2 回收站创建时长配置场景及处理原则

| 回收站创建时长的关系                                 | 删除或退订资源的原则                     | ECS处理结果 | EVS处理结果 |
|--------------------------------------------|--------------------------------|---------|---------|
| ECS < EVS<br>• ECS创建时长：7天<br>• EVS创建时长：15天 | 遵循ECS回收站策略                     | 进入回收站   | 进入回收站   |
| ECS > EVS<br>• ECS创建时长：15天<br>• EVS创建时长：7天 | ECS遵循ECS回收站策略<br>EVS遵循EVS回收站策略 | 直接删除或退订 | 进入回收站   |

绑定资源处理策略

删除或退订ECS时，如果满足回收站策略，ECS会进入回收站，其绑定资源的处理策略如下所示：

- 绑定的弹性公网IP的处理策略如表3-3所示。

表 3-3 绑定的弹性公网 IP 的处理策略

| 实例计费模式 | 操作                               | 是否进入回收站 | 恢复云服务器时处理结果 | 销毁云服务器时处理结果 |
|--------|----------------------------------|---------|-------------|-------------|
| 按需计费   | 删除云服务器时，勾选“释放弹性云服务器绑定的弹性公网IP地址”。 | 否       | 已删除，不可恢复    | 已删除         |

| 实例计费模式 | 操作                                | 是否进入回收站 | 恢复云服务器时处理结果 | 销毁云服务器时处理结果 |
|--------|-----------------------------------|---------|-------------|-------------|
|        | 删除云服务器时，不勾选“释放弹性云服务器绑定的弹性公网IP地址”。 | 否       | 已解绑，不可恢复    | 已解绑，不会删除    |
| 包年/包月  | 退订云服务器时，退订弹性公网IP。                 | 否       | 已删除，不可恢复    | 已删除         |
|        | 退订云服务器时，不退订弹性公网IP。                | 否       | 已解绑，不可恢复    | 已解绑，不会删除    |

- 绑定的云硬盘的处理策略如表3-4所示。

表 3-4 绑定的云硬盘的处理策略

| 实例计费模式 | 绑定资源的类型 | 操作                           | 是否进入回收站        | 恢复云服务器时处理结果         | 销毁云服务器时处理结果 |
|--------|---------|------------------------------|----------------|---------------------|-------------|
| 按需计费   | 系统盘     | 删除云服务器时，勾选“删除弹性云服务器挂载的数据盘”。  | 是              | 同步恢复                | 同步删除        |
|        |         | 删除云服务器时，不勾选“删除弹性云服务器挂载的数据盘”。 | 是              | 同步恢复                | 同步删除        |
|        | 数据盘（独享） | 删除云服务器时，勾选“删除弹性云服务器挂载的数据盘”。  | 是              | 同步恢复                | 同步删除        |
|        |         | 删除云服务器时，不勾选“删除弹性云服务器挂载的数据盘”。 | 否              | 未手动卸载，则保持与云服务器的挂载关系 | 已卸载，不会删除    |
|        | 数据盘（共享） | 删除云服务器时，勾选“删除弹性云服务器挂载的数据盘”。  | 否（共享盘挂载多个云服务器） | 未手动卸载，则保持与云服务器的挂载关系 | 已卸载，不会删除    |

| 实例计费模式 | 绑定资源的类型 | 操作                           | 是否进入回收站         | 恢复云服务器时处理结果         | 销毁云服务器时处理结果 |
|--------|---------|------------------------------|-----------------|---------------------|-------------|
|        |         |                              | 是（共享盘仅挂载一个云服务器） | 同步恢复                | 同步删除        |
|        |         | 删除云服务器时，不勾选“删除弹性云服务器挂载的数据盘”。 | 否               | 未手动卸载，则保持与云服务器的挂载关系 | 已卸载，不会删除    |
| 包年/包月  | 系统盘     | 退订云服务器。                      | 是               | 同步恢复                | 同步删除        |
|        | 数据盘（独享） | 退订云服务器，该云服务器挂载了同一订单的独享数据盘。   | 是               | 同步恢复                | 同步删除        |
|        |         | 退订云服务器，该云服务器挂载了不同订单的独享数据盘。   | 否               | 未手动卸载，则保持与云服务器的挂载关系 | 已卸载，不会删除    |
|        | 数据盘（共享） | 退订云服务器，该云服务器挂载了共享数据盘。        | 否               | 未手动卸载，则保持与云服务器的挂载关系 | 已卸载，不会删除    |

- 绑定的弹性网卡的处理策略如表3-5所示。

表 3-5 绑定的弹性网卡的处理策略

| 绑定资源的类型 | 操作         | 是否进入回收站 | 恢复云服务器时处理结果  | 销毁云服务器时处理结果 |
|---------|------------|---------|--------------|-------------|
| 主网卡     | 删除或退订云服务器。 | 否       | 保持与云服务器的绑定关系 | 同步删除        |



| 绑定资源的类型 | 操作         | 是否进入回收站 | 恢复云服务器时处理结果         | 销毁云服务器时处理结果                                                                           |
|---------|------------|---------|---------------------|---------------------------------------------------------------------------------------|
| 扩展网卡    | 删除或退订云服务器。 | 否       | 未手动解绑，则保持与云服务器的绑定关系 | <div><div></div><div>若手动解绑，删除云服务器时不会删除</div><div></div><div>若没有手动解绑，则同步删除</div></div> |

## 3.2 开启回收站

### 操作场景

当您主动删除按需计费的ECS或主动退订未到期的包年/包月ECS后，如果希望ECS保留一段时间，可以使用回收站功能，防止因误删除/退订ECS造成的业务损失。

ECS回收站功能默认关闭，如需要使用该功能，请参考本章节开启ECS回收站。

#### 说明

回收站目前在公测阶段，如需使用，请[提交工单](#)申请公测。

ECS的回收站功能按照IAM项目维度进行开启。如果使用多项目管理，需要对每个项目进行开启回收站操作。

### 前提条件

开启ECS回收站时，需优先开启云硬盘回收站。详细操作请参见[开启云硬盘回收站](#)。

### 操作步骤

1. 登录管理控制台。
2. 单击管理控制台左上角的，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”。
4. 选择ECS列表上方的“回收站”页签。

图 3-2 “回收站”页签



5. 在“回收站”页签下，单击“开启回收站”按钮。  
开启后“回收站”页签下会出现待销毁/恢复的ECS列表，此时可使用回收站功能。

## 3.3 关闭回收站

### 操作场景

如果您不想使用ECS回收站功能，可以随时关闭回收站功能。关闭回收站后，您的ECS在删除或退订后，不再进入回收站，会被立即删除且不可恢复。

#### 说明

关闭ECS回收站不会影响云硬盘回收站的使用。

### 前提条件

在关闭ECS回收站之前，您需要恢复或销毁回收站中的ECS，方法如下：

- [恢复回收站中的云服务器](#)
- [销毁回收站中的云服务器](#)

### 操作步骤

1. 登录管理控制台。
2. 单击管理控制台左上角的，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”。
4. 选择ECS列表上方的“回收站”页签。
5. 在“回收站”列表右上方单击“关闭回收站”。  
弹出“关闭须知”对话框。
6. 单击“确定”。  
完成关闭回收站功能。

## 3.4 配置回收站策略

### 操作场景

回收站功能开启后，您可以自定义回收站策略，需要配置：

- 创建时长：用于决定您的ECS创建多少天后，删除或退订时会放入回收站。
- 停留时长：控制ECS进入回收站后的保留时长。

#### 说明

停留时长仅对设置后放入回收站中的云服务器生效。

## 约束与限制

- ECS回收策略的创建时长默认为7天，最小可以配置1天，最大可配置1000天。
- 回收站中ECS的停留时长最小可以配置1小时，最大可以配置720小时。

## 操作步骤

1. 登录管理控制台。
  2. 单击管理控制台左上角的 ，选择区域和项目。
  3. 单击“”，选择“计算 > 弹性云服务器”。
  4. 选择ECS列表上方的“回收站”页签。
  5. 在“回收站”列表右上方单击“策略配置”。  
弹出“配置回收站策略”窗口。
  6. 配置回收站策略。
    - 创建时长：表示云服务器创建大于多少天时退订/删除后放入回收站。默认为7天。  
例如，创建时长设置为7天，表示7天前创建的ECS删除时放入回收站，按需收取费用；7天内创建的ECS删除时不放入回收站，彻底删除。
-  **说明**
- 建议将ECS和EVS的“创建时长”设置一致，避免因策略不同导致删除或退订资源时处理结果不同，详细内容，请参见[回收站策略配置建议](#)。
- 停留时长：表示放入回收站中的云服务器保留时长。默认为168小时。  
例如，停留时长设置为168小时，表示ECS在回收站内最多保存168小时，到期后自动销毁，销毁后ECS将不可恢复。
7. 单击“确定”，完成策略配置。

## 3.5 恢复回收站中的云服务器

### 操作场景

在未达到回收站的自定义停留时长时，您可以参考本章节恢复回收站中的ECS。

### 约束与限制

当账号冻结或受限时，回收站功能失效，回收站的ECS无法恢复。

### 操作步骤

1. 登录管理控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”。
4. 选择ECS列表上方的“回收站”页签。
5. 在“回收站”页签下，单击待恢复ECS所在行的操作列下的“恢复”。

进入“恢复云服务器”页面。

6. 单击“提交”，恢复回收站内的ECS。
  - 若恢复成功，您可以在ECS列表中查看ECS，状态为“运行中”。  
ECS恢复的绑定资源可参考[查看ECS详细信息（列表视图）](#)进行查看。
  - 若恢复失败，您可以在回收站中查看ECS，状态为“关机”。

#### 说明

恢复ECS后，绑定资源的恢复规则请参见[绑定资源处理策略](#)。

回收站中的ECS恢复后遵循按需计费模式。若要使用包年/包月，您可以将ECS按需计费变更为包年/包月，具体方法请参见[按需转包年/包月](#)。

## 3.6 销毁回收站中的云服务器

### 操作场景

在未达到回收站的自定义停留时长时，您可以参考本章节销毁回收站中的ECS。

#### 说明

销毁ECS后，ECS将不可恢复，请谨慎操作。

销毁ECS后，绑定资源的处理策略请参见[绑定资源处理策略](#)。

### 约束与限制

当账号欠费时，回收站中的ECS会进入宽限期、保留期。在未达到自定义停留时长时，根据宽限期和保留期策略，回收站中的ECS也可能被系统提前删除。

### 操作步骤

1. 登录管理控制台。
2. 单击管理控制台左上角的，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”。
4. 选择ECS列表上方的“回收站”页签。
5. 在“回收站”页签下，单击待恢复ECS所在行的操作列下的“销毁”。  
进入“您确定要销毁该云服务器吗？”页面。
6. 单击“确定”，彻底销毁回收站内的ECS。  
当ECS从“回收站”页签下的待销毁ECS列表中消失时，表示销毁成功。

## 3.7 导出回收站列表信息

### 操作场景

您可以将当前账号回收站列表中的所有弹性云服务器信息，以.xlsx文件的形式导出至本地。

该文件包含云服务器的名称、ID、状态、可用区、规格、镜像、IP地址、销毁倒计时、专属主机名称等信息。

## 操作步骤

1. 登录管理控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”。
4. 选择ECS列表上方的“回收站”页签。
5. 在回收站列表左上角，单击“导出”，导出列表。
  - 导出全部数据到XLSX：系统会将您账号下，当前区域回收站列表中的所有弹性云服务器信息自动导出，并下载至本地。
  - 导出已选中数据到XLSX：系统会将回收站列表中已勾选的弹性云服务器信息自动导出，并下载至本地。
6. 在本地计算机桌面的默认下载地址文件夹，可以获取到导出的回收站列表信息。

# 4 镜像管理

## 4.1 镜像概述

### 什么是镜像

镜像是一个包含了软件及必要配置的云服务器或裸金属服务器模板，包含操作系统或业务数据，还可以包含应用软件（例如，数据库软件）和私有软件。镜像分为公共镜像、私有镜像、共享镜像、市场镜像。

**镜像服务**（Image Management Service）提供简单方便的镜像自助管理功能。用户可以灵活便捷地使用公共镜像、私有镜像或共享镜像申请云服务器。同时，用户还能通过已有的云服务器或使用外部镜像文件创建私有镜像。

### 公共镜像

公共镜像是包含常见的标准操作系统的镜像，所有用户可见，包括操作系统以及预装的公共应用，支持Ubuntu，CentOS，Debian等主流操作系统。用户可以从丰富的公共镜像库中选择或创建私有镜像，从而快速创建或批量复制弹性云服务器。请根据您的实际情况自助配置应用环境或相关软件。

更多关于公共镜像的介绍，请参见“[公共镜像概述](#)”。

### 私有镜像

私有镜像包含操作系统或业务数据、预装的公共应用以及用户的私有应用的镜像，仅用户个人可见。

表 4-1 私有镜像类型

| 镜像类型  | 说明                                                |
|-------|---------------------------------------------------|
| 系统盘镜像 | 包含用户运行业务所需的操作系统、应用软件的镜像。系统盘镜像可以用于创建云服务器，迁移用户业务到云。 |
| 数据盘镜像 | 只包含用户业务数据的镜像。数据镜像可以用于创建云硬盘，将用户的业务数据迁移到云上。         |

| 镜像类型  | 说明                                                  |
|-------|-----------------------------------------------------|
| 整机镜像  | 包含用户运行业务所需的操作系统、应用软件和业务数据的镜像。整机镜像包含系统盘和其所挂载的所有数据盘。  |
| ISO镜像 | 将外部镜像的ISO文件注册到云平台的私有镜像。ISO镜像是特殊的镜像，只能发放用作临时过渡的云服务器。 |

如果您使用私有镜像切换操作系统请参考《[镜像服务用户指南](#)》提前完成私有镜像的制作。

- 如果需要指定弹性云服务器的镜像，请提前使用指定弹性云服务器创建私有镜像。
- 如果需要使用本地的镜像文件，请提前将镜像文件导入并注册为云平台的私有镜像。
- 如果需要使用其他区域的私有镜像，请提前复制镜像。
- 如果需要使用其他账号的私有镜像，请提前完成镜像共享。
- 带GPU、NPU以及编码卡的异构弹性云服务器暂不支持UEFI启动模式的私有镜像

共享镜像

用户将接受云平台其他用户共享的私有镜像，作为自己的镜像进行使用。更多关于共享镜像的使用，请参见[共享镜像](#)。

- 用户只能共享自己没有发布为市场镜像的私有镜像，已经发布为市场镜像的不能共享。
- 镜像共享的范围只能在区域内。如果您需要跨区域共享镜像，请先复制镜像到目标区域后再共享。
- 每个镜像最多可以共享给128个租户。
- 用户可以随时取消自己共享的镜像，无需通知镜像的接受方。
- 用户可以随时删除自己共享的镜像，无需通知镜像的接受方。
- 加密镜像不能共享。
- 只有通过云备份或云服务器（未通过旧版CSBS服务生成备份）创建的整机镜像，才支持共享。通过其他方式创建的整机镜像，暂不支持共享。

市场镜像

市场镜像提供预装操作系统、应用环境和各类软件的优质第三方镜像。无需配置，可一键部署，满足建站、应用开发、可视化管理等个性化需求。

市场镜像由镜像服务商定价，有免费镜像，也有付费镜像。使用付费镜像创建云服务器时，需要支付市场镜像的费用和云服务器费用。

相关链接

- [了解私有镜像的创建方式](#)
- [镜像源管理类常见问题](#)

## 4.2 创建镜像

### 操作场景

您可以使用已有的弹性云服务器创建系统盘镜像、数据盘镜像、整机镜像。

- 系统盘镜像：系统盘镜像包含用户运行业务所需的操作系统、应用软件，可以用于云服务器业务的迁移。
- 数据盘镜像：数据盘镜像只包含用户业务数据的镜像。用户可以通过创建数据盘镜像对云服务器的数据盘进行导出。数据盘镜像可以用于创建云硬盘，将用户的业务数据迁移到云上。
- 整机镜像：使用弹性云服务器携带其挂载的数据盘一起创建整机镜像，创建的整机镜像包含用户的业务数据，可用于快速发放包含用户业务数据的弹性云服务器。
- ISO 镜像：将外部镜像的ISO文件注册到云平台的私有镜像。ISO镜像是特殊的镜像，只能发放用作临时过渡的云服务器。

如果您使用私有镜像切换操作系统请参考《[镜像服务用户指南](#)》提前完成私有镜像的制作。

### 约束与限制

- “运行中”或“关机”状态的弹性云服务器才可以用来创建私有镜像。
- 请勿在创建镜像过程中对所选择的弹性云服务器及其相关联资源进行其他操作。
- 创建镜像操作免费，但是私有镜像会收取一定的存储费用。详细计费标准，可参考[镜像服务计费标准](#)。

更多关于创建私有镜像的信息，请参见[创建私有镜像](#)。

### 前提条件

创建镜像前，请确保弹性云服务器已完成相关初始化配置。

详细内容，请参考[创建私有镜像前云服务器或镜像文件需要完成哪些初始化配置？](#)

### 操作步骤

1. 登录管理控制台。
2. 单击管理控制台左上角的，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”。
4. 在弹性云服务器的“操作”列下，单击“更多 > 镜像 > 创建镜像”。
5. 根据界面要求填写如下信息：  
包含“镜像类型和来源”和“配置信息”两个信息块，各参数说明参见[表4-2](#)和[表4-3](#)。



表 4-2 镜像类型和来源

| 参数    | 说明                                                                            |
|-------|-------------------------------------------------------------------------------|
| 创建方式  | 选择“创建私有镜像”。                                                                   |
| 区域    | 请选择靠近您业务的区域。<br>如果区域选择错误，可以在私有镜像创建成功后通过“ <a href="#">跨区域复制镜像</a> ”将镜像复制到其他区域。 |
| 镜像类型  | 选择“系统盘镜像”。                                                                    |
| 选择镜像源 | 选择“云服务器”，然后从列表中选择已完成相关配置的云服务器。                                                |

表 4-3 配置信息

| 参数   | 说明                                                                                                                                            |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| 加密   | 镜像的加密属性，不可更改。 <ul style="list-style-type: none"><li>使用未加密的云服务器创建的私有镜像为未加密的私有镜像。</li><li>使用加密的云服务器创建的私有镜像为加密的私有镜像。</li></ul>                   |
| 名称   | 设置一个便于您识别的镜像名称。                                                                                                                               |
| 企业项目 | 从下拉列表中选择所在的企业项目。该参数针对企业用户使用，只有开通了企业项目的客户，或者权限为企业主账号的客户才可见。如需使用该功能，请联系您的客户经理申请开通。<br><br>企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。 |
| 标签   | 可选参数，为镜像设置标签键和标签值，便于识别和管理。                                                                                                                    |
| 描述   | 可选参数，对镜像进行描述。                                                                                                                                 |

6. 单击“立即创建”。

# 5 磁盘管理

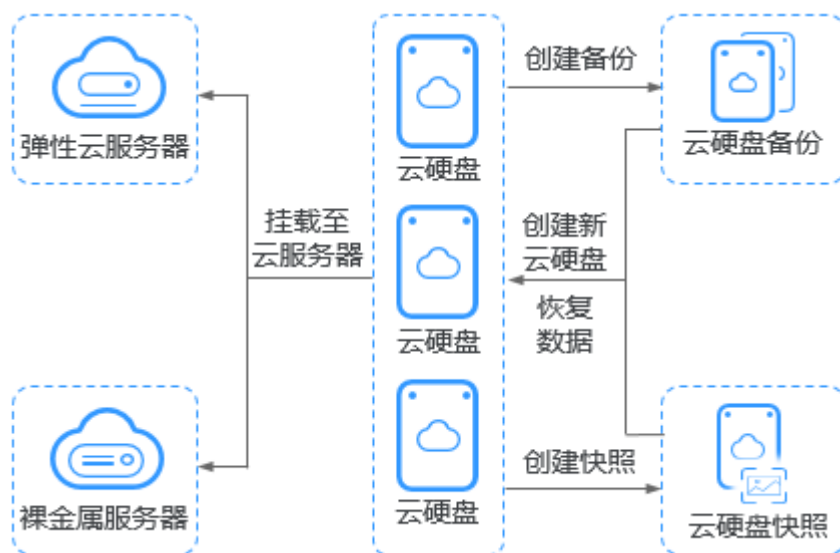
## 5.1 ECS 磁盘概述

### 什么是云硬盘

云硬盘（Elastic Volume Service，EVS）可以为弹性云服务器提供高可靠、高性能、规格丰富并且可弹性扩展的块存储服务，满足不同场景的业务需求，适用于分布式文件系统、开发测试、数据仓库以及高性能计算等场景。

云硬盘类似PC中的硬盘，需要挂载至云服务器使用，无法单独使用。您可以对已挂载的云硬盘执行初始化、创建文件系统等操作，并且把数据持久化地存储在云硬盘上。

图 5-1 云硬盘架构



- 系统盘：云服务器中安装操作系统的云硬盘，类似于电脑中的C盘。系统盘在购买云服务器时自动购买并挂载，无法单独新购买。系统盘的最大容量为1024 GiB。
- 数据盘：云服务器中用来存储数据的云硬盘，用来存放除操作系统之外的其他数据，类似于电脑中的D盘、E盘、F盘等。

数据盘可以在购买云服务器的时候购买，由系统自动挂载给云服务器。也可以在购买了云服务器之后，单独新购买云硬盘并挂载给云服务器。数据盘的最大容量为32768 GiB。

云硬盘的类型

根据性能，磁盘可分为极速型SSD V2、极速型SSD、通用型SSD V2、超高IO、通用型SSD、高IO、普通IO。不同类型云硬盘的性能各不相同，您可根据应用程序要求选择您所需的云硬盘。

更多关于云硬盘规格、性能等信息，请参见《[云硬盘类型及性能介绍](#)》。

云硬盘的磁盘模式

根据是否支持高级的SCSI命令来划分磁盘模式，分为VBD(虚拟块存储设备，Virtual Block Device)类型和SCSI (小型计算机系统接口, Small Computer System Interface) 类型。磁盘模式在购买磁盘时配置，购买完成后无法修改。

- VBD类型：  
当您通过管理控制台创建云硬盘时，云硬盘的磁盘模式默认为VBD类型。VBD类型的云硬盘只支持简单的SCSI读写命令。
- SCSI类型：  
您可以通过管理控制台创建SCSI类型的云硬盘，该类型的云硬盘支持SCSI指令透传，允许弹性云服务器操作系统直接访问底层存储介质。除了简单的SCSI读写命令，SCSI类型的云硬盘还可以支持更高级的SCSI命令。

 **说明**

更多关于SCSI类型云硬盘的使用（如驱动安装），请参见“[使用SCSI类型云硬盘需要安装驱动吗](#)”。

ECS 支持的磁盘模式

ECS支持的磁盘模式由规格类型决定，同时，还与ECS所属的操作场景相关。

表 5-1 ECS 支持的磁盘模式

| 操作场景   | 磁盘模式（系统盘）                                                                                                                                             | 磁盘模式（数据盘）                                                                                                                                                  |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 购买ECS时 | <ul style="list-style-type: none"><li>● 通用计算增强型C7：SCSI。</li><li>● 内存优化型M7：SCSI。</li><li>● 含“physical”附加标识的裸金属类型：SCSI。</li><li>● 其余规格类型：VBD。</li></ul> | <ul style="list-style-type: none"><li>● 通用计算增强型C7：SCSI。</li><li>● 内存优化型M7：SCSI。</li><li>● 含“physical”附加标识的裸金属类型：SCSI。</li><li>● 其余规格类型：VBD或SCSI。</li></ul> |

| 操作场景         | 磁盘模式（系统盘） | 磁盘模式（数据盘）                                                                                                                                                  |
|--------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 为已购买ECS挂载磁盘时 | 不涉及       | <ul style="list-style-type: none"><li>通用计算增强型C7：VBD或SCSI。</li><li>内存优化型M7：VBD或SCSI。</li><li>含“physical”附加标识的裸金属类型：SCSI。</li><li>其余规格类型：VBD或SCSI。</li></ul> |

## 相关链接

- [挂载磁盘](#)
- [初始化数据盘](#)
- [登录Windows弹性云服务器，找不到新购买的数据盘？](#)
- [怎样调整系统盘分区？](#)
- [一台弹性云服务器可以挂载多块磁盘吗？](#)
- [弹性云服务器挂载磁盘时有什么限制？](#)

## 5.2 为 ECS 新增磁盘

### 操作场景

当弹性云服务器的存储容量不够时，您可以选择购买云硬盘来扩充存储容量。

云服务器的磁盘包括系统盘和数据盘。系统盘在创建云服务器时自动创建并挂载，不支持单独购买。数据盘包括如下两种创建方式：

- 在创建购买云服务器的时候一同创建购买：该场景下，数据盘由系统自动挂载给云服务器。
- 在创建购买了云服务器之后，单独创建购买云硬盘：
  - 通过云硬盘控制台购买的数据盘，需要手动挂载到云服务器上。详细操作请参考[为ECS新增磁盘](#)。
  - 通过弹性云服务器控制台购买的数据盘，系统会自动将其挂载给云服务器。

本节操作介绍创建购买了云服务器之后，通过弹性云服务器控制台新增磁盘的操作步骤。

### 约束与限制

- 弹性云服务器创建成功后，最多支持挂载60块磁盘。  
不同规格类型和磁盘类型支持挂载的数量不同，详细信息，请参见[一台弹性云服务器可以挂载多块磁盘吗？](#)
- 新增磁盘仅适用于为弹性云服务器增加数据盘。

- 新增磁盘的区域和可用区与弹性云服务器一致。
- 新增磁盘的计费模式与弹性云服务器一致。
- 支持新增的磁盘类型及性能介绍，请参见[云硬盘](#)。

## 计费说明

云硬盘购买成功后开始计费。云硬盘收费跟类型、容量和时长有关，详情请参见[云硬盘计费说明](#)。

## 操作步骤

1. 登录管理控制台。
2. 单击管理控制台左上角的，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”。
4. 在弹性云服务器的“操作”列下，按计费模式进行操作。
  - 按需计费弹性云服务器：  
单击“更多 > 磁盘/备份 > 新增磁盘”。
  - 包年/包月弹性云服务器：
    - i. 单击“更多 > 变更”。
    - ii. 在“请选择变更类型”中，勾选“新增磁盘”并单击“下一步”。

图 5-2 新增磁盘

### 请选择变更类型

#### ☐ 变更规格

对弹性云服务器的规格（CPU、内存等）进行变更，资源的到期时间不会发生变化。您需要支付因规格变更产生的费用。

#### ☐ 变更产品(FlexusX)

将弹性云服务器变更为X实例，资源的到期时间不会发生变化，您可能需要支付因产品变更产生的费用。

#### ☒ 新增磁盘

为弹性云服务器增加包年/包月的云硬盘，新增的云硬盘仅支持绑定当前云服务器，并与当前云服务器的到期时间保持一致。

#### ☐ 删除云硬盘

删除与弹性云服务器捆绑购买的包年/包月云硬盘，并根据剩余时长进行退费。通过该云硬盘创建的快照也会被删除，请谨慎操作。

取消

下一步

系统跳转至购买磁盘页面。

5. 根据界面提示，设置新添加云硬盘的参数信息。  
云硬盘的参数信息配置请参考[购买云硬盘](#)。

#### 说明

- 新增磁盘默认与弹性云服务器计费模式保持一致。
  - 新增磁盘默认与弹性云服务器位于同一区域。
  - 新增磁盘默认与弹性云服务器位于同一可用区，不支持修改磁盘可用区。
  - 购买完成后新增磁盘默认已挂载至选择的弹性云服务器。
  - 新增包年/包月云硬盘与弹性云服务器的到期时间相同。
6. 单击“立即购买”，确认订单详情并完成支付。  
返回弹性云服务器控制台在“云硬盘”页签下，查看新增磁盘信息。

## 后续处理

在弹性云服务器控制台购买云硬盘后，会自动挂载至弹性云服务器，需要登录弹性云服务器初始化云硬盘，即格式化云硬盘，之后云硬盘才可以正常使用。

初始化数据盘的具体操作，请参见[初始化数据盘](#)。

## 相关链接

- [查看云硬盘详细信息](#)
- [如何查看云硬盘的可用容量](#)

## 5.3 为 ECS 挂载磁盘

### 操作场景

弹性云服务器创建成功后，如果发现磁盘不够用或当前磁盘不满足要求，可以将已有云硬盘挂载给弹性云服务器，或在“存储 > 云硬盘”页面购买新的磁盘，然后再挂载至弹性云服务器。

### 约束与限制

- 仅支持为“运行中”或“关机”状态的弹性云服务器挂载磁盘。
- ISO镜像创建的弹性云服务器只建议用来装机，部分功能受限，不支持挂载磁盘操作。
- 弹性云服务器创建成功后，最多支持挂载60块磁盘。  
不同规格类型和磁盘类型支持挂载的数量不同，详细信息，请参见[一台弹性云服务器可以挂载多块磁盘吗？](#)
- 磁盘仅支持挂载至同一区域、同一可用区的弹性云服务器上。
- 随包年/包月云服务器购买的系统盘，卸载后，如果继续作为系统盘使用，则只能挂载给原云服务器。
- 随按需计费云服务器购买的系统盘，卸载后，如果继续作为系统盘使用，则只能挂载给该系统盘镜像相同的云服务器；如果作为数据盘使用，则可以挂载给任意云服务器。
- 处于冻结状态的云硬盘，不支持挂载给弹性云服务器。

- 共享云硬盘只能用作数据盘，不能用作系统盘。
- 共享云硬盘挂载的多台弹性云服务器只能为Windows或Linux操作系统中的一种。  
比如：  
共享云硬盘首次挂载至多台Windows弹性云服务器，则卸载后，也不能挂载至Linux弹性云服务器。因为Windows和Linux支持的文件系统不同，无法识别云硬盘原有文件系统，如果操作不当会导致原有文件系统被破坏。

更多关于挂载磁盘的信息，请参见[挂载非共享云硬盘](#)和[挂载共享云硬盘](#)。

前提条件

- 已创建可用的云硬盘。  
创建云硬盘的操作请参考“[购买云硬盘](#)”。
- 磁盘未被锁定。  
磁盘加锁时，表示被锁定，此时不能执行磁盘的挂载操作。

操作步骤

- 登录管理控制台。
- 单击管理控制台左上角的，选择区域和项目。
- 单击“”，选择“计算 > 弹性云服务器”。
- 在弹性云服务器列表中的右上角，输入弹性云服务器名、IP地址或ID，并进行搜索。
- 单击待挂载云硬盘的弹性云服务器的名称。  
系统跳转至该弹性云服务器详情页面。
- 选择“云硬盘”页签，并单击“挂载磁盘”。  
系统跳转至“挂载磁盘”页面。

图 5-3 挂载磁盘（KVM）



- 根据界面提示，勾选目标磁盘，并指定该磁盘作为系统盘或数据盘。
  - 对于采用KVM虚拟化类型的弹性云服务器，您可以指定该磁盘作为系统盘或数据盘，但不能指定具体的磁盘挂载点。
  - 对于采用XEN虚拟化类型的弹性云服务器，系统支持指定具体的磁盘挂载点，如/dev/vdb。



### 📖 说明

- 如果无可用的云硬盘，请单击列表下方的“购买云硬盘”进行购买。
- 挂载磁盘时的约束限制，请参见[弹性云服务器挂载磁盘时有什么限制](#)。
- 对于磁盘增强型、超高I/O型中的I3型弹性云服务器，本地盘与云硬盘的磁盘挂载点占用规则如下：
  - 系统盘：占用sda（或vda）。
  - 本地盘：顺序占用sda（或vda）之后的磁盘挂载点。
  - 云硬盘：在本地盘之后顺序挂载，挂载点按字母顺序依次增加。

示例：

假设D1型弹性云服务器有2块本地盘，则这2块本地盘的磁盘挂载点分别为sdb、sdc（或vdb、vdc），云硬盘的磁盘挂载点为sdd、sde……（或vdd、vde……）

#### 8. 单击“确定”。

挂载成功后，在弹性云服务器详情页的“云硬盘”页签，即可看到新挂载的磁盘信息。

## 后续处理

如果挂载的磁盘是新创建的，则云硬盘挂载至云服务器后，需要登录云服务器初始化云硬盘，即格式化云硬盘，之后云硬盘才可以正常使用。

初始化数据盘的具体操作，请参见[初始化数据盘](#)。

## 5.4 初始化数据盘

一块全新的数据盘挂载到云服务器后，还不能直接存储数据，您需要对数据盘进行分区创建、文件系统挂载等初始化操作后，才可以正常使用。

本文介绍初始化数据盘的操作场景、操作指导和分区格式。

### 操作场景

#### • 系统盘

创建云服务器时，系统盘会被自动初始化，默认磁盘分区形式为主启动记录分区（MBR, Master boot record）。

#### • 全新数据盘

- 随云服务器创建的数据盘，系统已自动将数据挂载至云服务器，需要您对数据盘进行初始化后才能使用。
- 不随云服务器创建的数据盘，需要先挂载至云服务器后，再进行初始化。

全新数据盘初始化操作指导，请参见[表5-3](#)。

#### • 有数据的数据盘

有数据的数据盘是指从快照/备份/镜像创建的数据盘，或从其他云服务器上卸载后挂载至另一云服务器上的有数据的数据盘。

- 您可以选择不初始化，直接使用数据盘已有分区：
  - Linux：需要将现有分区挂载至系统指定目录，并设置开机自动挂载至系统指定目录。  
挂载操作请参见[初始化Linux数据盘（容量小于等于2TiB）](#)。



- Windows：无需做任何操作，直接可以使用。
  - 也可以选择对数据盘重新初始化：  
重新划分分区，数据盘已有数据将会被全部删除，建议您先使用快照为云硬盘备份数据。
    - Linux：需要先卸载目录，并删除现有分区（运行 **fdisk 数据盘名称** 命令，再输入“d”，输入分区编号，输入“w”保存），再重新初始化即可。
    - Windows：需要先删除现有分区（使用“删除卷”工具），再重新初始化即可。
- 初始化操作请参见[表5-3](#)。

 说明

初始化云硬盘不会删除云硬盘快照，初始化后仍可以使用快照回滚数据至原云硬盘。

磁盘分区格式

常用的磁盘分区格式有主启动记录分区（Master Boot Record，MBR）和全局分区表（Guid Partition Table，GPT）。针对Linux操作系统，不同的分区形式使用的分区工具不同，如[磁盘分区格式](#)所示。

表 5-2 磁盘分区形式

| 磁盘分区形式 | 支持最大云硬盘容量                   | 支持分区数量                                                                                      | 分区说明                                                                                                                                                                                              | Linux初始化工具                                                               |
|--------|-----------------------------|---------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| MBR    | 2 TiB                       | MBR支持如下分区形式： <ul style="list-style-type: none"><li>• 4个主分区</li><li>• 3个主分区和1个扩展分区</li></ul> | MBR分区包含主分区和扩展分区，其中扩展分区不可以直接使用，需要划分成若干个逻辑分区才可使用。<br>以创建6个分区为例，以下两种分区情况供参考： <ul style="list-style-type: none"><li>• 3个主分区，1个扩展分区，其中扩展分区中包含3个逻辑分区。</li><li>• 1个主分区，1个扩展分区，其中扩展分区中包含5个逻辑分区。</li></ul> | <ul style="list-style-type: none"><li>• fdisk</li><li>• parted</li></ul> |
| GPT    | 18 EiB（1 EiB = 1048576 TiB） | 不限制分区数量。                                                                                    | GPT格式下没有主分区、扩展分区以及逻辑分区之分。                                                                                                                                                                         | parted                                                                   |

## 操作指导

表 5-3 云硬盘初始化操作指导

| 云硬盘容量      | 分区格式    | 操作系统    | 参考文档                                    |
|------------|---------|---------|-----------------------------------------|
| 容量 <= 2TiB | GPT/MBR | Linux   | <a href="#">初始化Linux数据盘（容量小于等于2TiB）</a> |
|            |         | Windows | <a href="#">初始化Windows数据盘</a>           |
| 容量 > 2TiB  | GPT     | Linux   | <a href="#">初始化Linux数据盘（容量大于2TiB）</a>   |
|            |         | Windows | <a href="#">初始化Windows数据盘</a>           |

### 须知

- MBR分区支持的云硬盘最大容量为2 TiB，GPT分区支持的最大云硬盘容量为18 EiB，因此当云硬盘容量大于2 TiB或目前小于等于2 TiB但后续可能会扩容至2TiB以上时，请在初始化云硬盘时，分区格式选择GPT分区。
- 切换云硬盘分区格式，则该云硬盘上的数据将会被清除，请您在初始化时谨慎选择云硬盘的分区格式。

## 5.5 添加“包年/包月”磁盘

### 操作场景

对于“包年/包月”方式购买的弹性云服务器，支持添加“包年/包月”方式的云硬盘，新添加的云硬盘与弹性云服务器的到期时间相同。

### 约束与限制

- 弹性云服务器创建成功后，最多支持挂载60块磁盘。  
不同规格类型和磁盘类型支持挂载的数量不同，详细信息，请参见[一台弹性云服务器可以挂载多块磁盘吗？](#)
- 新增磁盘仅适用于为弹性云服务器增加数据盘。
- 新增磁盘的区域和可用区与弹性云服务器一致。
- 新增磁盘的计费模式与弹性云服务器一致。
- 支持新增的磁盘类型及性能介绍，请参见[云硬盘](#)。

### 操作步骤

1. 登录管理控制台。
2. 单击管理控制台左上角的，选择区域和项目。

3. 单击“”，选择“计算 > 弹性云服务器”。
4. 在弹性云服务器列表中的右上角，输入弹性云服务器名、IP地址或ID，并进行搜索。
5. 单击待添加云硬盘的“包年/包月”弹性云服务器的名称。  
系统跳转至该弹性云服务器详情页面。
6. 选择“云硬盘”页签，并单击“新增磁盘”。  
系统跳转至云硬盘购买页面。
7. 根据界面提示，设置新添加云硬盘的参数信息。
8. 单击“立即购买”。
9. 确认云硬盘的配置正确无误后，勾选协议，并单击“提交订单”。  
云硬盘购买成功后，会自动添加至指定的“包年/包月”弹性云服务器。

#### 说明

对于9中新增的磁盘，如果卸载后重新挂载，该磁盘只能挂载给原云服务器。

## 5.6 在线卸载磁盘

### 操作场景

将挂载在弹性云服务器中的磁盘卸载。

- 对于挂载在系统盘盘位（也就是“/dev/sda”或“/dev/vda”挂载点）上的磁盘，当前仅支持离线卸载。即卸载磁盘时，弹性云服务器需处于“关机”状态。
- 对于挂载在数据盘盘位（非/dev/sda挂载点）上的磁盘，不仅支持离线卸载，在使用部分操作系统时，还支持在线卸载磁盘功能。此时，弹性云服务器处于“运行中”状态。

本节旨在介绍在线卸载弹性云服务器磁盘的使用场景。

### 约束与限制

- 磁盘需挂载在数据盘盘位，即挂载点为非“/dev/sda”或“/dev/vda”挂载点。如果磁盘挂载在“/dev/sda”或“/dev/vda”挂载点上，则表示该磁盘作为弹性云服务器的系统盘使用，此时不允许在线卸载。
- 在线卸载云硬盘时，对于Windows弹性云服务器，请确认该弹性云服务器已安装UVP VMTools并且正常启用；对于Linux弹性云服务器，可以不安装UVP VMTools。  
安装UVP VMTools操作请参考[优化私有镜像](#)。
- 对于Windows弹性云服务器，在线卸载云硬盘前，请确保没有程序正在对该云硬盘进行读写操作。否则，将造成数据丢失。
- 对于Windows弹性云服务器，不支持在线卸载SCSI类型的云硬盘。
- 对于Linux弹性云服务器，在线卸载云硬盘前，客户需要先登录弹性云服务器，执行umount命令，取消待卸载云硬盘与文件系统之间的关联，并确保没有程序正在对该云硬盘进行读写操作。否则，卸载云硬盘将失败。
- 磁盘未被锁定。  
磁盘加锁时，表示被锁定，此时不能执行磁盘的卸载操作。

卸载须知

- 对于Windows弹性云服务器，在线卸载云硬盘时，如果云硬盘处于非“脱机”状态，系统会强制卸载云硬盘。此时，弹性云服务器后台可能会出现xenvbd告警提示，这种情况是正常的。
- 📖 说明

查看云硬盘状态的方法如下：
  - 选择“开始”，右键单击“计算机”，选择“管理”。  
弹出“计算机管理”窗口。
  - 在左侧导航树中，选择“存储 > 磁盘管理”。  
在右侧窗格中出现磁盘列表。
  - 查看磁盘列表中对对应磁盘的“状态”栏。

  - 弹性云服务器启动、关机、重启等操作过程中，不建议进行在线卸载云硬盘的操作。
  - 对于[支持在线卸载云硬盘的操作系统](#)以外其他操作系统的弹性云服务器，不建议进行在线卸载云硬盘操作。
  - 对于Linux弹性云服务器，在线卸载云硬盘后重新挂载云硬盘，可能会存在挂载前后盘符发生变化的情况。这是由于Linux系统的盘符分配机制造成的，属于正常情况。
  - 对于Linux弹性云服务器，在线卸载云硬盘后重启弹性云服务器，可能会存在重启前后盘符发生变化的情况。这是由于Linux系统的盘符分配机制造成的，属于正常情况。
- 支持在线卸载云硬盘的操作系统
- 支持在线卸载云硬盘的操作系统包括如下两个部分：
- 第一部分请参见[外部镜像文件的镜像格式和操作系统类型](#)。
  - 第二部分如[表5-4](#)所示。
- 表 5-4 支持在线卸载云硬盘的操作系统
- | 操作系统   | 版本                                        |
|--------|-------------------------------------------|
| CentOS | 7.3 64bit                                 |
|        | 7.2 64bit                                 |
|        | 6.8 64bit                                 |
|        | 6.7 64bit                                 |
| Debian | 8.6.0 64bit                               |
|        | 8.5.0 64bit                               |
| Fedora | 25 64bit                                  |
|        | 24 64bit                                  |
| SUSE   | SUSE Linux Enterprise Server 12 SP2 64bit |
|        | SUSE Linux Enterprise Server 12 SP1 64bit |
- 文档版本 01 (2025-06-13)

版权所有 © 华为云计算技术有限公司

308

| 操作系统                           | 版本                                        |
|--------------------------------|-------------------------------------------|
|                                | SUSE Linux Enterprise Server 11 SP4 64bit |
|                                | SUSE Linux Enterprise Server 12 64bit     |
| OpenSUSE                       | 42.2 64bit                                |
|                                | 42.1 64bit                                |
| Oracle Linux Server<br>release | 7.3 64bit                                 |
|                                | 7.2 64bit                                 |
|                                | 6.8 64bit                                 |
|                                | 6.7 64bit                                 |
| Ubuntu Server                  | 16.04 64bit                               |
|                                | 14.04 64bit                               |
|                                | 14.04.4 64bit                             |
| Windows（不支持在线卸载SCSI类型的云硬盘）     | Windows Server 2008 R2 Enterprise 64bit   |
|                                | Windows Server 2012 R2 Standard 64bit     |
|                                | Windows Server 2016 R2 Standard 64bit     |
| Redhat Linux Enterprise        | 7.3 64bit                                 |
|                                | 6.8 64bit                                 |

 说明

对于其他操作系统的弹性云服务器，请先关机然后再进行卸载磁盘操作，避免由于云硬盘设备与弹性云服务器在线卸载不兼容而产生未知问题。

操作步骤

- 在弹性云服务器页面，单击待卸载磁盘的弹性云服务器名称，跳转至弹性云服务器详情页。
- 选择“云硬盘”页签，单击待卸载磁盘所在行的“卸载”，卸载云硬盘。

5.7 扩容云硬盘

操作场景

当您已有的云硬盘存储容量不足时，可以通过扩容云硬盘增加弹性云服务器的存储容量。您可以在不中断用户业务的情况下，增加现有云硬盘的存储容量。通过扩容操作，您可以轻松提升云硬盘的空间，确保数据存储的连续性和业务的稳定性。系统盘和数据盘均支持扩容。

本文介绍通过管理控制台扩容云硬盘容量的方法，支持扩容单个云硬盘容量，也支持批量扩容云硬盘容量。

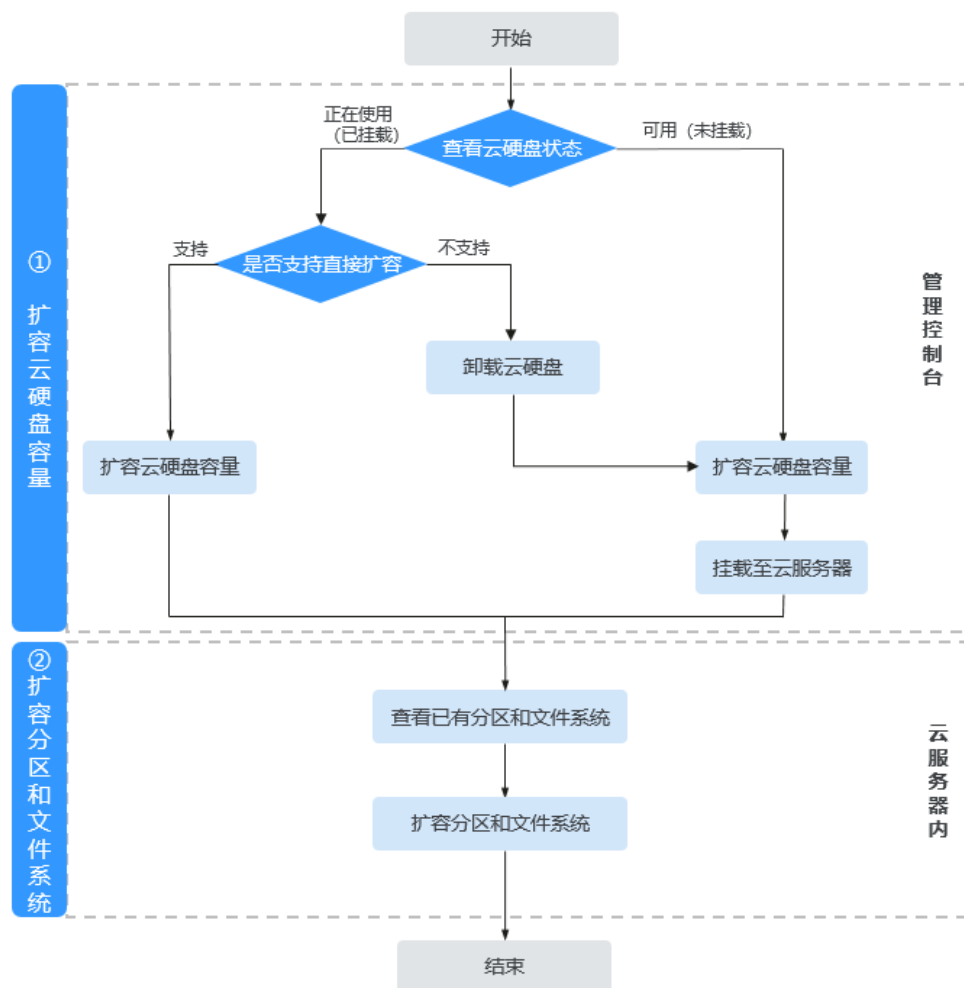
## 云硬盘扩容流程

| 操作步骤                     | 操作指导                             |
|--------------------------|----------------------------------|
| 步骤一：在控制台上扩容云硬盘容量         | <a href="#">步骤一：扩容云硬盘容量</a>      |
| 步骤二：在弹性云服务器上扩容云硬盘分区和文件系统 | <a href="#">步骤二：扩容云硬盘分区和文件系统</a> |

## 说明

- MBR分区支持的云硬盘最大容量为2 TiB，GPT分区支持的最大云硬盘容量为18 EiB。对于已选择MBR分区格式的云硬盘，如果希望将其扩容至2 TiB以上，需要先将分区格式从MBR转换为GPT后，再进行扩容，转换方式参见[如何转换磁盘MBR分区为GPT分区](#)。
- Linux系统磁盘分区形式，请参见[如何查看磁盘分区形式](#)。

图 5-4 云硬盘扩容流程



## 约束与限制

- 仅支持扩大云硬盘容量，不支持缩小云硬盘容量，即扩容后的容量必须大于现有容量，且小于等于云硬盘支持的容量上限。
- 系统盘支持的最大容量为1 TiB，数据盘支持的最大容量为32 TiB，最小扩容步长均为 1GiB。

### 说明

随弹性云服务器一起购买的系统盘，如果卸载后挂载至弹性云服务器用作数据盘时，其扩容后的容量上限仍为1 TiB。

- 批量扩容云硬盘的数量上限为50个。
- ECS实例仅在“运行中”或“关机”状态下支持本操作。
- 部分ECS实例磁盘扩容后，需要重启实例才能生效，详细约束请参见[查询操作系统是否满足要求](#)。

## 计费说明

云硬盘扩容，会收取新增容量的费用。新增容量的计费方式和购买云硬盘时的计费方式一致。

- 按需计费模式的云硬盘：扩容后立即生效，并立即按照新容量的费用开始计费。
- 包年/包月计费模式的云硬盘：扩容容量需要补差价，扩容后云硬盘的到期时间不变。

云硬盘计费详细内容，请参见[云硬盘计费说明](#)。

## 前提条件

扩容前请通过CBR或快照功能备份数据，防止误操作造成数据丢失。CBR备份请参见[备份弹性云服务器](#)，快照备份请参见[创建云硬盘快照](#)。两种备份方式的差异请参考[云硬盘备份与快照的区别](#)。

## 步骤一：扩容云硬盘容量

1. 登录管理控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”。
4. 选择扩容入口。
  - 方法一：支持扩容弹性云服务器挂载的单个磁盘。
    - i. 在待扩容磁盘的弹性云服务器的“操作”列，单击“更多 > 磁盘/备份 > 扩容磁盘”。
    - ii. 在“扩容磁盘”页面的磁盘列表中，勾选待扩容的磁盘，系统跳转至云硬盘控制台的“扩容磁盘”页面。

### 说明

如果列表中无可扩容磁盘，则表示当前弹性云服务器挂载的磁盘不支持扩容，详细内容请参见[扩容云硬盘容量](#)的“约束与限制”。

- 方法二：支持批量扩容多个磁盘。



- i. 在[磁盘列表页](#)，勾选待扩容的磁盘。  
如果要批量扩容磁盘，可勾选多个磁盘。
  - ii. 单击列表上方左侧的“扩容”，系统弹出“批量扩容”页面。
  - iii. 单击“确定”，系统跳转至“扩容磁盘”页面。
5. 根据界面提示，设置“目标容量”。  
目标容量表示扩容后的容量，目标容量不允许小于当前容量。

#### 说明

- 如果扩容多个磁盘，可以选择为每个磁盘设置“目标容量”，也可以在磁盘列表上方，通过“批量设置扩容后容量”将多个磁盘扩容至相同的目标容量。
6. 设置完成后，单击“下一步”并根据界面提示完成订单提交。  
当云硬盘状态由“正在扩容”变为“正在使用”或“可用”，并且容量增加时，表示已成功扩大云硬盘存储容量。云硬盘状态查看方法请参见[查看云硬盘详细信息](#)。  
如果云硬盘状态为“可用”，还需要将扩容成功后的云硬盘挂载至云服务器，具体请参见[为ECS挂载磁盘](#)。  
如果在弹性云服务器关机状态下执行扩容操作，则开机后，Windows系统盘、Windows数据盘、Linux系统盘的新增容量可能会自动扩展至末尾分区内，此时新增容量可以直接使用。如果新增容量未自动扩展，请参考[步骤二：扩容云硬盘分区和文件系统](#)自行扩展分区和文件系统。  
更多关于扩容云硬盘的详细操作，请参考[云硬盘扩容概述](#)。

## 步骤二：扩容云硬盘分区和文件系统

在管理控制台扩容云硬盘容量成功后，仅扩大了云硬盘的存储容量，对应的分区和文件系统并未扩容，还需要登录云服务器，扩容云硬盘的分区和文件系统，才可以看到新增容量并使用。即将扩容新增的容量划分至已有分区和文件系统内或使用扩容新增的容量新建分区和文件系统。

不同云服务器的操作系统的扩容分区和文件系统操作可能不同，具体如下：

- Linux操作系统，请参见[扩容云硬盘分区和文件系统（Linux）](#)。
- Windows操作系统，请参见[扩容云硬盘分区和文件系统（Windows）](#)。

## 相关操作

对于Windows弹性云服务器，如果您想通过清理磁盘文件的方式扩大磁盘容量，可以参考[清理 WinSxS 文件夹](#)使用Windows中内置的工具来减小WinSxS文件夹的大小。

云硬盘扩容常见问题请参见[云硬盘扩容问题](#)。

如果扩容失败，您可以使用快照回滚数据，详情请参见[使用快照回滚数据至云硬盘](#)。

## 5.8 扩容本地盘

### 操作场景

对于磁盘增强型弹性云服务器，可使用本地盘和云硬盘两类磁盘存储数据。本地盘常用于存放用户的业务数据，磁盘吞吐量更高。



由于磁盘增强型弹性云服务器不支持规格变更，因此，当本地盘容量不足时，需要通过创建更大规格磁盘增强型弹性云服务器的方式进行扩容处理，原磁盘增强型弹性云服务器中保存的数据可以通过云硬盘进行迁移。

## 操作步骤

1. 根据需要转移的数据量大小，创建云硬盘。
2. 挂载云硬盘。  
将步骤1中创建的云硬盘挂载至磁盘增强型弹性云服务器。
3. 备份本地盘数据。  
将本地盘中需要转移的数据，备份至当前规格的磁盘增强型弹性云服务器的云硬盘中。
  - 对于Windows系统弹性云服务器，建议您直接复制需要转移的数据至目标云硬盘。
  - 对于Linux系统弹性云服务器，建议您使用cp命令复制需要转移的数据至目标云硬盘。
4. 卸载云硬盘。
  - a. 在弹性云服务器页面，选择该规格的磁盘增强型弹性云服务器，确认云服务器为“关机”状态。  
如果云服务器为“开机”状态，您可单击“更多 > 关机”将云服务器关机。
  - b. 单击该磁盘增强型弹性云服务器的名称，查看详情。
  - c. 选择“云硬盘”页签，并单击数据盘所在行的“卸载”，卸载该云硬盘。
5. 准备一台大规格的磁盘增强型弹性云服务器。  
该云服务器的规格大于原云服务器规格，且其本地盘容量能够满足用户的需求。
6. 挂载云硬盘至大规格的磁盘增强型弹性云服务器。  
在弹性云服务器页面，单击步骤5中准备的弹性云服务器名称，展开详情。
7. 选择“云硬盘”页签，并单击“挂载磁盘”。  
在“挂载磁盘”对话框中，选择步骤4中卸载的云硬盘，并设置挂载点。
8. 迁移云硬盘数据。  
将步骤7中云硬盘的数据，迁移至大规格磁盘增强型弹性云服务器的本地盘中。

# 6 弹性网卡管理

## 6.1 弹性网卡概述

弹性网卡（Elastic Network Interfaces，以下简称ENI）即虚拟网卡，您可以通过创建并配置弹性网卡，并将其附加到您的云服务器实例（包括弹性云服务器和裸金属服务器）上，实现灵活、高可用的网络方案配置。

### 弹性网卡类型

- **主弹性网卡：**在创建实例时，随实例默认创建的弹性网卡称为主弹性网卡。无法解除主弹性网卡和实例的绑定关系。
- **扩展弹性网卡：**您在弹性网卡控制台创建的是扩展弹性网卡，可以将网卡绑定到实例上，也可以解除网卡和实例的绑定关系。

### 弹性网卡应用场景

- **灵活迁移**  
通过将弹性网卡从云服务器实例解绑后再绑定到另外一台服务器实例，保留已绑定私网IP、弹性公网IP和安全组策略，无需重新配置关联关系，将故障实例上的业务流量快速迁移到备用实例，实现服务快速恢复。
- **业务分离管理**  
可以为服务器实例配置多个分属于同一VPC内不同子网的弹性网卡，特定网卡分别承载云服务器实例的内网、外网、管理网流量。针对子网可独立设置访问安全控制策略与路由策略，弹性网卡也可配置独立安全组策略，从而实现网络隔离与业务流量分离。

### 弹性网卡的使用限制

- 云服务器可绑定的弹性网卡数量由云服务器实例规格决定，具体请参见[规格清单](#)。

表 6-1 不同类型网卡使用限制

| 弹性网卡类型 | 创建网卡           | 实例绑定                   | 外部通信                                                            | 网卡与云公共服务区的互通能力 |
|--------|----------------|------------------------|-----------------------------------------------------------------|----------------|
| 主弹性网卡  | 随实例默认创建，无法独立创建 | 无法解除和实例的绑定关系           | 默认支持和外部正常通信                                                     | 具备             |
| 扩展弹性网卡 | 可以在弹性网卡控制台单独创建 | 支持绑定到实例上，也可以解除和实例的绑定关系 | 需要在弹性云服务器内部配置策略路由来实现和外部正常通信<br><a href="#">配置多网卡弹性云服务器的策略路由</a> | 不具备            |

- 扩展弹性网卡不支持直接访问华为云内公共云服务，如内网DNS等，推荐使用VPCEP访问华为云公共云服务，具体参见[购买连接“接口”型终端节点服务的终端节点](#)。

相关链接

- [弹性云服务器添加网卡后是否会自动启动？](#)
- [怎样修改云服务器子网的网段？](#)
- [怎样检查IB云服务器的网络是否正常？](#)
- [怎样给IB网卡手动配置IP地址？](#)
- [网卡无法正常工作，怎么办？](#)

6.2 绑定弹性网卡

操作场景

当您的弹性云服务器需要多个弹性网卡时，可以参考下面步骤为弹性云服务器绑定弹性网卡。

操作步骤

1. 登录管理控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”。
4. 单击待绑定弹性网卡的弹性云服务器名称。  
系统跳转至该弹性云服务器详情页面。
5. 在“弹性网卡”页签，单击“绑定弹性网卡”。
6. 选择不同方式，为弹性云服务器绑定弹性网卡。

- 选择“选择已有弹性网卡”。
  - i. （可选）根据“名称”、“ID”或“私有IP”搜索待绑定的弹性网卡。
  - ii. 在弹性网卡列表中，勾选待绑定的弹性网卡。
- 选择“创建新的弹性网卡”。  
根据界面提示，设置待增加弹性网卡的子网和安全组。

图 6-1 选择子网和安全组

绑定弹性网卡

云服务器名称ecs-

方式

选择已有弹性网卡

创建新的弹性网卡

所属虚拟私有云vpc-f551

所属子网

subnet:

查看已有子网

私有IP地址

自动分配IP地址

查看已使用IP地址

选择安全组

请输入安全组名称搜索

查看安全组

☐安全组名称

描述

☐defaultDefault security group

取消

确定

- 所属子网：待绑定弹性网卡所属的子网。
  - 私有IP地址：如果需要给弹性云服务器添加一张指定IP地址的网卡，用户需填写“私有IP地址”。
  - 选择安全组：您可以同时勾选多个安全组，此时，弹性云服务器的访问规则遵循几个安全组规则的并集。
7. 单击“确定”。
- 为保证扩展弹性网卡和外部正常通信，弹性网卡绑定完成后，还需要在云服务器内部为这些弹性网卡配置策略路由。
- 详细操作，请参见[配置多网卡弹性云服务器的策略路由](#)。

后续任务

- 部分操作系统无法识别新绑定的弹性网卡，需手动激活弹性网卡。下面以Ubuntu系统为例介绍具体激活弹性网卡的操作步骤，其他操作系统请自行完成相关操作，如有问题，请参见对应操作系统的官网指导或手册来完成操作。
1. 在弹性云服务器所在行的“操作”列下，单击“远程登录”。  
登录弹性云服务器。
  2. 执行如下命令，查看弹性网卡名称。  
**ifconfig -a**  
例如，查询到的弹性网卡名为：eth2。
  3. 执行如下命令，进入相应目录。

```
cd /etc/network
```

4. 执行如下命令，打开interfaces文件。

```
vi interfaces
```

5. 在interfaces文件中，增加类似如下信息。

```
auto eth2
```

```
iface eth2 inet dhcp
```

6. 执行如下命令，保存并退出interfaces文件。

```
:wq
```

7. 执行命令**ifup ethX**或**/etc/init.d/networking restart**，使新增弹性网卡生效。  
上述命令中的X为具体的网卡名称序号，例如，**ifup eth2**。

8. 执行如下命令，查看回显信息中是否包括2查询到的弹性网卡。

```
ifconfig
```

例如，回显信息中包含弹性网卡eth2。

- 是，表示新增弹性网卡生效，结束。
- 否，表示新增弹性网卡未生效，执行9。

9. 登录管理控制台，在弹性云服务器所在行的“操作”列下，选择“更多”，并单击“重启”。

10. 再次执行命令**ifconfig**，查看回显信息中是否包括2查询到的弹性网卡。

- 是，结束。
- 否，请联系客服获取技术支持。

## 6.3 解绑弹性网卡

### 操作场景

弹性云服务器最多可以有12个弹性网卡，其中包括一个主弹性网卡，且主弹性网卡不可删除。本节操作介绍解绑弹性网卡的操作步骤，当您的弹性云服务器需要解绑主网卡以外的其他弹性网卡时，可以参考以下操作步骤。

#### 注意

解绑弹性网卡前，请谨慎评估该操作可能带来的业务影响，避免由于误操作造成网络中断。

### 操作步骤

1. 登录管理控制台。
2. 单击“”，选择“计算 > 弹性云服务器”。
3. 在弹性云服务器列表中，单击待解绑弹性网卡的弹性云服务器名称。  
系统跳转至该弹性云服务器详情页面。
4. 选择“弹性网卡”页签，并单击待解绑弹性网卡右侧的“解绑”。

#### 说明

对于该弹性云服务器的主弹性网卡（默认为网卡列表中显示的第一个弹性网卡），用户不能执行解绑操作。

5. 在弹出的对话框中单击“是”，解绑弹性网卡。

#### 说明

对于部分弹性云服务器，不支持在线解绑弹性网卡功能，具体以界面显示为准。您需要先关机弹性云服务器，然后再执行解绑弹性网卡操作。

## 6.4 切换虚拟私有云

### 操作场景

本节操作介绍为弹性云服务器切换虚拟私有云的操作步骤。

您可以为单台弹性云服务器切换虚拟私有云，也可以通过云运维中心（Cloud Operations Center，简称COC）的作业管理功能批量为多台弹性云服务器切换虚拟私有云。

为云耀云服务器（旧版）切换虚拟私有云的操作指导，请参见[切换虚拟私有云](#)。

### 约束与限制

- 仅支持处于“运行中”或“关机”状态的弹性云服务器执行此操作。
- 仅支持单网卡切换虚拟私有云。
- 切换虚拟私有云前如果重装/切换过云服务器的操作系统，请先登录云服务器，验证重装/切换时设置的密码或密钥是否注入成功。
  - 如果成功登录云服务器，说明密码或密钥注入完成，可继续执行其他操作。
  - 否则说明系统正在注入密码或密钥信息，在此期间请勿对云服务器执行其他操作。
- 切换虚拟私有云过程中，请勿执行绑定、解绑或更换弹性公网IP等操作，若执行会提示权限不足，无需处理。
- 如果网卡上有IPv6地址，无法切换虚拟私有云。
- 批量为多台ECS切换虚拟私有云时，单次最多支持50个ECS。

### 切换须知

- 切换虚拟私有云支持在开机状态下操作，但是过程中会导致云服务器网络中断。

#### 说明

若弹性云服务器处于开机状态，可能由于网卡有流量访问而导致切换虚拟私有云失败，建议您稍后重试或关机后再进行切换。

- 切换虚拟私有云后，云服务器子网、私有IP地址、MAC地址、操作系统内网卡名称都会发生改变。
- 切换虚拟私有云后，请重新配置源/目的检查和虚拟IP地址。
- 虚拟私有云切换完成后，与网络配置相关的应用软件需要重新配置。与网络相关的服务也需要重新配置，例如ELB、VPN、NAT、流量镜像、全域弹性公网IP、DNS等。

## 前提条件

已准备好待切换的目标VPC、子网、私有IP地址和安全组。

如果批量为多台弹性云服务器切换VPC，则：

- 开通并授权云运维中心（Cloud Operations Center，简称COC）。  
对于IAM用户，需额外配置COC资源操作类权限，详细内容，请参见[配置ECS自助运维自定义策略](#)。
- 创建委托以授权云运维中心访问ECS。  
详细内容，请参见[委托授权云运维中心访问ECS](#)。

## 操作步骤

您可以根据业务需要选择为单台ECS切换VPC，或者批量为多台ECS切换VPC。

### 切换虚拟私有云（单台 ECS）

1. 登录管理控制台。
  2. 单击“”，选择“计算 > 弹性云服务器”。
  3. 在弹性云服务器列表中，单击“操作”列下的“更多 > 网络/安全组 > 切换VPC”。
- 系统弹窗显示“切换VPC”页面。

图 6-2 切换虚拟私有云

切换VPC

切换虚拟私有云会导致云服务器网络中断，同时更改云服务器子网、IP地址、MAC地址。  
切换虚拟私有云过程中，请勿操作云服务器的弹性公网IP，或对云服务器做其他操作。  
切换虚拟私有云后，请重新配置源/目的检查、虚拟IP地址、网络相关的服务和应用软件（例如ELB、VPN、NAT、流量镜像、全域弹性公网IP、DNS等）。

云服务器ecs-

虚拟私有云vpc-

查看虚拟私有云

子网subnet-

查看已有子网

私有IP地址

现在创建

使用已有

自动分配IP地址

查看已使用IP地址

安全组-请选择-

查看安全组

取消

确定

4. 根据界面提示，在下拉列表中选择可用的虚拟私有云、子网，设置私有IP地址和安全组。  
您可以同时勾选多个安全组，此时，弹性云服务器的访问规则遵循几个安全组规则的并集。

说明

使用多个安全组可能会影响弹性云服务器的网络性能，建议您选择安全组的数量不多于5个。

5. 单击“确定”。

切换虚拟私有云（多台 ECS）

1. 登录管理控制台。
2. 单击“≡”，选择“计算 > 弹性云服务器”。
3. 在弹性云服务器列表中，勾选待批量切换VPC的多台ECS。
4. 在弹性云服务器列表上方，单击“更多 > 切换VPC”。

图 6-3 切换虚拟私有云



5. 在切换VPC页面，选择“IAM权限委托”，该委托需授权COC访问ECS，并具有ECS的相关操作权限。
- 若无可用委托，则单击“新建委托”进行创建，详细操作，请参见[委托授权云运维中心访问ECS](#)。
6. 根据界面提示，在下拉列表中选择可用的虚拟私有云、子网，设置私有IP地址和安全组。
- 您可以同时勾选多个安全组，此时，弹性云服务器的访问规则遵循几个安全组规则的并集。



#### 说明

使用多个安全组可能会影响弹性云服务器的网络性能，建议您选择安全组的数量不多于5个。

7. 单击“确定”。

批量切换VPC的操作下发成功，您可以进入云运维中心查看[作业工单](#)的操作结果。

更多关于云运维中心作业管理功能的介绍，请参见[执行公共作业](#)。

## 6.5 修改私有 IP 地址

### 操作场景

云平台支持修改主网卡的私有IP地址，具体操作请参见本节内容。如需修改扩展网卡的私有IP地址，请删除网卡，并挂载新网卡。

### 约束与限制

- 弹性云服务器已关机。
- 如果网卡绑定了虚拟IP或者DNAT规则，需要先解绑。
- 如果网卡上有IPv6地址，无法修改（包括IPv4和IPv6的）私有IP地址。
- 如需修改弹性负载均衡后端服务器的私有IP地址，请先移出后端服务器组后再修改私有IP。

### 操作步骤

1. 登录管理控制台。
2. 单击“”，选择“计算 > 弹性云服务器”。
3. 单击待修改私有IP地址的弹性云服务器名称。  
系统跳转至该弹性云服务器详情页面。
4. 选择“弹性网卡”页签，并单击主网卡所在行的“修改私有IP地址”。
5. 请根据需要修改主网卡的“子网”、“私有IP地址”。

#### 说明

只能在同一VPC下更换子网。

如果未填写修改后的“私有IP地址”，系统会自动分配一个新的私有IP地址给主网卡使用。

## 6.6 管理虚拟 IP 地址

### 操作场景

虚拟IP地址用于为网卡提供第二个IP地址，同时支持与多个的网卡绑定，从而实现多个弹性云服务器之间的高可用性。

## 绑定虚拟 IP 地址

1. 登录管理控制台。
2. 单击“”，选择“计算 > 弹性云服务器”。
3. 在弹性云服务器列表中，单击待绑定虚拟IP地址的弹性云服务器名称。  
系统跳转至该弹性云服务器详情页面。
4. 选择“弹性网卡”页签，单击“管理虚拟IP地址”。
5. 选择“IP地址管理”页签，在需要绑定弹性公网IP或者弹性云服务器的虚拟IP地址所在行的操作列下，单击“绑定弹性公网IP”或者“绑定服务器”。  
多个主备部署的弹性云服务器可以在绑定虚拟IP地址时选择同一个虚拟IP地址，增强容灾性能。
6. 单击“确定”。

## 登录 ECS 配置虚拟 IP 地址

当为一个ECS绑定一个虚拟IP或者多个虚拟IP时，在控制台执行完绑定虚拟IP的操作后，您还需要参考以下章节，登录弹性云服务器手工配置虚拟IP地址。

本文提供以下操作系统的配置示例，其他操作系统，请您参考对应官网帮助文档进行配置。弹性云服务器重启后，配置不会丢失。

- Linux系统：CentOS 7.2 64bit、Ubuntu 22.04 server 64bit
- Windows系统：Windows Server

## Linux 系统（CentOS）

以下操作以“CentOS 7.2 64bit”为例，供您参考。

1. 执行以下命令，查看并记录需要绑定虚拟IP的网卡及对应连接。

**nmcli connection**

回显类似如下信息：

```
[172.16.0.247 ~]# nmcli connection
NAME UUID TYPE DEVICE
Wired connection 1 5e72ec5a-6165-3bd6-a34b-ce43981acb27 ethernet eth0
docker0 cd351a91-c5eb-4b69-83eb-df092a2ccf6b bridge docker0
```

本示例的回显信息说明如下：

- **DEVICE**列的eth0为需要绑定虚拟IP的网卡。
  - **NAME**列的Wired connection 1为网卡对应的连接。
2. 执行以下命令，在目标网卡连接中添加虚拟IP。

**nmcli connection modify "网卡对应的连接名称" +ipv4.addresses 虚拟IP地址**

参数说明如下：

- 网卡对应的连接名称：为1中查到的网卡对应的连接，本示例中为**Wired connection 1**。
- 虚拟IP地址：待添加的虚拟IP地址，如果一次添加多个虚拟IP地址，多个虚拟IP地址之间用“,”隔开。

命令示例：

- 添加单个虚拟IP：**nmcli connection modify "Wired connection 1" +ipv4.addresses 172.16.0.125**

- 添加多个虚拟IP: **nmcli connection modify "Wired connection 1" +ipv4.addresses 172.16.0.125,172.16.0.126**
3. 执行以下命令,使2的配置生效。

**nmcli connection up "网卡对应的连接名称"**

命令示例:

**nmcli connection up "Wired connection 1"**

回显类似如下信息:

```
[root@ecs-X-ubuntu:~]# nmcli connection up "Wired connection 1"
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/6)
```

4. 执行以下命令,检查虚拟IP配置是否成功。

**ip a**

回显类似如下信息,可以看到eth0网卡下存在虚拟IP地址,为172.16.0.125。

```
[root@ecs-X-ubuntu:~]# 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 pfifo_fast state UP group default qlen 1000
 link/ether fa:16:3e:c5:d5:cd brd ff:ff:ff:ff:ff:ff
 inet 172.16.0.247/24 brd 172.16.0.255 scope global noprefixroute dynamic eth0
 valid_lft 86398sec preferred_lft 86398sec
 inet 172.16.0.125/32 brd 172.16.0.125 scope global noprefixroute eth0
 valid_lft forever preferred_lft forever
 inet6 2001:db8:a583:62c:7dd3:a19a:4031:d6fb/128 scope global tentative noprefixroute dynamic
 valid_lft 86400sec preferred_lft 86400sec
 inet6 fe80::5371:9bf9:b652:e35b/64 scope link noprefixroute
 valid_lft forever preferred_lft forever
```

## 说明

如果您需要删除已添加的虚拟IP,可以使用以下方法:

1. 在目标网卡连接中删除虚拟IP。

**nmcli connection modify "网卡对应的连接名称" -ipv4.addresses 虚拟IP地址**

一次删除多个虚拟IP地址时,多个IP之间用“,”隔开,命令示例:

- 删除单个虚拟IP: **nmcli connection modify "Wired connection 1" -ipv4.addresses 172.16.0.125**
- 删除多个虚拟IP: **nmcli connection modify "Wired connection 1" -ipv4.addresses 172.16.0.125,172.16.0.126**

2. 参考3,使删除操作生效。

## Linux 系统 (Ubuntu)

以下操作以“Ubuntu 22.04 server 64bit”为例,当弹性云服务器的操作系统为Ubuntu 22和Ubuntu 20时,请您参考下述方法。

1. 执行以下命令,查看并记录需要绑定虚拟IP的网卡。

**ifconfig**

回显类似如下信息,本示例中绑定虚拟IP的网卡名称为eth0。

```
root@ecs-X-ubuntu:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
 inet 172.16.0.210 netmask 255.255.255.0 broadcast 172.16.0.255
 inet6 fe80::f816:3eff:fe01:f1c3 prefixlen 64 scopeid 0x20<link>
 ether fa:16:3e:01:f1:c3 txqueuelen 1000 (Ethernet)
 RX packets 43915 bytes 63606486 (63.6 MB)
 RX errors 0 dropped 0 overruns 0 frame 0
 TX packets 3364 bytes 455617 (455.6 KB)
 TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
...
```

2. 执行以下命令，进入“/etc/netplan”目录。

```
cd /etc/netplan
```

3. 执行以下命令，为目标网卡添加虚拟IP地址。

- a. 执行以下命令，打开配置文件“01-netcfg.yaml”。

```
vim 01-netcfg.yaml
```

- b. 按i进入编辑模式。

- c. 在对应网卡配置区域内，添加虚拟IP地址。

本示例为eth0添加虚拟IP地址，待添加内容如下：

**addresses:**

**- 172.16.0.26/32**

添加后文件内容如下：

```
network:
 version: 2
 renderer: NetworkManager
 ethernets:
 eth0:
 dhcp4: true
 addresses:
 - 172.16.0.26/32
 eth1:
 dhcp4: true
 eth2:
 dhcp4: true
 eth3:
 dhcp4: true
 eth4:
 dhcp4: true
```

- d. 添加完成后，按“ESC”，并输入“:wq!”，保存后退出文件。

4. 执行以下命令，使3的配置生效。

```
netplan apply
```

5. 执行以下命令，检查虚拟IP配置是否成功。

```
ip a
```

回显类似如下信息，可以看到eth0网卡下存在虚拟IP地址，为172.16.0.26。

```
root@ecs-X-ubuntu:/etc/netplan# ip a
...
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
 link/ether fa:16:3e:01:f1:c3 brd ff:ff:ff:ff:ff:ff
 altname enp0s3
 altname ens3
 inet 172.16.0.26/32 scope global noprefixroute eth0
 valid_lft forever preferred_lft forever
 inet 172.16.0.210/24 brd 172.16.0.255 scope global dynamic noprefixroute eth0
 valid_lft 107999971sec preferred_lft 107999971sec
 inet6 fe80::f816:3eff:fe01:f1c3/64 scope link
 valid_lft forever preferred_lft forever
```

### 📖 说明

如果您需要删除已添加的虚拟IP，可以使用以下方法：

1. 参考3，打开配置文件“01-netcfg.yaml”，并删除对应网卡下虚拟IP的地址。
2. 参考4，使删除操作生效。

## Windows 系统（Windows Server）

以下操作以“Windows Server”为例，供您参考。

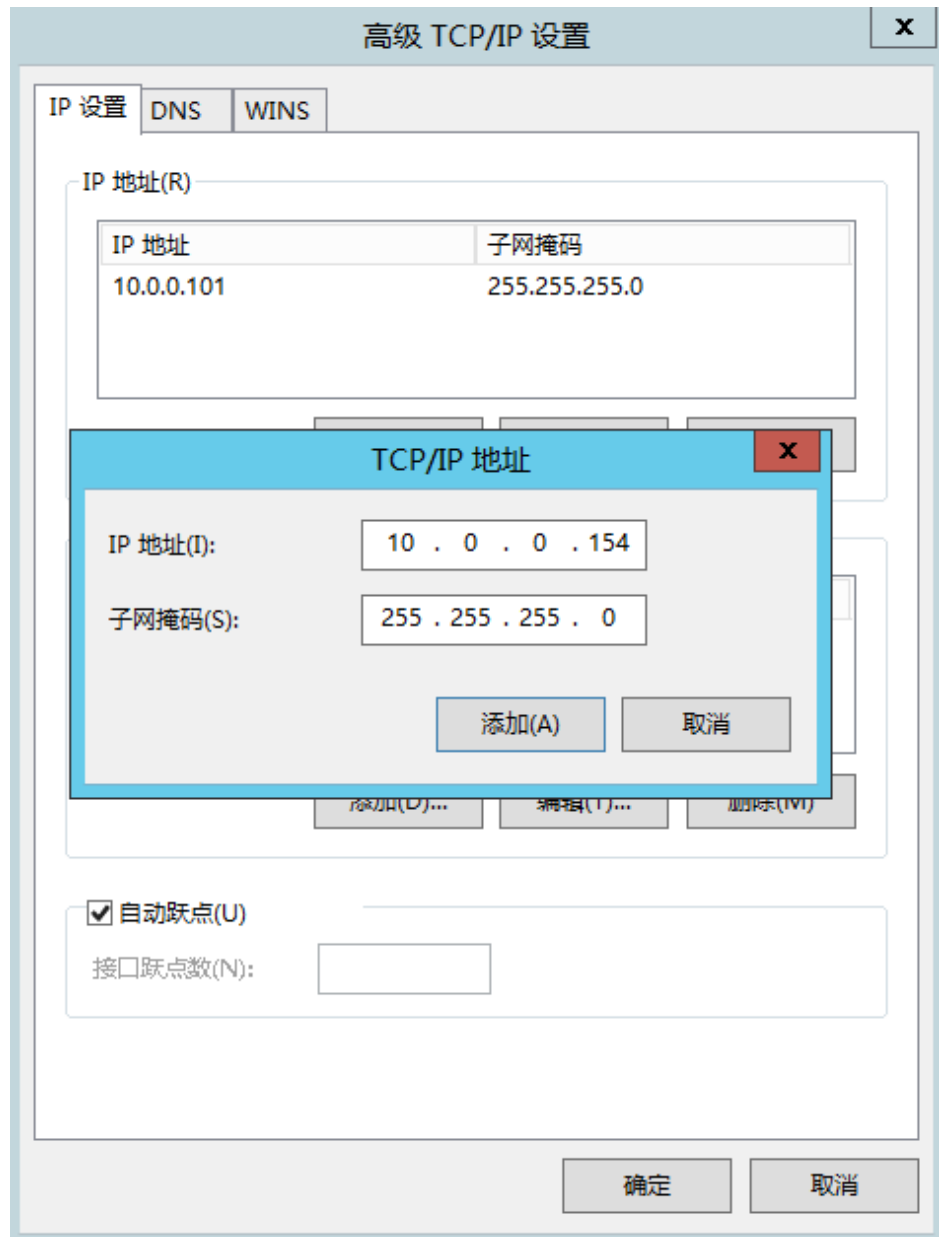
1. 在“控制面板 > 网络和共享中心”路径下，单击对应的本地连接。
2. 在打开的本地连接页面中，单击“属性”。
3. 在“网络”页签中选择“Internet 协议版本 4（TCP/IPv4）”。
4. 单击“属性”。
5. 选择“使用下面的IP地址”，IP地址配置为弹性云服务器的私有IP地址，例如：10.0.0.101。

图 6-4 配置私有 IP 地址



6. 单击“高级”。
7. 在“IP设置”页签内“IP地址”区域，单击“添加”。  
添加虚拟IP地址，例如：10.0.0.154。

图 6-5 配置虚拟 IP 地址



8. 单击“确定”，保存更改。
9. 在“开始”菜单中打开Windows命令行窗口，执行以下命令确认是否配置了虚拟IP地址。

#### **ipconfig /all**

回显样例中IPv4 Address包含虚拟IP地址10.0.0.154，表示弹性云服务器内部网卡的虚拟IP地址配置正常。

## 相关操作

当不再使用虚拟IP时，可以删除虚拟IP地址，详细内容，请参考[删除虚拟IP地址](#)。

弹性云服务器的网卡解绑并删除虚拟IP地址后，需要在弹性云服务器上手工删除虚拟IP地址。

**Linux系统**（本文以“CentOS 7.2 64bit”为例，其他规格请参考对应官网帮助文档）

1. 执行以下命令，查看并记录需要删除虚拟IP的网卡及对应连接。

**nmcli connection**

回显类似如下信息：

```
1172.16.0.247_m4net18-ecs-post-guest-dgdb-ipv4 ~]#nmcli connection
NAME UUID TYPE DEVICE
Wired connection 1 5e72ec5a-6165-3bd6-a34b-ce43981acb27 ethernet eth0
docker0 cd351a91-c5eb-4b69-83eb-df092a2ccf6b bridge docker0
```

本示例的回显信息说明如下：

- **DEVICE**列的eth0为需要删除虚拟IP的网卡。
- **NAME**列的Wired connection 1为网卡对应的连接。

2. 执行以下命令，在目标连接中删除虚拟IP。

**nmcli connection delete "CONNECTION" ipv4.addresses VIP**

参数说明如下：

- **CONNECTION**：为步骤1中查到的网卡对应的连接。
- **VIP**：待删除的虚拟IP地址。

3. 执行以下命令，使配置生效。

**nmcli connection up "CONNECTION"**

命令示例：

**nmcli connection up "Wired connection 1"**

4. 执行以下命令，检查虚拟IP配置是否成功。

**ip a**

可以看到eth0网卡下已经不存在添加的虚拟IP地址。

## 6.7 开启网卡多队列功能

### 操作场景

随着网络IO的带宽不断提升，单核CPU处理网络中断存在瓶颈，不能完全满足网卡的需求，通过开启网卡多队列功能，您可以将弹性云服务器中的网卡中断分散给不同的CPU处理，以满足网卡的需求，从而提升网络PPS和带宽性能。

假设以下场景所述的弹性云服务器满足规格和虚拟化类型要求：

- 使用[网卡多队列支持列表](#)中的公共镜像创建的弹性云服务器，默认已开启网卡多队列，无需执行本节操作。
- 对于私有镜像场景，如果您的外部镜像文件的操作系统在[网卡多队列支持列表](#)范围内，需要按照如下流程开启网卡多队列：
  - a. [将外部镜像文件导入镜像服务控制台](#)。
  - b. [为私有镜像添加网卡多队列标签](#)。
  - c. [使用私有镜像创建弹性云服务器](#)。
  - d. [执行网卡多队列的配置脚本](#)。

#### 说明

云服务器开启网卡多队列功能后，如果后续有新增或删除网卡，切换VPC等操作，需要重新对云服务器设置网卡多队列，详细操作请参考[执行网卡多队列的配置脚本](#)。

网卡多队列支持列表

网卡多队列的支持情况和实例规格、虚拟化类型、镜像的操作系统有关，只有同时满足这些要求，弹性云服务器才能开启网卡多队列功能。

- 支持网卡多队列的实例规格请参见“[规格清单](#)”。

说明

网卡多队列数为大于1的值，表示支持网卡多队列。

- 虚拟化类型必须为KVM。
- [表6-3](#)所列的Linux公共镜像，支持网卡多队列。

说明

- Windows操作系统弹性云服务器的驱动pvdriver有一套动态调整网卡队列数的策略，会根据vCPU数计算队列数并进行动态调整，因此无需对windows网卡多队列的队列数进行设置。
- Windows 2008公共镜像已下线，可通过私有镜像支持。
- Linux操作系统弹性云服务器建议将操作系统内核版本升级至2.6.35及以上，否则不支持网卡多队列。  
建议您使用命令**uname -r**查询内核版本，如果低于2.6.35请联系技术支持升级内核。

表 6-2 Windows 弹性云服务器网卡多队列支持列表

| 镜像                                                          | 是否支持多队列 | 是否默认开启多队列 |
|-------------------------------------------------------------|---------|-----------|
| Windows Server 2008 R2 Standard/Enterprise/DataCenter 64bit | 是       | 是         |
| Windows Server 2008 Enterprise SP2 64bit                    | 是       | 是         |
| Windows Server 2008 Web R2 64 bit                           | 是       | 是         |
| Windows Server 2008 R2 Enterprise 64bit_WithGPUdriver       | 是       | 是         |
| Windows Server 2012 R2 Standard 64bit_WithGPUdriver         | 是       | 是         |
| Windows Server 2012 R2 Standard/DataCenter 64 bit           | 是       | 是         |
| Windows Server 2016 Standard/DataCenter 64 bit              | 是       | 是         |
| Windows Server 2019 DataCenter 64 bit                       | 是       | 是         |



表 6-3 Linux 弹性云服务器网卡多队列支持列表

| 镜像                                                 | 是否支持多队列 | 是否默认开启多队列 |
|----------------------------------------------------|---------|-----------|
| Ubuntu 14.04/16.04/18.04/20.04 server 64bit        | 是       | 是         |
| OpenSUSE 42.2/15.* 64bit                           | 是       | 是         |
| SUSE Enterprise 12 SP1/SP2 64bit                   | 是       | 是         |
| CentOS 6.8/6.9/7.*/8.* 64bit                       | 是       | 是         |
| Debian 8.0.0/8.8.0/8.9.0/9.0.0/10.0.0/10.2.0 64bit | 是       | 是         |
| Fedora 24/25/30 64bit                              | 是       | 是         |
| EulerOS 2.2/2.3/2.5 64bit                          | 是       | 是         |

将外部镜像文件导入镜像服务控制台

将外部镜像文件导入镜像服务控制台，详细操作请参见《 镜像服务用户指南 》中“注册镜像”章节。导入完成后，在镜像详情页查看“网卡多队列”参数取值。

- 如果为“支持”，执行[使用私有镜像创建弹性云服务器](#)。
- 如果为“不支持”，执行[为镜像添加网卡多队列标签](#)。

为镜像添加网卡多队列标签

Windows操作系统暂未商用支持网卡多队列，如果对Windows操作系统镜像添加网卡多队列标签，开启网卡多队列功能，可能会引起操作系统启动速度变慢等问题。

用户可以选择以下任一种方式设置镜像的网卡多队列属性。

方式1：

1. 登录管理控制台。
2. 单击“”，选择“计算 > 镜像服务”。
3. 单击“私有镜像”页签，在对应镜像所在行的“操作”列下，单击“修改”。
4. 设置镜像的网卡多队列属性。

方式2：

1. 登录管理控制台。
2. 单击“”，选择“计算 > 镜像服务”。
3. 单击“私有镜像”页签，在镜像列表中，单击镜像名称，进入镜像详情页面。
4. 单击右上角的“修改”，在弹出的“修改镜像”对话框中，设置镜像的网卡多队列属性。

方法3：通过API为镜像添加网卡多队列标签hw\_vif\_multiqueue\_enabled

1. 获取Token的方法请参考“[认证鉴权](#)”。

2. “更新镜像信息”的API使用方法请参考“[更新镜像信息（OpenStack原生）](#)”。
3. 在请求消息头中增加“X-Auth-Token”。  
“X-Auth-Token”的取值为步骤1中获取的Token。
4. 在请求消息头中增加“Content-Type”。

“Content-Type”取值为application/openstack-images-v2.1-json-patch

请求的URI格式为：

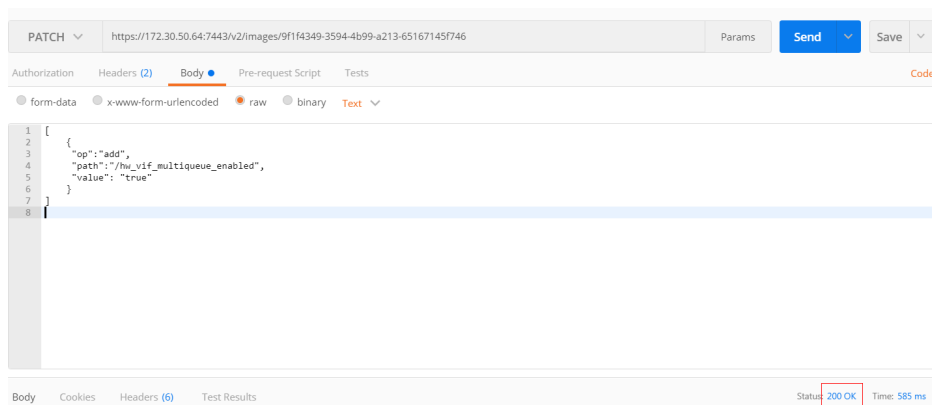
PATCH /v2/images/{image\_id}

请求的body体如下所示。

```
[
 {
 "op": "add",
 "path": "/hw_vif_multiqueue_enabled",
 "value": "true"
 }
]
```

支持网卡多队列修改样例如图6-6所示。

图 6-6 支持网卡多队列修改样例



## 使用私有镜像创建弹性云服务器

使用注册好的私有镜像创建弹性云服务器。在配置参数时，需要注意以下两点：

- 区域：必须选择私有镜像所在的区域。
- 镜像：选择“私有镜像”，并在下拉列表中选择需要的镜像。

## 执行网卡多队列的配置脚本

Windows操作系统使用的半虚拟化驱动pvdriver有一套动态调整网卡队列数的策略，会根据vCPU数计算队列数并进行动态调整，因此无需对windows网卡多队列的队列数进行设置。

Linux操作系统提供了自动开启网卡多队列功能的配置脚本，配置成功后，弹性云服务器支持网卡多队列功能。

### 📖 说明

自动开启网卡多队列功能的配置脚本当前仅支持处理eth0类型的网卡。

1. 登录弹性云服务器，查看网卡支持和已开启的队列数。

### ethtool -l 网卡

示例：

```
[root@localhost ~]# ethtool -l eth0 #查询网卡eth0的队列数
Channel parameters for eth0:
Pre-set maximums:
RX: 0
TX: 0
Other: 0
Combined: 4 #表示此网卡最多支持设置4个队列
Current hardware settings:
RX: 0
TX: 0
Other: 0
Combined: 1 #表示当前已开启的是1个队列
```

如果返回信息中，两个“Combined”字段取值相同，则表示网卡已开启多队列，无需执行以下操作。

2. 执行以下命令，下载配置脚本“multi-queue-hw”。

**wget 下载地址URL**

下载地址：<https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/multi-queue-hw>

3. 执行以下命令，添加执行权限。

**chmod +x multi-queue-hw**

4. 执行以下命令，将脚本“multi-queue-hw”放到目录/etc/init.d下。

**mv multi-queue-hw /etc/init.d**

5. 执行以下命令，运行脚本“multi-queue-hw”。

**/etc/init.d/multi-queue-hw start**

运行脚本后，立即生效。但关机后，网卡多队列功能将自动失效。

6. 为了使网卡多队列功能开机自动生效，各个OS需要增加开机启动配置：

- CentOS/Redhat/Fedora/EulerOS/Suse/OpenSuse使用如下命令，增加开机启动项，使网卡多队列配置开机：

**chkconfig multi-queue-hw on**

- Ubuntu使用如下命令，增加开机启动项：

**update-rc.d multi-queue-hw defaults 90 10**

- Debian使用如下命令，增加开机启动项：

**systemctl enable multi-queue-hw**

## 查看网卡队列数

以Linux系统ECS为例，介绍查看网卡队列数的操作指导。

### 说明

Windows系统ECS的网卡队列数您可以通过调用[查询云服务器网卡信息](#)接口查看。  
通过该接口的响应参数“multiqueue\_num”可获得ECS的网卡队列数。

1. 登录弹性云服务器。
2. 执行以下命令，查看网卡支持和已开启的队列数。

**ethtool -l 网卡**

示例：

```
[root@localhost ~]# ethtool -l eth0 #查询网卡eth0的队列数
Channel parameters for eth0:
Pre-set maximums:
RX: 0
TX: 0
Other: 0
Combined: 4 #表示此网卡最多支持设置开启4个队列
Current hardware settings:
RX: 0
TX: 0
Other: 0
Combined: 4 #表示当前开启的是4个队列
```

## 6.8 开启网卡 IPv6 功能

### 操作场景

IPv4/IPv6双栈网络，支持为ECS提供两个版本的IP地址，包括IPv4地址和IPv6地址。

您可以在购买ECS时，选择支持IPv6的规格和已开启IPv6的主网卡，这样在ECS购买成功后，即可同时拥有IPv4地址和IPv6地址。该场景下的详细操作，请参见[网络](#)。

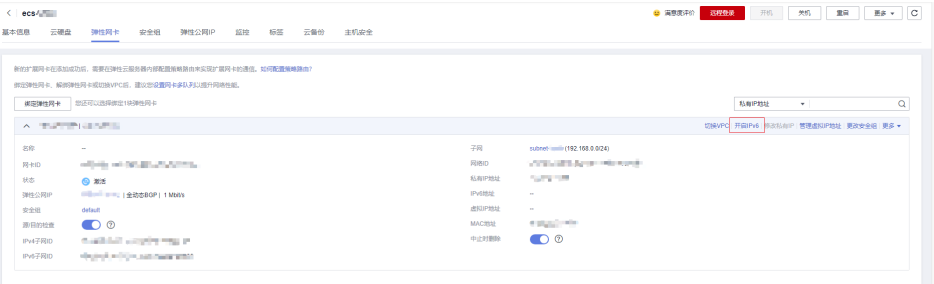
如果购买ECS时未开启IPv6，则ECS不支持在IPv4/IPv6的双栈网络模式下运行，ECS仅拥有IPv4地址。此时，您可以通过“开启IPv6”功能为已创建的ECS开启IPv6功能。

本文介绍如何为已创建ECS开启IPv6功能。

### 约束与限制

- 请确保ECS的规格支持创建后开启IPv6功能。  
当前仅v7及v7以上代系版本的规格支持创建后开启IPv6功能，例如C7、M7等。  
您可以在ECS详情页的“弹性网卡”页签进行查看，如果右上角有“开启IPv6”，则表示支持创建后开启IPv6功能。

图 6-7 开启 IPv6



- 同一个网卡上，只能绑定一个IPv6地址。

### 步骤一：开启子网的 IPv6 网段（可选）

#### 说明

- 云服务器所属子网的IPv6功能开启后会自动分配IPv6网段，开启后不允许关闭。
  - 若在创建子网时已勾选“开启IPv6”，则系统会自动为子网分配IPv6网段，无需执行下面步骤。
- 登录管理控制台，单击[弹性云服务器](#)列表页。

2. 单击待开启IPv6的ECS的名称，进入ECS详情页。
3. 在“基本信息”页签的“网卡”区域，单击子网名称，进入子网详情页。
4. 在子网详情页的“基本信息”页签，单击“开启IPv6”。

图 6-8 开启子网的 IPv6 网段

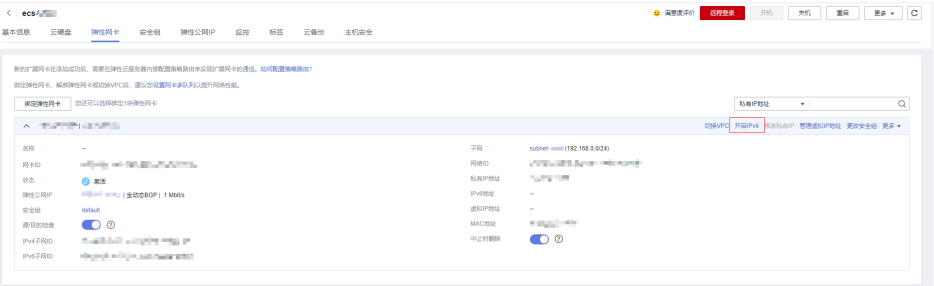


5. 单击“确定”，完成子网IPv6网段的开启。

步骤二：开启 ECS 网卡的 IPv6 功能

1. 单击弹性云服务器列表页。
2. 单击待开启IPv6的ECS的名称，进入ECS详情页。
3. 在“弹性网卡”页签，单击网卡折叠面板右上角的“开启IPv6”。

图 6-9 开启 IPv6



说明

- 仅当云服务器规格支持创建后开启IPv6功能时，显示“开启IPv6/关闭IPv6”。您可以参考[约束与限制](#)判断云服务器规格是否支持创建后开启IPv6。
  - 开启IPv6后，如果云服务器未获取IPv6地址，建议您重启云服务器后重新查看，或参考[动态获取IPv6地址](#)进行配置。
  - 开启IPv6后，如需实现IPv6公网通信，需要创建EIP共享带宽，并将云服务器的IPv6地址添加至共享带宽。详细内容，请参见[通过VPC快速搭建IPv4/IPv6双栈网络](#)。
  - 若不再使用弹性云服务器的IPv6功能，可以在当前页面单击“关闭IPv6”，关闭网卡的IPv6功能，关闭后该网卡的“IPv6地址”为空。
  - 关闭IPv6后，如果重新开启弹性云服务器的IPv6，在重启云服务器后，需要登录弹性云服务器手动清理IPv6缓存，并重新请求获取IPv6地址。

4. 单击“确定”，完成ECS网卡IPv6功能的开启。

## 6.9 动态获取 IPv6 地址

### 操作场景

IPv6的使用，可以有效弥补IPv4网络地址资源有限的问题。如果当前云服务器使用IPv4，那么启用IPv6后，云服务器可在双栈模式下运行，即云服务器可以拥有两个不同版本的IP地址：IPv4地址和IPv6地址，这两个IP地址都可以进行内网/公网访问。

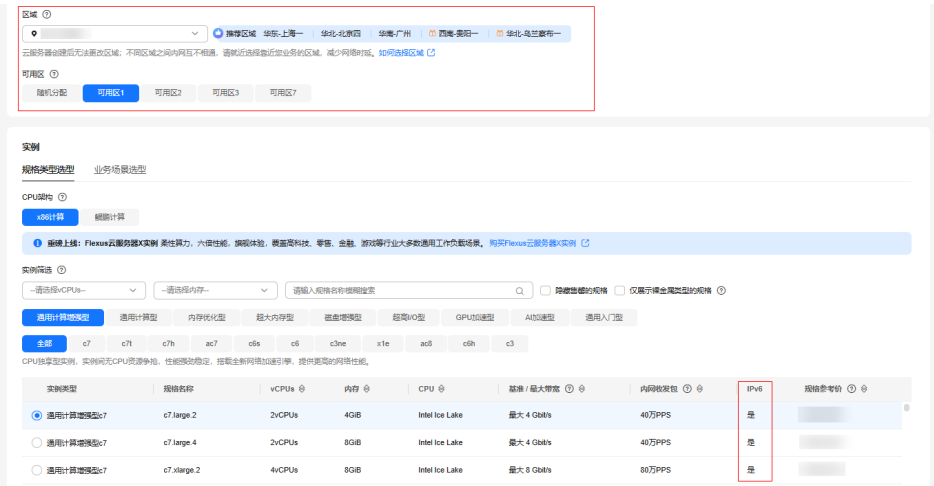
按照[约束与限制](#)中的网络环境要求创建的云服务器，有些不能动态获取到IPv6地址，需要进行相关配置才行。如果云服务器使用的是公共镜像，则支持情况如下：

- Windows公共镜像默认已开启IPv6动态获取功能，无需配置，文中的[Windows 2012操作系统](#)和[Windows 2008操作系统](#)部分供您验证、参考。
- Linux公共镜像开启动态获取IPv6功能时，需要先判断是否支持IPv6协议栈，再判断是否已开启动态获取IPv6。目前，所有Linux公共镜像均已支持IPv6协议栈。

### 约束与限制

- 请确保云服务器所在的子网已开启IPv6功能。  
若云服务器所在子网未开启IPv6功能，需参考[开启网卡IPv6功能](#)进行开启，开启后不允许关闭。
- 请确保云服务器规格支持IPv6功能。  
不同区域、不同可用区支持IPv6双栈的云服务器规格不同。ECS是否支持IPv6双栈，请选择区域、可用区后，以控制台的显示为准，查询方法如下图所示。

图 6-10 查询支持 IPv6 的 ECS 规格



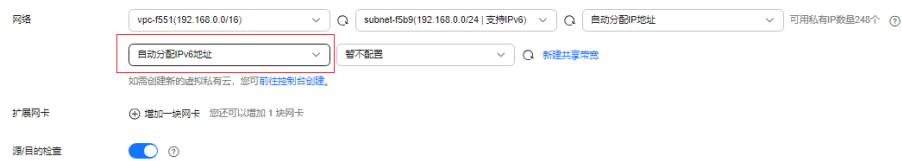
当ECS规格列表中包含“IPv6”参数，且取值为“是”时，表示该ECS规格支持IPv6。

#### 说明

规格是否支持IPv6由“可用区”和“规格”两个参数决定。  
如果设置“可用区”后，规格列表中不显示“IPv6”参数或参数值为“否”，表示当前规格不支持IPv6。

- 请确保创建云服务器时已选择“自动分配IPv6地址”。

图 6-11 选择“自动分配 IPv6 地址”



- 云服务器启动之后动态插拔的网卡不支持IPv6地址动态获取功能。
  - 仅弹性云服务器支持IPv6双栈，裸金属服务器不支持。
  - 同一个网卡上，只能绑定一个IPv6地址。
  - 云服务器网络配置需处于正常状态。
- 检查网络配置是否正常的方法，请参见[检查云服务器网络配置状态](#)。
- 如果网络配置不正常，请[提交工单](#)获取技术支持。

操作导航

- Windows系统：本文以Windows 2012版本、Windows 2008版本为例，介绍Windows操作系统启用IPv6的方法，如[表6-4](#)所示。
  - Linux系统：本文提供了自动配置、手动配置两种方式启用IPv6，推荐您使用自动配置方法，如[表6-4](#)所示。
- 对于CentOS 6.x和Debian操作系统，云服务器内部配置IPv6自动获取功能之后，将该云服务器制作为私有镜像，使用该镜像在非IPv6网络环境中创建云服务器时，由于等待获取IPv6地址超时，导致云服务器启动较慢，此时您可以参考[设置云服务器获取IPv6地址超时时间](#)操作。

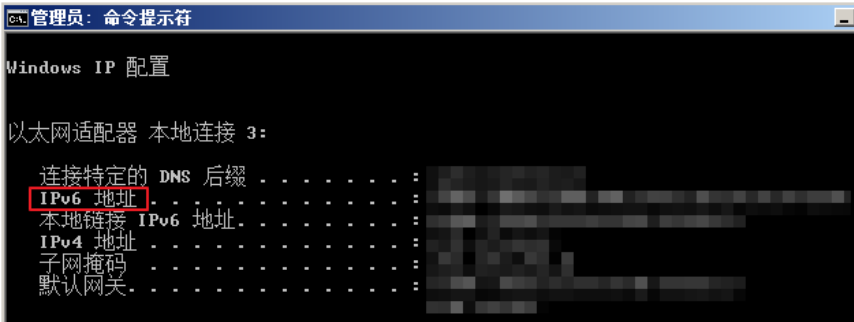
表 6-4 不同操作系统启用 IPv6 操作指导

| 操作系统         | 方式             | 操作指导                                  |
|--------------|----------------|---------------------------------------|
| Windows 2012 | 自动配置启用IPv6     | <a href="#">Windows 2012操作系统</a>      |
| Windows 2008 | 自动配置启用IPv6     | <a href="#">Windows 2008操作系统</a>      |
| Linux        | 自动配置启用IPv6（推荐） | <a href="#">Linux操作系统（自动配置启用IPv6）</a> |
| Linux        | 手动配置启用IPv6     | <a href="#">Linux操作系统（手动配置启用IPv6）</a> |

Windows 2012 操作系统

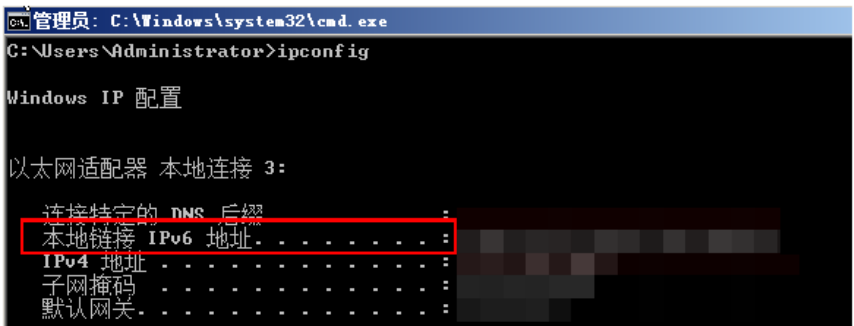
- 步骤1** 检查是否启用IPv6。
- 打开cmd窗口，执行如下命令，查看当前云服务器是否启用IPv6。
- ipconfig**
- 如果已启用IPv6，则会显示IPv6的地址。

图 6-12 显示 IPv6 的地址



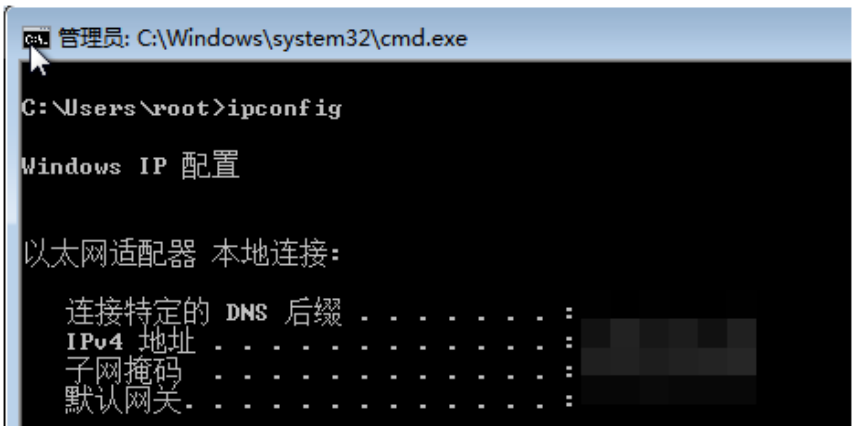
- 如果显示只有本地链接IPv6地址，则表示无法动态获取到IPv6地址。请执行[步骤2](#)。

图 6-13 本地链接 IPv6 地址



- 如果未启用IPv6，则不会显示IPv6的地址。请执行[步骤3](#)。

图 6-14 未启用 IPv6



说明

Windows公共镜像默认已经配置了IPv6动态获取功能，即回显如[图6-12](#)所示，无需特殊配置。

**步骤2** 配置动态获取IPv6。

- 单击“开始 > 控制面板”。
- 单击“网络和共享中心”。



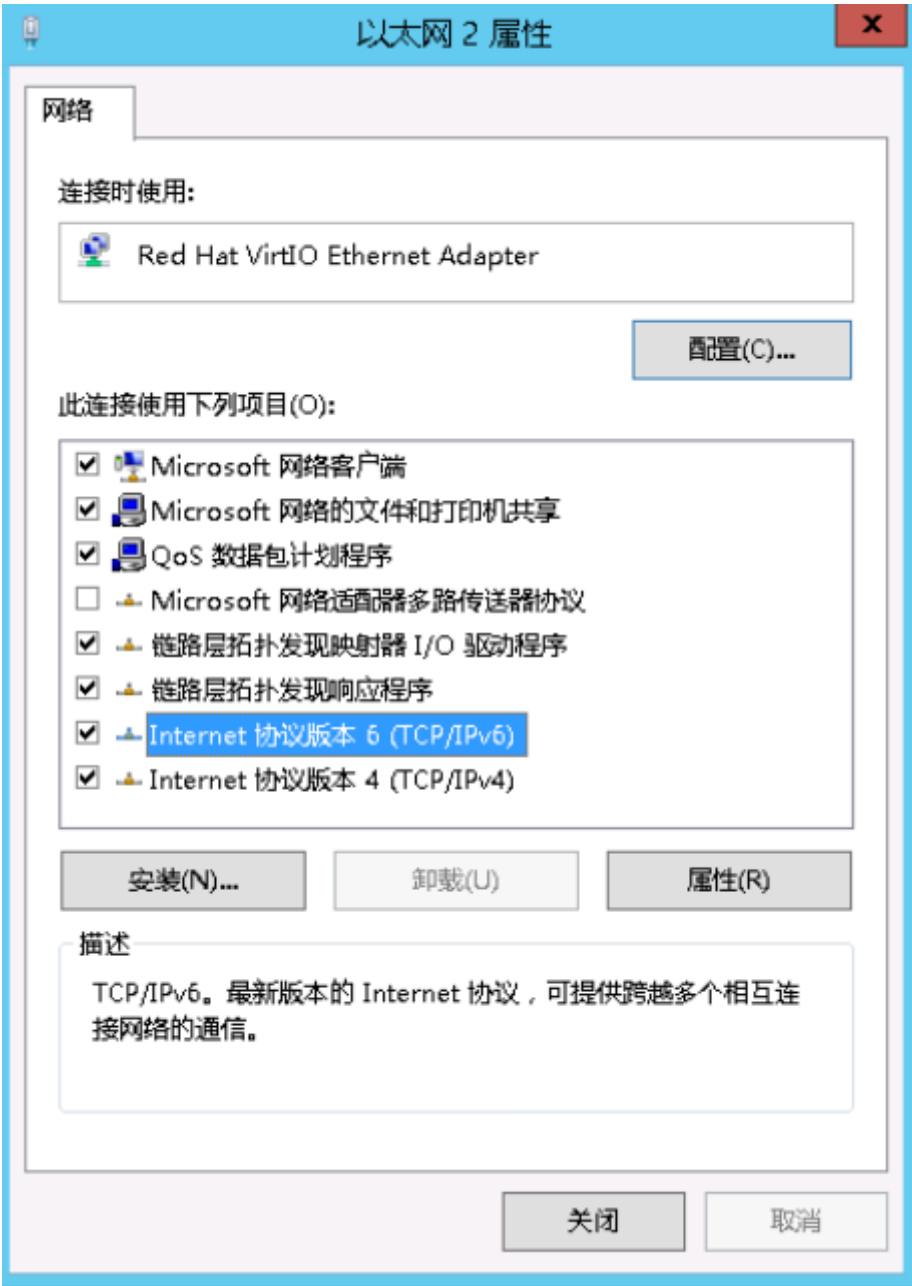
3. 单击以太网连接。

图 6-15 以太网连接



4. 在以太网状态的弹窗中单击左下角的“属性”。
5. 勾选“Internet协议版本 6 (TCP/IPv6)”，然后单击“确定”。

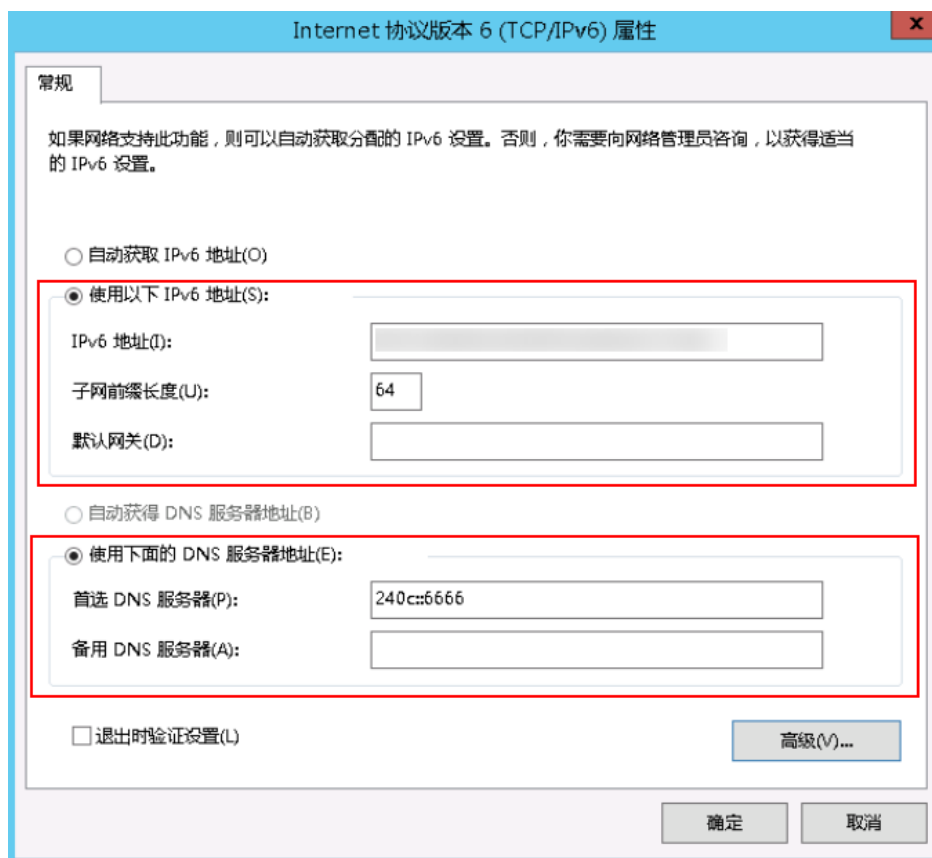
图 6-16 配置动态获取 IPv6



6. 执行**步骤1**检查是否已开启动态获取IPv6。

**步骤3** 启用和配置IPv6。

1. 在“Internet 协议版本 6 (TCP/IPv6) 属性”弹窗中，配置云服务器的IPv6地址和DNS服务器地址。
  - IPv6地址：创建云服务器时分配的IPv6地址，请从控制台云服务器的列表页面获取。
  - 子网前缀长度：64
  - DNS服务器：推荐使用240c::6666

**图 6-17** 在控制台获取 IPv6 地址

2. （可选配置）根据操作系统不同请分别执行以下命令。  
Windows Server 2012操作系统云服务器请在PowerShell或者cmd中执行如下命令：  
**Set-NetIPv6Protocol -RandomizeIdentifiers disabled**
3. 执行**步骤1**检查是否已开启动态获取IPv6。

----结束

## Windows 2008 操作系统

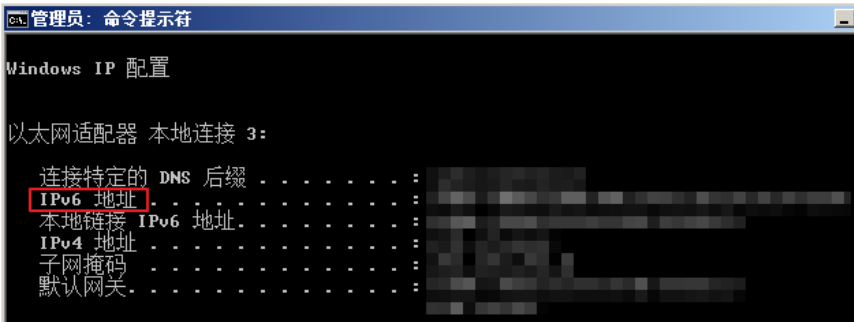
**步骤1** 检查是否启用IPv6。

打开cmd窗口，执行如下命令，查看当前云服务器是否启用IPv6。

**ipconfig**

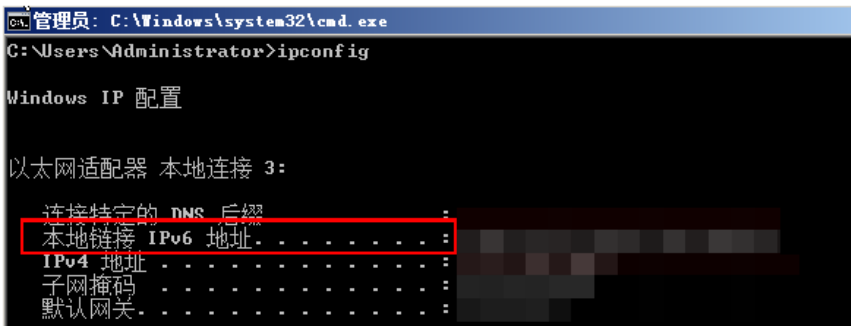
- 如果已启用IPv6，则会显示IPv6的地址。

图 6-18 显示 IPv6 的地址



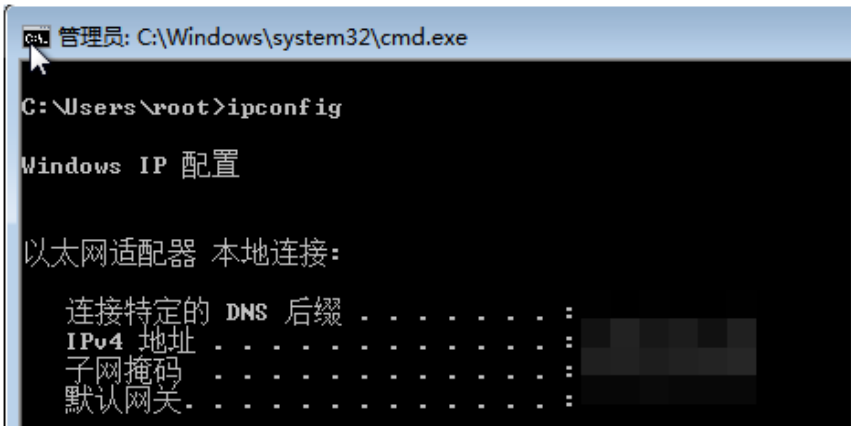
- 如果显示只有本地链接IPv6地址，则表示无法动态获取到IPv6地址。请执行[步骤 2](#)。

图 6-19 本地链接 IPv6 地址



- 如果未启用IPv6，则不会显示IPv6的地址。请执行[步骤3](#)。

图 6-20 未启用 IPv6



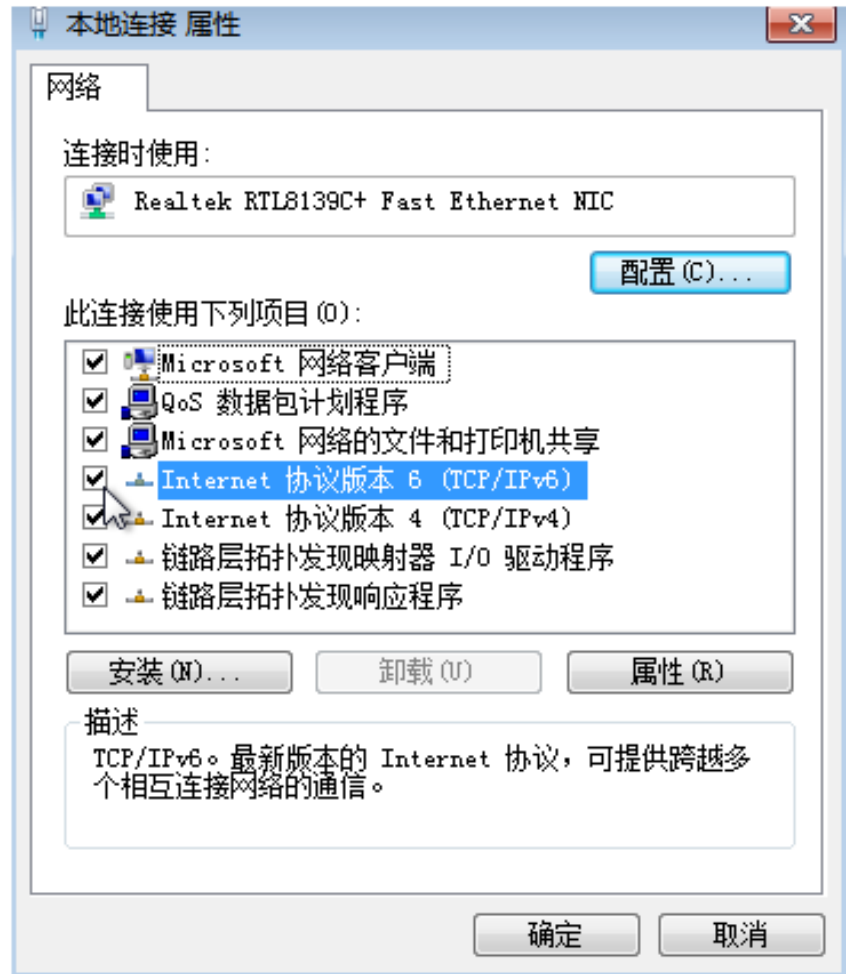
**说明**

Windows公共镜像默认已经配置了IPv6动态获取功能，即回显如[图6-18](#)所示，无需特殊配置。

**步骤2 配置动态获取IPv6。**

1. 单击“开始 > 控制面板”。
2. 单击“网络和共享中心”。
3. 左键单击“更改适配器设置”。
4. 右键单击网络连接并选择“属性”。
5. 勾选“Internet协议版本 6 (TCP/IPv6)”，然后单击“确定”。

图 6-21 配置动态获取 IPv6

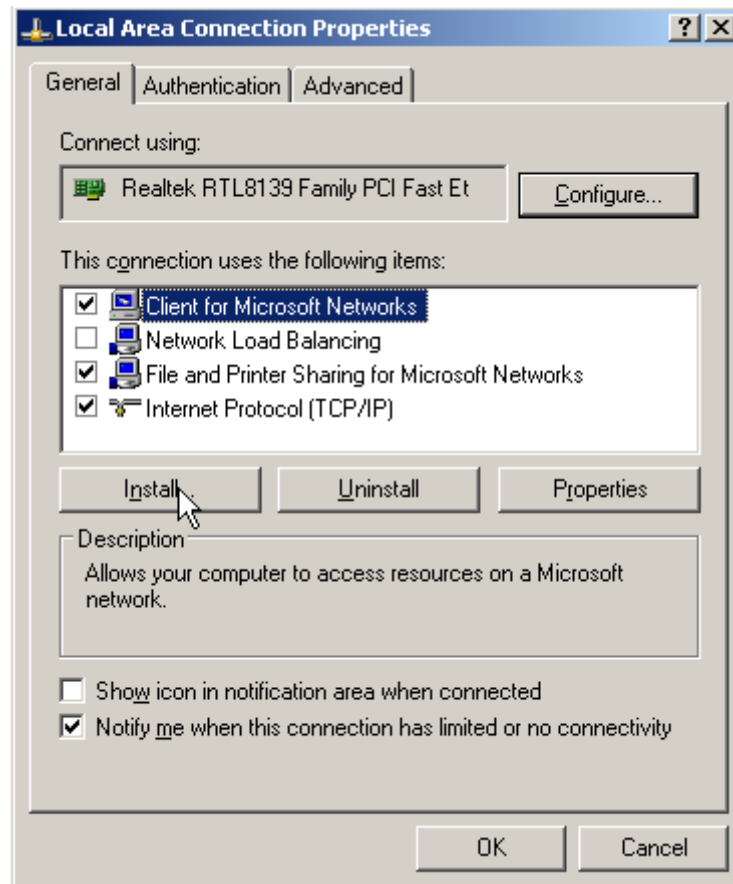


6. 执行[步骤1](#)检查是否已开启动态获取IPv6。

**步骤3** 启用和配置IPv6。

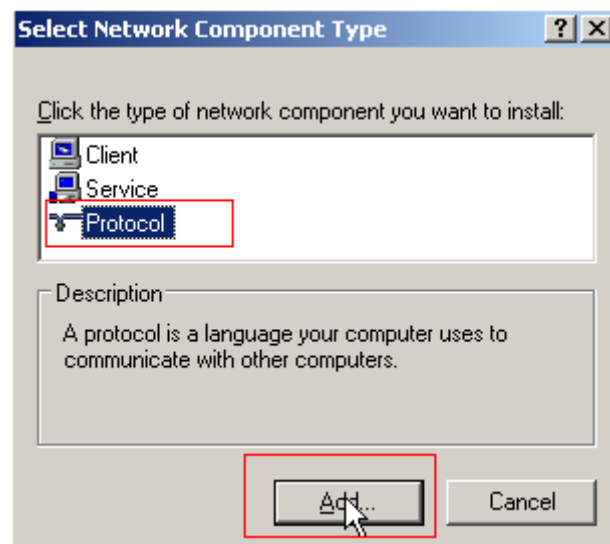
1. 选择“开始 > 控制面板 > 网络连接 > 本地连接”。
2. 选择“属性”，确认勾选以下选项后单击“安装”。

图 6-22 启用和配置 IPv6



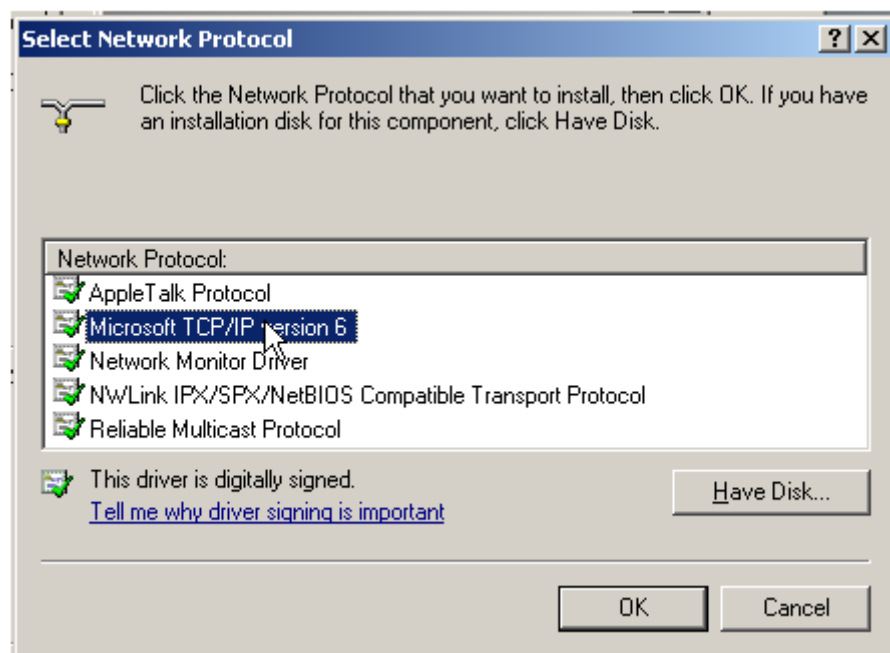
3. 选择“协议”，然后单击“添加”。

图 6-23 添加协议



4. 在网络协议列表中选择“Microsoft TCP/IP版本 6”，然后单击“确定”。

图 6-24 网络协议列表



5. （可选配置）根据操作系统不同请分别执行以下命令。

Windows Server 2008操作系统云服务器请在PowerShell或者cmd中执行如下命令：

**netsh interface ipv6 set global randomizeidentifiers=disable**

设置云服务器先禁用本地连接，再重启本地连接。

禁用本地连接：单击“开始 > 控制面板 > 网络和共享中心 > 更改适配器配置”，选择本地连接，单击右键选择“禁用”。

重启本地连接：单击“开始 > 控制面板 > 网络和共享中心 > 更改适配器配置”，选择本地连接，单击右键选择“启用”。

6. 执行[步骤1](#)检查是否已开启动态获取IPv6。

----结束

## Linux 操作系统（自动配置启用 IPv6）

ipv6-setup-xxx工具能为开启IPv6协议栈的Linux操作系统自动配置动态获取IPv6地址。其中，xxx表示工具系列：rhel或debian。

您也可以参考[Linux操作系统（手动配置启用IPv6）](#)手动配置启用IPv6。

### ⚠ 注意

- ipv6-setup-xxx工具运行时会自动重启网络服务，导致网络短暂不可用。
- CentOS 6.x和Debian操作系统的云服务器内部配置IPv6自动获取功能之后，将该云服务器制作为私有镜像，使用该镜像在非IPv6网络环境中创建云服务器时，由于等待获取IPv6地址超时，导致云服务器启动较慢，您可以参考[设置云服务器获取IPv6地址超时时间](#)设置获取IPv6地址超时时间为30s，然后再重新制作私有镜像。

**步骤1** 执行如下命令，查看当前云服务器是否启用IPv6。

**ip addr**

- 如果没有开启IPv6协议栈，则只能看到IPv4地址，如下图所示，请参考[设置云服务器获取IPv6地址超时时间](#)先开启IPv6协议栈。

**图 6-25** 云服务器未开启 IPv6 协议栈

```
eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
link/ether fa:16:3e: fa:16:3e: brd ff:ff:ff:ff:ff:ff
inet brd scope global noprefixroute dynamic eth0
 valid_lft 1193sec preferred_lft 1193sec
```

- 如果已开启IPv6协议栈，则可以看到LLA地址（fe80开头）。

**图 6-26** 云服务器已开启 IPv6 协议栈

```
eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
link/ether fa:16:3e: fa:16:3e: brd ff:ff:ff:ff:ff:ff
inet brd scope global noprefixroute dynamic eth0
 valid_lft 76391sec preferred_lft 76391sec
inet6 fe80::f816: /64 scope link
 valid_lft forever preferred_lft forever
```

- 如果已开启IPv6协议栈并且已获取到IPv6地址，则会看到如下地址：

**图 6-27** 云服务器已开启 IPv6 协议栈并且已获取到 IPv6 地址

```
eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
link/ether fa:16:3e:75:af:4c brd ff:ff:ff:ff:ff:ff
inet brd scope global noprefixroute dynamic eth0
 valid_lft 86395sec preferred_lft 86395sec
inet6 2407:c080:802: /128 scope global dynamic
 valid_lft 7496sec preferred_lft 7196sec
inet6 fe80::f816:3eff: /64 scope link noprefixroute
 valid_lft forever preferred_lft forever
```

#### 说明

Linux公共镜像均已开启IPv6协议栈，如[图6-26](#)所示；

**步骤2** 开启Linux云服务器IPv6协议栈。

- 执行如下命令，确认内核是否支持IPv6协议栈。

**sysctl -a | grep ipv6**

- 如果有输出信息，表示内核支持IPv6协议栈。
- 如果没有任何输出，说明内核不支持IPv6协议栈，需要执行[2.b](#)加载IPv6模块。

- 执行以下命令，加载IPv6模块。

**modprobe ipv6**

- 修改“/etc/sysctl.conf”配置文件，增加如下配置：

**net.ipv6.conf.all.disable\_ipv6=0**

- 保存配置并退出，然后执行如下命令，加载配置。

**sysctl -p**

**步骤3** 自动配置启用IPv6。

- 下载对应系统版本的工具ipv6-setup-rhel或ipv6-setup-debian，并上传至待操作的云服务器。

ipv6-setup-xxx工具会添加或者修改网卡设备的配置文件，添加IPv6动态获取的配置信息，然后重启网卡或者网络服务。ipv6-setup-rhel和ipv6-setup-debian的工具下载地址如表6-5所示。

表 6-5 工具下载地址

| 系列     | 发行版                                                                                                  | 下载地址                                                                                                                                                                                  |
|--------|------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RHEL   | <ul style="list-style-type: none"><li>CentOS 6/7</li><li>EulerOS 2.2/2.3</li><li>Fedora 25</li></ul> | <a href="https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/ipv6/ipv6-setup-rhel">https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/ipv6/ipv6-setup-rhel</a>     |
| Debian | <ul style="list-style-type: none"><li>Ubuntu 16/18</li><li>Debian 8/9/10</li></ul>                   | <a href="https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/ipv6/ipv6-setup-debian">https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/ipv6/ipv6-setup-debian</a> |

2. 执行以下命令，添加执行权限。  
**chmod +x ipv6-setup-xxx**
3. 执行以下命令，指定一个网卡设备，配置动态获取IPv6地址。  
**./ipv6-setup-xxx --dev [dev]**  
示例：  
**./ipv6-setup-xxx --dev eth0**

#### 说明

- 如需对所有网卡配置动态获取IPv6地址，命令为**./ipv6-setup-xxx**，即不带参数。
- 如需查询工具的用法，请执行命令**./ipv6-setup-xxx --help**。

----结束

## Linux 操作系统（手动配置启用 IPv6）

### 注意

CentOS 6.x和Debian操作系统的云服务器内部配置IPv6自动获取功能之后，将该云服务器制作作为私有镜像，使用该镜像在非IPv6网络环境中创建云服务器时，由于等待获取IPv6地址超时，导致云服务器启动较慢，您可以参考[设置云服务器获取IPv6地址超时时间](#)设置获取IPv6地址超时时间为30s，然后再重新制作私有镜像。

**步骤1** 执行如下命令，查看当前云服务器是否启用IPv6。

**ip addr**

- 如果没有开启IPv6协议栈，则只能看到IPv4地址，如下图所示，请参考[步骤2](#)先开启IPv6协议栈。

图 6-28 未开启 IPv6 协议栈

```
eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
 link/ether fa:16:3e:xxxx:xx:xx brd ff:ff:ff:ff:ff:ff
 inet xxx.xxx.xxx.xxx brd xxx.xxx.xxx.xxx scope global noprefixroute dynamic eth0
 valid_lft 1193sec preferred_lft 1193sec
```



- 如果已开启IPv6协议栈，则可以看到LLA地址（fe80开头）。

图 6-29 已开启 IPv6 协议栈

```
eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
link/ether fa:16:3e:75:af:4c brd ff:ff:ff:ff:ff:ff
inet 10.0.0.1 brd 10.0.0.255 scope global noprefixroute dynamic eth0
 valid_lft 76391sec preferred_lft 76391sec
inet6 fe80::f816:3eff:fe00:0000/64 scope link
 valid_lft forever preferred_lft forever
```

- 如果已开启IPv6协议栈并且已获取到IPv6地址，则会看到如下地址：

图 6-30 已开启 IPv6 协议栈并且已获取到 IPv6 地址

```
eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
link/ether fa:16:3e:75:af:4c brd ff:ff:ff:ff:ff:ff
inet 10.0.0.1 brd 10.0.0.255 scope global noprefixroute dynamic eth0
 valid_lft 86395sec preferred_lft 86395sec
inet6 2407:c080:802::1/128 scope global dynamic
 valid_lft 7496sec preferred_lft 7196sec
inet6 fe80::f816:3eff:fe00:0000/64 scope link noprefixroute
 valid_lft forever preferred_lft forever
```

#### 说明

Linux公共镜像均已开启IPv6协议栈，如图6-29所示；

#### 步骤2 开启Linux云服务器IPv6协议栈。

- 执行如下命令，确认内核是否支持IPv6协议栈。  
**sysctl -a | grep ipv6**
  - 如果有输出信息，表示内核支持IPv6协议栈。
  - 如果没有任何输出，说明内核不支持IPv6协议栈，需要执行[步骤2.2](#)加载IPv6模块。
- 执行以下命令，加载IPv6模块。  
**modprobe ipv6**
- 修改“/etc/sysctl.conf”配置文件，增加如下配置：  
**net.ipv6.conf.all.disable\_ipv6=0**
- 保存配置并退出，然后执行如下命令，加载配置。  
**sysctl -p**

#### 步骤3 手动配置启用IPv6。操作系统不同，步骤有所差别。

- Ubuntu 18.04/20.04操作系统云服务器配置动态获取IPv6。
  - 执行以下命令，进入“/etc/netplan/”。**cd /etc/netplan**
  - 执行以下命令，查询配置文件名。  
**ls**

图 6-31 查询配置文件名

```
root@ecs-: /etc/netplan# ls
01-netcfg.yaml 01-network-manager-all.yaml
```

- 执行以下命令，编辑“01-network-manager-all.yaml”配置文件。  
**vi 01-network-manager-all.yaml**

- d. 在“01-network-manager-all.yaml”下增加如下内容，注意yaml文件格式及缩进：

```
ethernets:
 eth0:
 dhcp6: true
```

图 6-32 修改结果

```
Let NetworkManager manage all devices on this system
network:
 version: 2
 renderer: NetworkManager
 ethernets:
 eth0:
 dhcp6: true
```

修改完成后保存退出。

- e. 执行以下命令，使更改生效。

**sudo netplan apply**

- Ubuntu 22.04操作系统云服务器配置动态获取IPv6。

- a. 执行以下命令，进入“/etc/netplan/”。

**cd /etc/netplan**

- b. 执行以下命令，查询配置文件名。

**ls**

图 6-33 查询配置文件名

```
root@ecs-485b:/etc/netplan# ls
01-netcfg.yaml
```

- c. 执行以下命令，编辑“01-netcfg.yaml”配置文件。

**vi 01-netcfg.yaml**

- d. 在“01-netcfg.yaml”中增加如下内容，注意yaml文件格式及缩进：

```
ethernets:
 eth0:
 dhcp6: true
```

图 6-34 修改结果

```
network:
 version: 2
 renderer: NetworkManager
 ethernets:
 eth0:
 dhcp4: true
 dhcp6: true
 eth1:
 dhcp4: true
 eth2:
 dhcp4: true
 eth3:
 dhcp4: true
 eth4:
 dhcp4: true
```

修改完成后保存退出。

- e. 执行以下命令，使更改生效。

```
sudo netplan apply
```

- f. 执行以下命令，编辑“/etc/NetworkManager/NetworkManager.conf”文件。

```
vi /etc/NetworkManager/NetworkManager.conf
```

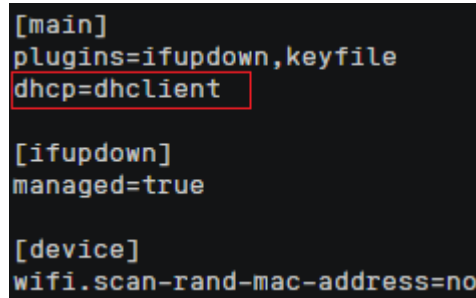
- g. 在“NetworkManager.conf”中增加如下内容，注意文件格式及缩进：

```
[main]
plugins=ifupdown,keyfile
dhcp=dhclient

[ifupdown]
managed=true

[device]
wifi.scan-rand-mac-address=no
```

图 6-35 修改结果



```
[main]
plugins=ifupdown,keyfile
dhcp=dhclient

[ifupdown]
managed=true

[device]
wifi.scan-rand-mac-address=no
```

- h. 执行以下命令，使配置生效。

```
systemctl restart NetworkManager
```

- Debian操作系统云服务器配置动态获取IPv6。

- a. 编辑“/etc/network/interfaces”文件，使之包含以下内容：

```
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet dhcp
iface eth0 inet6 dhcp
pre-up sleep 3
```

- b. 如果有多个网卡，则在“/etc/network/interfaces”文件中，增加对应网卡的配置，以eth1为例，需要增加：

```
auto eth1
iface eth1 inet dhcp
iface eth1 inet6 dhcp
pre-up sleep 3
```

- c. 执行如下命令重启网络服务。

```
service networking restart
```

#### 说明

如果将网卡进行down/up操作之后无法获取IPv6地址，也可以通过此命令重启网络服务。

- d. 执行步骤[步骤1](#)检查是否已开启动态IPv6。

- CentOS/EulerOS/Fedora操作系统云服务器配置动态获取IPv6。

- a. 编辑主网卡配置文件“/etc/sysconfig/network-scripts/ifcfg-eth0”。

补充如下配置项：

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

- b. 编辑“/etc/sysconfig/network”，按如下所示添加或修改以下行。

```
NETWORKING_IPV6=yes
```

- c. CentOS 6系列从网卡需要编辑对应的配置文件，以eth1为例，编辑“/etc/sysconfig/network-scripts/ifcfg-eth1”。

补充如下配置项：

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

CentOS 6.3系统中默认ip6tables会过滤dhcpv6-client请求，所以CentOS 6.3除了需要编辑“ifcfg-eth\*”文件外，还需要额外添加一条允许dhcpv6-client请求的ip6tables规则。操作如下：

- i. 执行以下命令，添加ip6tables规则。

```
ip6tables -A INPUT -m state --state NEW -m udp -p udp --dport 546 -d fe80::/64 -j ACCEPT
```

- ii. 执行以下命令，保存ip6tables规则。

```
service ip6tables save
```

图 6-36 命令示例

```
[root@ecs-cd02 log]# ip6tables -A INPUT -m state --state NEW -m udp -p udp --dport 546 -d fe80::/64 -j ACCEPT
nf_conntrack version 0.5.0 (7964 buckets, 31856 max)
[root@ecs-cd02 log]# service ip6tables save
ip6tables: Saving firewall rules to /etc/sysconfig/ip6tablef OK]
```

- d. （可选配置）CentOS 7/CentOS 8系列需要将扩展网卡的IPv6 LLA地址模式修改为EUI64。

- i. 执行如下命令查看网卡信息。

```
nmcli con
```

图 6-37 查看网卡信息

```
[root@ecs-166b ~]# nmcli con
NAME UUID TYPE DEVICE
System eth0 5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03 ethernet eth0
Wired connection 1 9c92fad9-6ecb-3e6c-eb4d-8a47c6f50c04 ethernet eth1
Wired connection 1 3a73717e-65ab-93e8-b518-24f5af32dc0d ethernet eth2
```

- ii. 将eth1的IPv6 LLA地址模式按以下命令修改为EUI64：

```
nmcli con modify "Wired connection 1" ipv6.addr-gen-mode eui64
```

#### 说明

CentOS不同系列，网卡信息存在差异，命令中的“Wired connection 1”需要根据实际查询的网卡信息的“NAME”列进行替换。

- iii. 通过ifconfig命令将eth1进行down/up操作。

```
ifdown eth1
```

```
ifup eth1
```

- e. 重启网络服务。

- i. CentOS 6系列执行以下命令，重启网络服务。

```
service network restart
```

- ii. CentOS 7/EulerOS/Fedora系列执行以下命令，重启网络服务。  
**systemctl restart NetworkManager**
- f. 执行步骤**步骤1**检查是否已开启动态IPv6。
- SUSE/openSUSE/CoreOS操作系统云服务器配置动态获取IPv6。  
SUSE 11 SP4不支持IPv6自动获取。  
SUSE 12 SP1、SUSE 12 SP2无需特殊配置。  
openSUSE 13.2、openSUSE 42.2无需特殊配置。  
CoreOS 10.10.5无需特殊配置。

----结束

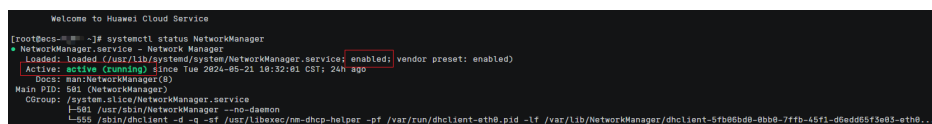
## 检查云服务器网络配置状态

1. 执行以下命令，检查云服务器网络服务状态是否正常。

**systemctl status NetworkManager**

如果网络服务状态正常，则执行结果中服务处于active (running)状态且是enable的。

图 6-38 网络服务器状态



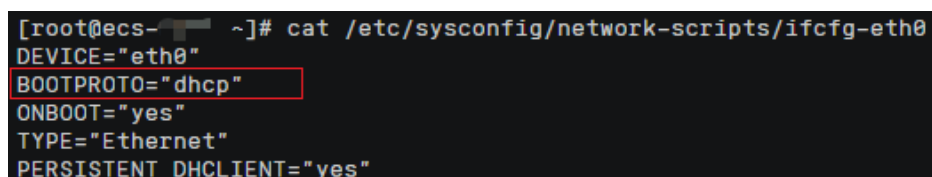
2. 执行以下命令，检查云服务器网卡获取IP地址的方式。

**cat /etc/sysconfig/network-scripts/ifcfg-ethx**

### 说明

- “ethx”需替换为具体的网卡，例如eth0。
- 该命令以CentOS 7为例进行介绍。

图 6-39 网卡获取 IP 地址的方式



- 如果BOOTPROTO字段的值为dhcp：表示云服务器网卡通过动态DHCP获取IP地址，继续执行**3**。
  - 如果BOOTPROTO字段的值为static：表示云服务器网卡通过静态配置的方式设置网络，继续执行**4**。
3. 如果云服务器网卡通过动态DHCP获取IP地址，则需要执行以下命令，确认DHCP相关进程是否正常。

**systemctl status NetworkManager**

回显中包含相关网卡的dhclient进程则代表正常。

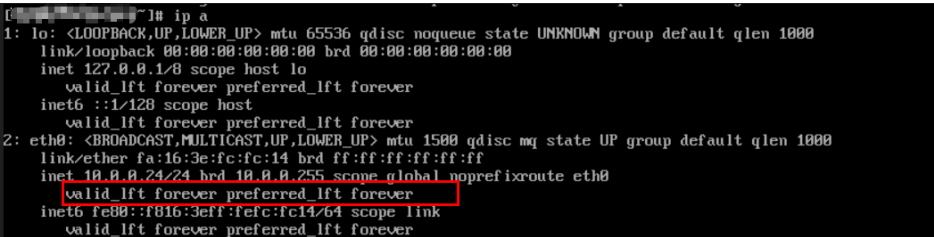
图 6-40 检查 DHCP 进程



4. 如果云服务器网卡通过静态配置的方式设置网络，则需要执行以下命令，确认IP地址配置是否生效。

**ip a**  
回显中IP配置字段是forever则代表配置已经生效。

图 6-41 检查静态配置



设置云服务器获取 IPv6 地址超时时间

CentOS 6.x和Debian操作系统的云服务器内部配置IPv6自动获取功能之后，将该云服务器制作为私有镜像，使用该镜像在非IPv6网络环境中创建云服务器时，由于等待获取IPv6地址超时，导致云服务器启动较慢，您可以参考本节操作设置获取IPv6地址超时时间为30s，然后再重新制作私有镜像。

- CentOS 6.x:
  - a. 执行以下命令编辑“dhclient.conf”文件。  
**vi /etc/dhcp/dhclient.conf**
  - b. 按“i”进入编辑模式，在文件中增加timeout属性。  
timeout 30;
  - c. 输入:wq保存后退出。
- Debian 7.5:
  - a. 执行以下命令编辑“networking”文件。  
**vi /etc/init.d/networking**
  - b. 按“i”进入编辑模式，增加延迟命令timeout，修改点如下图所示。

图 6-42 修改点 1

```
115 case "$1" in
116 start)
117 if init_is_upstart; then
118 exit 1
119 fi
120 process_options
121 check_ifstate
122
123 if ["$CONFIGURE_INTERFACES" = no]
124 then
125 log_action_begin_msg "Not configuring network interfaces, see /etc/default/networking"
126 exit 0
127 fi
128 set -f
129 exclusions=$(process_exclusions)
130 log_action_begin_msg "Configuring network interfaces"
131 if /usr/bin/timeout 30 ifup -a $exclusions $verbose && ifup_hotplug $exclusions $verbose
132 then
133 log_action_end_msg $?
134 else
135 log_action_end_msg $?
136 fi
137 ;;
138
139 stop)
140 if init_is_upstart; then
141 exit 0
142 fi
143 check_network_file_systems
144 check_network_swap
145
146 log_action_begin_msg "Deconfiguring network interfaces"
147 if /usr/bin/timeout 30 ifdown -a --exclude=lo $verbose; then
148 log_action_end_msg $?
```

图 6-43 修改点 2

```
154 reload)
155 process_options
156
157 log_action_begin_msg "Reloading network interfaces configuration"
158 state=$(cat /run/network/ifstate)
159 if /usr/bin/timeout 30 ifdown -a --exclude=lo $verbose || true
160 if /usr/bin/timeout 30 ifup --exclude=lo $state $verbose ; then
161 log_action_end_msg $?
162 else
163 log_action_end_msg $?
164 fi
165 ;;
166
167 force-reload|restart)
168 if init_is_upstart; then
169 exit 1
170 fi
171 process_options
172
173 log_warning_msg "Running $0 $1 is deprecated because it may not re-enable some interfaces"
174 log_action_begin_msg "Reconfiguring network interfaces"
175 if /usr/bin/timeout 30 ifdown -a --exclude=lo $verbose || true
176 set -f
177 exclusions=$(process_exclusions)
178 if /usr/bin/timeout 30 ifup -a --exclude=lo $exclusions $verbose && ifup_hotplug $exclusions $verbose
179 then
180 log_action_end_msg $?
181 else
182 log_action_end_msg $?
```

- Debian 8.2.0/8.8.0
  - a. 执行以下命令编辑“network-pre.conf”文件。  
**vi /lib/systemd/system/networking.service.d/network-pre.conf**
  - b. 按“i”进入编辑模式，在文件中增加timeout属性。  
[Service]  
TimeoutStartSec=30
- Debian 9.0
  - a. 执行以下命令编辑“networking.service”文件。  
**vi /etc/systemd/system/network-online.target.wants/networking.service**
  - b. 按“i”进入编辑模式，将TimeoutStartSec=5min改为  
TimeoutStartSec=30。

## 6.10 委托授权云运维中心访问 ECS

### 操作场景

批量切换VPC操作需要使用云运维中心COC的作业管理功能，在使用前需要创建委托以授权云运维中心访问ECS，同时授权该委托ECS的相关操作权限。

当您需要批量为多台ECS切换VPC时，可参考本节创建委托。

### 操作步骤

1. 登录[IAM控制台](#)。
2. 在统一身份认证服务的左侧导航窗格中，选择“委托”页签，单击“创建委托”。
3. 在创建委托页面，设置委托相关参数。
  - 委托名称：设置委托名称。
  - 委托类型：选择“云服务”。
  - 云服务：选择需要授权的云服务，如“云运维中心”。
  - 持续时间：根据业务需要设置。
  - （可选）描述：填写“委托描述”。

图 6-44 创建委托

委托 / 创建委托

\* 委托名称

\* 委托类型 ☐ 普通账号  
将账号内资源的操作权限委托给其他华为云账号。  
☒ 云服务  
将账号内资源的操作权限委托给华为云服务。

\* 云服务

\* 持续时间

描述

0/255

完成 取消



4. 单击“完成”。
5. 在授权的确认弹窗中，单击“立即授权”。
6. 勾选需要授予委托的权限。

若列表中无可用策略，可单击列表右上角的“新建策略”进行创建。详细操作步骤，请参见[创建自定义策略](#)。

自定义策略需包含如下内容：

```
{
 "Version": "1.1",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "ecs:cloudServers:changeVpc",
 "ecs:cloudServers:list"
]
 }
]
}
```

7. 单击“下一步”，选择权限的作用范围，给委托授权。
8. 单击“确定”，委托创建完成。

# 7 弹性公网 IP 管理

---

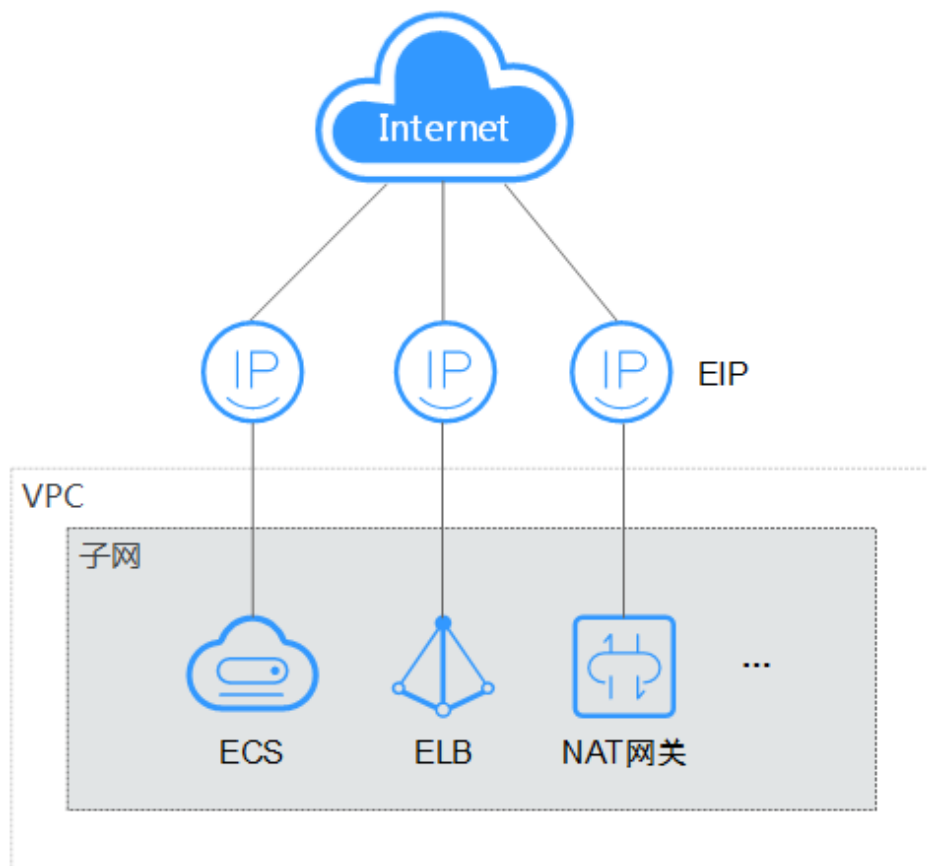
## 7.1 弹性公网 IP 概述

### 弹性公网 IP

弹性公网IP（Elastic IP，简称EIP）提供独立的公网IP资源，包括公网IP地址与公网出口带宽服务。可以与弹性云服务器、裸金属服务器、虚拟IP、弹性负载均衡、NAT网关等资源灵活地绑定及解绑。拥有多种灵活的计费方式，可以满足各种业务场景的需要。

一个弹性公网IP只能绑定一个云资源使用。

图 7-1 通过 EIP 访问公网



## 相关链接

- [绑定弹性公网IP](#)
- [解绑弹性公网IP](#)
- [修改弹性公网IP的带宽](#)
- [弹性公网IP类常见问题](#)
- [访问网站或应用故障类常见问题](#)

## 7.2 绑定弹性公网 IP

### 操作场景

可以通过申请弹性公网IP并将弹性公网IP绑定到弹性云服务器上，实现弹性云服务器访问公网的目的。

申请弹性公网IP请参考[为弹性云服务器申请和绑定弹性公网IP](#)。

### 操作步骤

1. 登录管理控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。

3. 单击“”，选择“计算 > 弹性云服务器”。
4. 在弹性云服务器列表中，找到待绑定弹性公网IP的弹性云服务器，单击“操作”列下的“更多 > 网络/安全组 > 绑定弹性公网IP”。
5. 选择弹性公网IP。

 说明

如果当前区域没有可用的弹性公网IP，则弹性公网IP列表为空，请购买弹性公网IP后重新执行绑定操作。

图 7-2 绑定弹性公网 IP



6. 设置“释放行为”。
- 对于勾选了“随实例释放”的弹性公网IP，将在删除云服务器同时执行删除。
7. 单击“确定”。
- 完成绑定后，可以在云服务器列表页查看已绑定的弹性公网IP。

相关操作

- Windows云服务器访问公网不通应如何处理？

7.3 解绑弹性公网 IP

操作场景

本节操作介绍从云服务器解绑弹性公网IP的操作步骤。

 **注意**

解绑弹性公网IP会导致弹性云服务器实例无法访问公网，在解绑前请确保不再需要访问公网或者有替代的网络连接方式。

操作步骤

1. 登录管理控制台。

2. 单击管理控制台左上角的 ，选择区域和项目。
3. 单击 “”，选择“计算 > 弹性云服务器”。
4. 在弹性云服务器列表中，在待调整带宽的弹性云服务器操作列下，单击“操作”列下的“网络/安全组 > 解绑弹性公网IP”。
5. 确认弹性公网IP信息，单击“确定”。

#### 说明

未绑定弹性云服务器的弹性公网IP会继续计费，如果不再使用请根据控制台的引导释放弹性公网IP。

详细操作，请参见[释放/退订弹性公网IP](#)。

## 7.4 更换弹性公网 IP

### 操作场景

如果您的弹性云服务器绑定了弹性公网IP，您可以参考本节操作更换弹性公网IP。

暂不支持直接更换弹性云服务器的弹性公网IP。您需要先解绑当前的弹性公网IP，再重新为弹性云服务器绑定新的弹性公网IP。

如果无可更换的弹性公网IP，您需要先申请新的弹性公网IP，再进行更换操作。

#### 注意

更换弹性公网IP前，请谨慎评估该操作可能带来的业务影响，避免由于误操作造成网络中断。

### 约束限制

为防止误删除操作，弹性公网IP存在24小时缓存机制，对于已释放过弹性公网IP的用户，24小时内会优先分配之前使用过的弹性公网IP。

如需申请新的弹性公网IP地址，建议您先购买新的弹性公网IP后再释放旧的弹性公网IP。

详细内容请参考[弹性公网IP的分配策略](#)。

### 前提条件

已购买新的弹性公网IP。

详细内容，请参见[申请弹性公网IP](#)。

### 解绑弹性公网 IP

1. 登录管理控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。

3. 选择指定云服务器，单击“操作”列下的“更多 > 网络/安全组 > 解绑弹性公网 IP”。
4. 确认弹性公网IP信息，解绑EIP。

 说明

未绑定弹性云服务器的弹性公网IP会继续计费，如果不再使用请根据控制台的引导释放弹性公网IP。

绑定新的弹性公网 IP

1. 登录管理控制台。
2. 单击管理控制台左上角的，选择区域和项目。
3. 选择指定云服务器，单击“操作”列下的“更多 > 网络/安全组 > 绑定弹性公网 IP”。
4. 选择弹性公网IP，单击“确定”完成新的弹性公网IP的绑定。

 说明

如果当前区域没有可用的弹性公网IP，则弹性公网IP列表为空，请购买弹性公网IP后重新执行绑定操作。

图 7-3 绑定新的弹性公网 IP



相关操作

- Windows云服务器访问公网不通应如何处理？

7.5 修改弹性公网 IP 的带宽

操作场景

弹性公网IP的带宽可以为弹性云服务器提供公网和弹性云服务器间的访问流量。如果当前弹性公网IP的带宽不满足您的业务需要，可以参考本节操作调整弹性云服务器带宽。

## 约束与限制

降低带宽大小，可能会影响业务流量造成丢包，请确认对业务产生的影响，谨慎操作。

## 前提条件

弹性云服务器已绑定弹性公网IP，详细操作，请参见[绑定弹性公网IP](#)。

## 操作步骤

1. 登录管理控制台。
2. 单击管理控制台左上角的，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”。
4. 在弹性云服务器列表中，在待调整带宽的弹性云服务器操作列下，单击“操作”列下的“更多 > 网络/安全组 > 修改带宽”。
5. 根据页面提示，修改“带宽名称”、“计费方式”和“带宽大小”。

## 相关操作

- [Windows云服务器访问公网不通应如何处理？](#)

# 7.6 无公网 IP 的弹性云服务器访问 Internet

## 操作场景

为保证安全和节省公网IP资源，通常只为特定的弹性云服务器配置公网IP，可直接访问Internet，其他弹性云服务器只配置私网IP，无法直接访问Internet。

因此，当只配置了私网IP的弹性云服务器需要访问Internet，执行软件升级、给系统打补丁或者其他需求时，可选择以下方案：

- **（推荐）通过NAT（NAT Gateway）网关服务**  
NAT网关能够为VPC内的弹性云服务器提供SNAT和DNAT功能，通过灵活简易的配置，即可轻松构建VPC的公网出入口，实现多个弹性云服务器共享弹性公网IP访问Internet或使弹性云服务器对互联网提供服务。
- **通过Linux操作系统的代理主机**  
如果您已拥有一台绑定了EIP的弹性云服务器，可将该弹性云服务器作为代理，为同一网段且同一安全组内的其他无公网IP的云服务器提供访问通道，正常访问Internet。

## （推荐）通过 NAT（NAT Gateway）网关服务

### 说明

本方案需要：

- 已购买弹性公网IP和公网NAT网关。
- 公网NAT网关和其他需要访问Internet的弹性云服务器处于同一VPC内。

表 7-1 NAT 网关操作指引

| 操作场景                    | 网关规则 | 相关链接                                     |
|-------------------------|------|------------------------------------------|
| 无公网IP的弹性云服务器访问 Internet | SNAT | <a href="#">通过公网NAT网关的SNAT规则访问公网</a>     |
| 无公网IP的弹性云服务器对互联网提供服务    | DNAT | <a href="#">通过公网NAT网关的DNAT规则面向公网提供服务</a> |

通过 Linux 操作系统的代理主机

说明

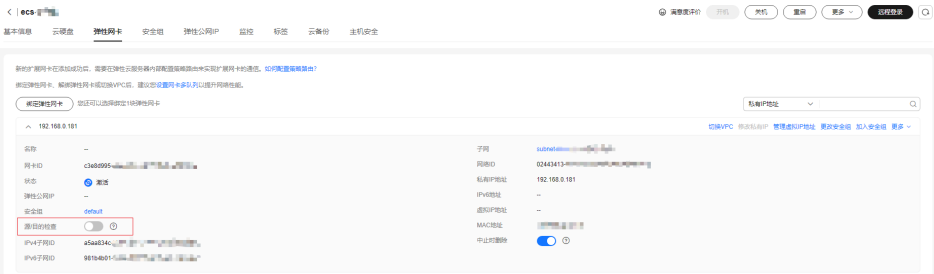
- 本方案需要：
- 已拥有一台绑定了公网IP的弹性云服务器作为代理弹性云服务器。
  - 代理弹性云服务器和其他需要访问Internet的弹性云服务器均处于同一网段，并且在同一安全组内。

本节操作中，以代理弹性云服务器的操作系统是CentOS 7.9为例进行介绍，适用于CentOS 7.9及以下版本、Huawei Cloud EulerOS 2.0版本。

其他操作系统及版本，请您参考对应官网帮助文档进行配置，或采用（推荐）通过[NAT（NAT Gateway）网关服务](#)。

1. 登录管理控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”。
4. 在弹性云服务器列表中的右上角，输入代理云服务器名称进行搜索。
5. 单击代理弹性云服务器的名称，查看详情。
6. 在代理弹性云服务器详情页面，选择“弹性网卡”页签，并展开 ，将“源/目的检查”选项设置为“OFF”。

图 7-4 关闭“源/目的检查”



默认情况下，“源/目的检查”状态为“启用”，系统会检查弹性云服务器发送的报文中源IP地址是否正确，否则不允许弹性云服务器发送该报文。这有助于防止伪装报文攻击，提升安全性。但在该场景中，这种保护机制会导致报文的发送者无法接收到返回的报文。因此，需设置“源/目的检查”状态为禁用。



7. 登录代理弹性云服务器。  
详细操作方法请参见[Linux ECS登录方式概述](#)。
8. 执行以下命令，检测代理弹性云服务器是否可以正常连接Internet。  
**ping www.huaweicloud.com**  
回显包含类似如下信息时，表示代理弹性云服务器可正常连接Internet。

图 7-5 检测是否可以正常连接 Internet

```
[root@ecs-f4f0 ~]# ping www.baidu.com
PING www.a.shifen.com (61.135.169.121) 56(84) bytes of data:
64 bytes from 61.135.169.121 (61.135.169.121): icmp_seq=1 ttl=47 time=2.77 ms
64 bytes from 61.135.169.121 (61.135.169.121): icmp_seq=2 ttl=47 time=2.65 ms
64 bytes from 61.135.169.121 (61.135.169.121): icmp_seq=3 ttl=47 time=2.61 ms
64 bytes from 61.135.169.121 (61.135.169.121): icmp_seq=4 ttl=47 time=2.83 ms
64 bytes from 61.135.169.121 (61.135.169.121): icmp_seq=5 ttl=47 time=2.69 ms
64 bytes from 61.135.169.121 (61.135.169.121): icmp_seq=6 ttl=47 time=2.63 ms
```

9. （可选）执行以下命令，安装iptables服务并配置iptables服务开机自启动。  
仅CentOS 7.x版本的弹性云服务器，需要执行此步骤。

```
yum install iptables-services -y
systemctl start iptables
systemctl enable iptables
```

10. 执行以下命令，查看代理弹性云服务器的IP转发功能是否开启。

```
cat /proc/sys/net/ipv4/ip_forward
```

- 回显为“0”表示关闭，请执行11。
- 回显为“1”表示开启，请执行16。

11. 执行以下命令，打开IP转发功能配置文件。

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

12. 按“i”，进入编辑模式。

13. 修改如下参数的值。

将参数“net.ipv4.ip\_forward”的值修改为“1”。

#### 说明

如果“sysctl.conf”文件中不存在参数“net.ipv4.ip\_forward”，执行以下命令进行添加：

```
echo net.ipv4.ip_forward=1 >> /etc/sysctl.conf
```

14. 按“Esc”，输入:wq，按“Enter”。

保存设置并退出vi编辑器。

15. 执行以下命令，使配置文件修改生效。

```
sysctl -p /etc/sysctl.conf
```

16. 执行以下命令，清除原有iptables规则。

```
iptables -F
```

17. 执行以下命令，配置SNAT，使代理弹性云服务器所在的网段内其他弹性云服务器可通过代理弹性云服务器访问Internet。

```
iptables -t nat -A POSTROUTING -o eth0 -s subnet/netmask-bits -j SNAT
--to nat-instance-ip
```

假设代理弹性云服务器所在的网段为192.168.125.0，子网掩码为24位，私网IP地址为192.168.125.4，则执行如下命令。

```
iptables -t nat -A POSTROUTING -o eth0 -s 192.168.125.0/24 -j SNAT --to 192.168.125.4
```

### 说明

为了确保重启后上述规则不丢失，可以执行 `vi /etc/rc.local` 编辑 `rc.local` 文件，将 17 中的规则复制到 `rc.local` 文件，按“ESC”退出编辑模式，输入“:wq”保存并退出。

18. 执行以下命令，保存 iptables 的配置并设置开机自启动。

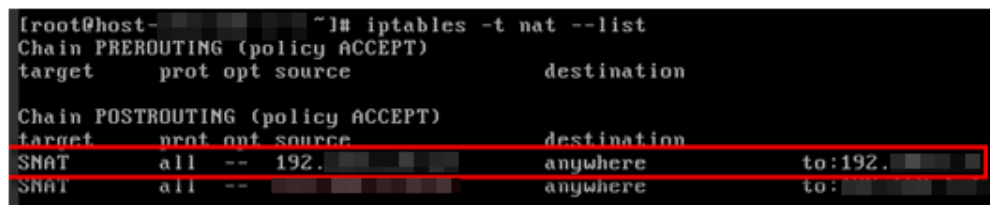
```
service iptables save
chkconfig iptables on
```

19. 执行以下命令，查看 SNAT 配置是否成功。

```
iptables -t nat --list
```

回显类似如图 7-6 所示时，表示 SNAT 配置成功。

图 7-6 SNAT 配置成功



```
[root@host- ~]# iptables -t nat --list
Chain PREROUTING (policy ACCEPT)
target prot opt source destination

Chain POSTROUTING (policy ACCEPT)
target prot opt source destination
SNAT all -- 192.168.125.0/24 anywhere to:192.168.125.4
SNAT all -- anywhere to:192.168.125.4
```

20. 添加自定义路由。

- 登录管理控制台。
- 单击管理控制台左上角的 ，选择区域和项目。
- 选择“网络 > 虚拟私有云”。
- 选择需要添加路由表的虚拟私有云，在“路由表”页面，单击“添加路由信息”。
- 根据界面提示，填写路由信息。
  - 目的地址：是目的网段，默认是 0.0.0.0/0。
  - 下一跳地址：是代理弹性云服务器的私有 IP 地址。  
您可以在弹性云服务器页面，查看该弹性云服务器的私有 IP 地址。

21. 如需删除添加的 iptables 规则，需执行以下命令：

```
iptables -t nat -D POSTROUTING -o eth0 -s subnet/netmask-bits -j SNAT --to nat-instance-ip
```

假设代理弹性云服务器所在的网段为 192.168.125.0，子网掩码为 24 位，私网 IP 地址为 192.168.125.4，则执行如下命令。

```
iptables -t nat -D POSTROUTING -o eth0 -s 192.168.125.0/24 -j SNAT --to 192.168.125.4
```

# 8 安全管理

## 8.1 提升云服务器安全性方法概述

### 操作场景

如果云服务器没有设置相关的安全防护，可能受到病毒入侵或外部攻击，导致数据泄露或丢失，影响业务的正常运行。

怎样保护云服务器免受攻击或病毒入侵？本节操作介绍常见的提升云服务器安全的措施。

### 防护类型简介

提升云服务器的安全性，分为云服务器“外部安全防护”和“内部安全防护”两方面。

表 8-1 提升云服务器安全的方法

| 类型     | 说明                                                                             | 防护方法                                                                                                                              |
|--------|--------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| 外部安全防护 | 常见的DDoS攻击、木马或病毒的入侵都是常见的外部安全问题。针对这类问题有多种常见的防护方案，例如开启主机安全防护您可以根据您的实际业务选择合适的防护方案。 | <ul style="list-style-type: none"><li>• 开启主机安全防护</li><li>• 配置云堡垒机</li><li>• 监控云服务器</li><li>• 开启防DDoS攻击</li><li>• 定期备份数据</li></ul> |
| 内部安全防护 | 弱密码、开放错误的端口可能引起内部安全防护问题，不提升云服务器的内部安全防护，外部安全防护方案就无法有效的拦截和阻断各种外部攻击。              | <ul style="list-style-type: none"><li>• 增加登录密码的强度</li><li>• 提升云服务器的端口安全</li><li>• 定期升级操作系统</li></ul>                              |

## 开启主机安全防护

企业主机安全服务（Host Security Service，HSS）是以工作负载为中心的安全产品，集成了主机安全、容器安全和网页防篡改，旨在解决混合云、多云数据中心基础架构中服务器工作负载的独特保护要求。HSS通过对主机、容器进行系统完整性的保护、应用程序控制、行为监控和基于主机的入侵防御等，保护工作负载免受攻击。

主机安全是旨在增强主机整体安全性的服务，通过主机管理、风险防御、入侵检测、安全运营、网页防篡改功能等功能，能够全面识别并管理主机内的信息资产，实时监测主机中潜在风险，并阻止非法入侵行为，帮助企业构建服务器安全体系，降低服务器所面临的安全威胁。主机安全工作原理请参考[什么是企业主机安全](#)。

使用主机安全需要在云服务器中安装Agent。安装Agent后，您的云服务器将受到HSS云端防护中心全方位的安全保障，在安全控制台可视化界面上，您可以统一查看并管理同一区域内所有主机的防护状态和主机安全风险。

针对新创建的云服务器和已有的云服务器提供不同的开启方式。

## 新创建云服务器开启主机安全

购买弹性云服务器，选择部分操作系统的公共镜像时，系统推荐您配套使用主机安全服务（Host Security Service，HSS）。

开启“主机安全”需要设置“安全防护”参数：

- 免费试用一个月主机安全基础防护：开启后，免费体验HSS基础版30天，为您的主机提供操作系统漏洞检测、弱口令检测、暴力破解检测等功能。

### 说明

主机安全基础防护免费使用期限结束后，该防护配额将自动释放，停止相应的实时防护能力。

如您需要保留或升级原有安全防护能力，建议您购买高阶防护。详细情况，请参见主机安全的[免费试用HSS基础版到期后怎么办？](#)。

购买弹性云服务器时，默认设置该选项。

- 购买高阶防护：高阶防护支持基础版、企业版、旗舰版和网页防篡改版，需付费使用。

购买后您可以在主机安全服务控制台切换不同版本。各版本之间的差异请参考[服务版本差异](#)。

- 不使用安全防护：若您不需要进行安全防护，可选择此选项。

选择主机安全后系统自动安装主机安全Agent，开启账号防御，启用主机安全服务的功能。

若基础版或企业版不满足要求，您可以[购买其他版本配额](#)，在主机安全服务控制台[切换不同版本](#)，获取更高级的防护，且不需要重新安装Agent。

图 8-1 开通主机安全



## 已创建的云服务器开启主机安全

对于已经创建完成的弹性云服务器，可能由于创建时尚未支持主机安全服务或未设置“安全防护”参数而暂未开启主机安全服务。开启主机安全的流程如下：

表 8-2 开启主机安全流程说明

| 序号 | 步骤            | 说明                                                                                                                                                                                                                                                                   |
|----|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | 购买防护配额        | 企业主机安全HSS提供基础版、专业版、企业版、旗舰版、网页防篡改版和容器版供您选择，每个版本支持的功能特性存在差异，您需要根据对主机的防护需求，购买对应的防护版本。HSS各版本的区别请参见 <a href="#">产品功能</a> 。                                                                                                                                                |
| 2  | 为华为云主机安装Agent | Agent是企业主机安全提供的一款软件，安装在云服务器上，用于与企业主机安全的云端防护中心进行数据交互，实现对主机的安全检测和防护。安装Agent后，您才能使用企业主机安全。                                                                                                                                                                              |
| 3  | 开启防护          | 完成购买防护配额、安装Agent后，HSS还未对云服务器进行防护，您需要为云服务器开启防护。                                                                                                                                                                                                                       |
| 4  | （可选）开启告警通知    | 默认情况下，HSS在防护主机/容器过程中发现的安全风险展示在管理控制台，您需要登录管理控制台查看。如果您需要及时了解主机/容器的安全风险，可以开启告警通知，开启后，HSS会将安全风险通过短信或邮件的方式发送给您。                                                                                                                                                           |
| 5  | （可选）常用安全配置    | 您可以根据实际业务需求，配置如下云服务器安全保护项，提升云服务器安全性： <ul style="list-style-type: none"><li>● 主机登录保护：配置常用登录地、常用登录IP、SSH登录IP白名单，对使用非常用登录地、登录IP进行登录的行为进行告警，拒绝白名单以外的IP登录。</li><li>● 双因子认证：双因素身份验证机制，结合短信/邮箱验证码，对登录云服务器行为进行二次认证。</li><li>● 恶意程序隔离查杀：对识别出的后门、木马、蠕虫等恶意程序进行自动隔离查杀。</li></ul> |

## 配置云堡垒机

云堡垒机（Cloud Bastion Host，CBH）可以实时收集和监控网络环境中每个组成部分的系统状态、安全事件和网络活动，保障网络和数据不受来自外部或内部用户的入侵和破坏，便于集中报警、及时处理及审计定责。

登录云堡垒机后，您需要依次创建用户、资源、访问策略，依次创建成功后才能对资源进行管理和运维。

- 云堡垒机支持Web浏览器、SSH客户端和MSTSC客户端三种登录方式。  
Web浏览器登录：支持系统管理和资源运维功能。建议系统管理员admin或管理人员使用Web浏览器登录进行系统管理和授权审计。  
SSH客户端登录：在不改变用户原来使用SSH客户端习惯的前提下，可对授权资源进行运维管理。运维人员可选择使用SSH客户端直接登录运维资源。

**MSTSC客户端登录**：在不改变用户原来使用MSTSC客户端习惯的前提下，可对授权资源进行运维管理。运维人员可选择使用MSTSC客户端直接登录运维资源。

- 在使用云堡垒机进行系统管理和运维前，管理人员需要在CBH系统中**创建系统用户**，为用户分配不同系统角色。

根据角色系统权限的不同，用户拥有不同的系统操作和访问权限，新创建的用户登录系统，即可访问角色权限内模块。

#### 说明

仅admin拥有管理系统角色的权限。

- 云堡垒机系统集中管理云资源，主要包括管理资源账户和运维权限管理。为实现统一管理资源，需**添加资源到系统**。

一个主机或应用资源可能有多个登录主机或应用的账户。

CBH系统纳管主机或应用的账户（资源账户）后，无需反复输入账户和密码，通过登录资源账户，自动登录资源进行运维管控。

系统默认资源账户Empty，登录Empty资源账户时需手动输入主机账户和对应密码。

- 若需通过云堡垒机运维资源，还需**配置访问控制策略**，关联用户和资源，赋予用户相应资源访问控制权限。
- 用户获取资源访问控制权限后，通过系统登录资源**进行运维**，运维过程被全程监控记录。

运维用户可根据资源类型选择不同登录方式。

- 用户获取相应系统权限和运维权限后，可通过云堡垒机登录已授权的资源进行运维操作，以及在系统进行系统数据管理操作。

管理员可在系统Web页面审计用户系统登录和操作，以及**审计用户运维会话**。

## 监控云服务器

监控是保持弹性云服务器可靠性、可用性和性能的重要部分，通过监控，用户可以观察弹性云服务器资源。为使用户更好地掌握自己的弹性云服务器运行状态，云平台提供了云监控。您可以使用该服务监控您的弹性云服务器，执行自动实时监控、告警和通知操作，帮助您更好地了解弹性云服务器的各项性能指标。详细介绍请参考**什么是云监控服务？**。

主机监控分为基础监控、操作系统监控和进程监控。

- **基础监控**

基础监控无需安装Agent，是ECS自动上报的监控指标。基础监控指标的监控周期为5分钟（KVM实例）。

- **操作系统监控**

操作系统监控需要在弹性云服务器中安装Agent插件，为用户提供服务器的系统级、主动式、细颗粒度监控服务。操作系统监控的监控周期为1分钟（KVM实例）。

**购买云服务器时的开启操作系统监控的方法：**

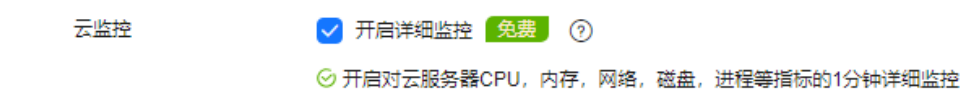
您可以在购买时勾选“开启详细监控”，勾选后云平台将自动安装操作系统监控所需的Agent插件。

#### 说明

当前仅部分操作系统支持在购买时开启详细监控。



图 8-2 购买云服务器时开启操作系统监控



为已创建完成的云服务器开启操作系统监控的方法：

如果创建时未勾选“开启详细监控”，如需使用操作系统监控，您需要手动安装 Agent。

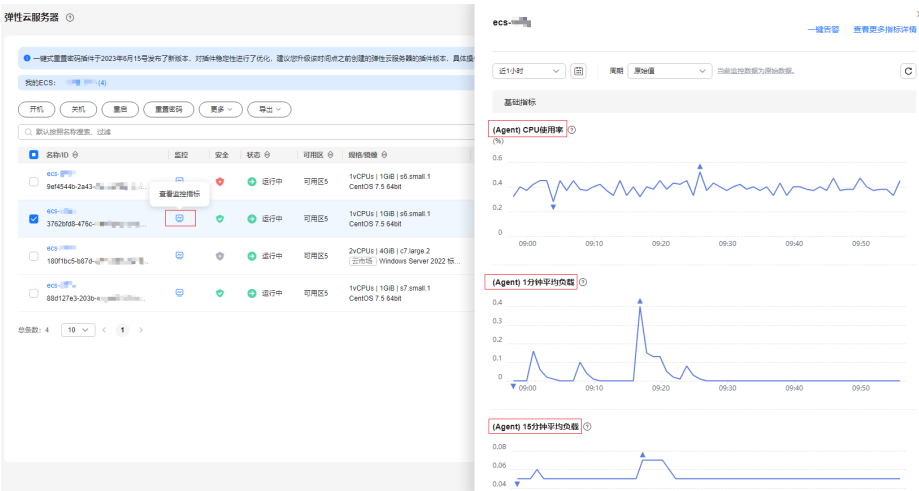
安装配置Agent相关操作请参考云监控服务“[Agent安装配置方式说明](#)”。

- 进程监控  
进程监控需要在弹性云服务器中安装Agent插件，对主机内活跃进程进行监控，进程监控的监控周期为1分钟（KVM实例）。

开启主机监控后您可以通过设置弹性云服务器告警规则，自定义监控目标与通知策略，及时了解弹性云服务器运行状况，从而起到预警作用。

在ECS的控制台单击 即可查看监控指标。

图 8-3 查看云服务器监控指标



开启防 DDoS 攻击

针对DDoS攻击，华为云提供多种安全防护方案，您可以根据您的实际业务选择合适的防护方案。华为云DDoS防护服务（Anti-DDoS Service，简称AAD）提供了DDoS原生基础防护（Anti-DDoS流量清洗）、DDoS原生专业防护和DDoS高防三个子服务。

其中，DDoS原生基础防护为免费服务，DDoS原生专业防护和DDoS高防为收费服务。

关于DDoS原生专业防护和DDoS高防请单击[DDoS防护](#)了解更多。

购买弹性云服务器时，如果选择了购买弹性公网IP，那么控制台会提示您已免费开启DDoS基础防护。

图 8-4 免费开启 DDoS 基础防护

弹性公网IP

现在购买

使用已有

暂不购买

线路

全动态BGP

静态BGP

公网带宽

按带宽计费

按流量计费

加入共享带宽

带宽大小

1

2

5

10

100

200

自定义

免费开启DDoS基础防护

DDoS原生基础防护（Anti-DDoS流量清洗）服务（以下简称Anti-DDoS）为云服务器提供DDoS攻击防护和攻击实时告警通知。同时，Anti-DDoS可以提升用户带宽利用率，确保用户业务稳定运行。

Anti-DDoS通过对互联网访问公网IP的业务流量进行实时监测，及时发现异常DDoS攻击流量。在不影响正常业务的前提下，根据用户配置的防护策略，清洗掉攻击流量。同时，Anti-DDoS为用户生成监控报表，清晰展示网络流量的安全状况。

定期备份数据

数据备份是防止系统出现数据丢失，将全部或部分数据以其他方式保留的过程。本节以云备份方法为例，了解更多备份方法请参考[云备份概述](#)。

云备份可以为云服务器、云硬盘提供简单易用的备份服务，当发生病毒入侵、人为误删除、软硬件故障等事件时，可将数据恢复到任意备份点。保障用户数据的安全性和正确性，确保业务安全。

购买云服务器时启用云备份的方法：

购买云服务器时，设置开启云备份完成后，系统会将云服务器绑定至云备份存储库并绑定所选备份策略，定期备份弹性云服务器。

- 现在购买：
  - a. 输入云备份存储库的名称：只能由中文字符、英文字母、数字、下划线、中划线组成，且长度小于等于64个字符。例如：vault-f61e。默认的命名规则为“vault\_xxxx”。
  - b. 输入存储库的容量：此容量为备份云服务器所需的容量。存储库的空间不能小于云服务器的空间。取值范围为[云服务器总容量，10485760]GB。
  - c. 设置备份策略：在下拉列表中选择备份策略，或进入云备份控制台查看或编辑备份策略。
- 使用已有：
  - a. 选择云备份存储库的名称：在下拉列表中选择已有的云备份存储库。
  - b. 设置备份策略：在下拉列表中选择备份策略，或进入云备份控制台查看或编辑备份策略。
- 暂不购买：跳过云备份的配置步骤。如云服务器购买成功后仍需设置备份保护，请进入云备份控制台找到目标存储库，绑定服务器。



图 8-5 设置云备份

云备份 使用云备份服务，需购买备份存储库，存储库是存放服务器产生的备份副本的容器。

ⓘ

云备份存储库名称

云备份存储库容量

为了保证连续性，建议存储库空间不小于备份服务器空间。

备份策略  ⓘ

当前备份策略状态为停用，绑定该策略的存储库不会进行自动备份。单击[应用备份策略](#)。

如需创建或修改备份策略，请[前往云备份控制台](#)进行操作，操作后请单击刷新按钮同步备份策略。

已创建完成的云服务器创建云备份的方法：

**备份云服务器**可以通过“云服务器备份”和“云硬盘备份”功能实现：

- 云服务器备份（推荐）：如果是对弹性云服务器中的所有云硬盘（系统盘和数据盘）进行备份，推荐使用云服务器备份功能，同时对所有云硬盘进行备份，避免因备份创建时间差带来的数据不一致问题。
- 云硬盘备份：如果对指定的单个或多个云硬盘（系统盘或数据盘）进行备份，推荐使用云硬盘备份功能，在保证数据安全的同时降低备份成本。

## 增加登录密码的强度

“密钥对”方式创建的弹性云服务器安全性更高，建议选择“密钥对”方式。

如果您习惯使用“密码”方式，请增强密码的复杂度，保证密码符合要求，防止恶意攻击。详细内容，请参见[密码使用场景介绍](#)。

系统不会定期自动修改弹性云服务器密码。为安全起见，建议您定期修改密码。

密码设置建议：

- 密码应该长度不少于10位。
- 建议不要使用有一定特征和规律容易被破解的常用口令的密码（如：在常用彩虹表中的密码、滚键盘密码等），且密码复杂度至少包含大写字母、小写字母、数字、特殊字符四类中的三种。
- 密码尽量不要包含账户名如：administrator/administrator，test/test，root/root，oracle/oracle，mysql/mysql。
- 建议至少每90天更改一次密码。
- 建议不要重复使用最近5次（含5次）内已使用的密码。
- 建议根据不同应用设置不同的账号密码，不建议多个应用使用同一密码。

## 提升云服务器的端口安全

安全组是云服务器的守卫，是重要的网络安全隔离手段，可以保护云服务器的网络安全。安全组可以控制进出云服务器的网络流量。网络流量分为出方向和入方向，出方向是指您想访问别人，入方向就是别人想访问您。如果把云服务器比作一个宫殿，那安全组就像是一个守卫者，谁能进出，都由安全组规则控制。

通过[配置安全组规则](#)，限定云服务器出方向和入方向的访问端口，通常建议您关闭高危端口，仅开启必要的云服务器端口。

常见的高危端口如表8-3所示，建议您修改敏感端口为其它非高危端口来承载业务。请参考云服务器常用端口。

表 8-3 常见的高危端口

| 协议  | 端口                                                                                              |
|-----|-------------------------------------------------------------------------------------------------|
| TCP | 42 135 137 138 139 444 445 593 1025 1068 1434 3127 3128 3129 3130 4444 4789 5554 5800 5900 9996 |
| UDP | 135~139 1026 1027 1028 1068 1433 1434 4789 5554 9996                                            |

定期升级操作系统

云服务器申请完成后，系统内的所有配置都是需要您自行维护，云平台不负责客户系统补丁的升级，对于官方发布的一些漏洞预警，会有安全公告，需要您自行升级维护。

8.2 安全组

8.2.1 安全组概述

安全组

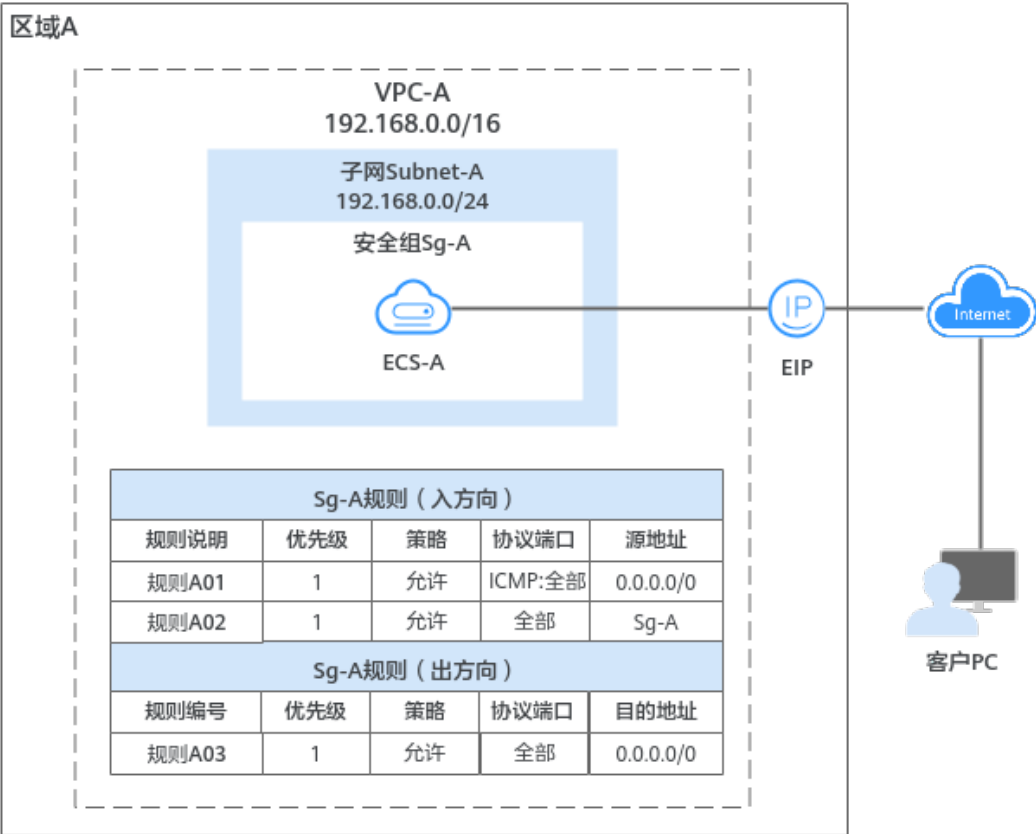
安全组是一个逻辑上的分组，为具有相同安全保护需求并相互信任的云服务器提供访问策略。安全组创建后，用户可以在安全组中定义各种访问规则，当云服务器加入该安全组后，即受到这些访问规则的保护。

您在创建弹性云服务器时，必须将实例加入一个安全组，如果此前您还未创建任何安全组，那么系统会自动为您创建默认安全组并关联至该实例。除了默认安全组，您还可以根据业务需求创建自定义安全组并关联至实例。一个实例可以关联多个安全组，多个安全组按照优先级顺序依次匹配流量。

安全组中包括入方向规则和出方向规则，您可以针对每条入方向规则指定来源、端口和协议，针对出方向规则指定目的地、端口和协议，用来控制安全组内实例入方向和出方向的网络流量。以图8-6为例，在区域A内，某客户有一个虚拟私有云VPC-A和子网Subnet-A，在子网Subnet-A中创建一个云服务器ECS-A，并为ECS-A关联一个安全组Sg-A来保护ECS-A的网络安全。

- 安全组Sg-A的入方向存在一条放通ICMP端口的自定义规则，因此可以通过个人PC(计算机)ping通ECS-A。但是安全组内未包含允许SSH流量进入实例的规则，因此您无法通过个人PC远程登录ECS-A。
- 当ECS-A需要通过EIP访问公网时，由于安全组Sg-A的出方向规则允许所有流量从实例流出，因此ECS-A可以访问公网。

图 8-6 安全组架构图



云上一分钟，了解什么是安全组。

说明

- 安全组需在网络互通的情况下生效。若实例属于不同VPC，但同属于一个安全组，则此安全组不生效，您可以使用对等连接等产品建立VPC连接互通。VPC连接请参见[VPC连接](#)。
- 您可以免费使用安全组资源，当前不收取任何费用。

安全组规则

安全组创建后，您可以在安全组中设置出方向、入方向规则，这些规则会对安全组内部的云服务器出入方向网络流量进行访问控制，当云服务器加入该安全组后，即受到这些访问规则的保护。安全组规则工作原理请参考[安全组及规则的工作原理](#)。

每个安全组都自带默认安全组规则，详情请参见[默认安全组和规则](#)。您也可以自定义添加安全组规则，请参见[配置安全组规则](#)。

安全组中包括入方向规则和出方向规则，用来控制安全组内实例的入方向和出方向的网络流量。

- 入方向规则：控制外部请求访问安全组内的实例，即流量流入实例。
- 出方向规则：控制安全组内实例访问外部的请求，即流量从实例流出。

安全组规则由协议端口、源地址/目的地址等组成，详见[表8-4](#)。

表 8-4 安全组规则关键参数说明

| 参数       | 说明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 策略       | 支持允许或拒绝。当流量的协议、端口、源地址/目的地址成功匹配某个安全组规则后，会对流量执行规则对应的策略，允许或拒绝流量。                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 优先级      | 可选范围为1-100，数字越小，规则优先级级别越高。<br>安全组规则匹配流量时，首先按照优先级进行排序，其次按照策略排序，拒绝策略高于允许策略，更多信息请参见 <a href="#">流量匹配安全组规则的顺序</a> 。                                                                                                                                                                                                                                                                                                                                                                                         |
| 类型       | 支持设置IPv4和IPv6协议的规则。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 协议端口     | 包括网络协议类型和端口范围。 <ul style="list-style-type: none"><li>● <b>网络协议</b>：匹配流量的协议类型，支持TCP、UDP、ICMP和GRE协议。<ul style="list-style-type: none"><li>– <b>TCP协议</b>：擅长可靠传输，适用于远程登录、网页浏览、邮件传输和文件传输等对数据完整性要求高的场景。</li><li>– <b>UDP协议</b>：传输速度快，适用于在线游戏、视频会议等对速度要求高的应用，减少数据传输的延迟，确保体验的流畅性。</li><li>– <b>ICMP协议</b>：用于网络设备间通信，传递控制信息，如使用ping命令检测网络设备之间的连通性、生成错误报告供运维使用、传递诊断信息用于分析优化网络等。</li><li>– <b>GRE协议</b>：通用性强，用于封装和传输不同网络协议数据，实现跨网络传输，如封装IP数据包。</li></ul></li><li>● <b>端口范围</b>：匹配流量的目的端口，取值范围为：1～65535。</li></ul> |
| 源地址或目的地址 | 在入方向中，匹配流量的源地址。在出方向中，匹配流量的目的地址。<br>您可以使用IP地址、安全组、IP地址组作为源地址或者目的地址。 <ul style="list-style-type: none"><li>● <b>IP地址</b>：某个固定的IP地址或者网段，支持IPv4和IPv6地址。比如：192.168.10.10/32（IPv4地址）、192.168.1.0/24（IPv4网段）、2407:c080:802:469::/64（IPv6网段）。</li><li>● <b>安全组</b>：目标安全组和当前安全组位于同一区域，表示流量匹配目标安全组内所有实例的私有IP地址。比如：当安全组A内有实例a，安全组B内有实例b，在安全组A的入方向规则中，放通源地址为安全组B的流量，则来自实例b的内网访问请求被允许进入实例a。</li><li>● <b>IP地址组</b>：<a href="#">创建IP地址组</a>是一个或者多个IP地址的集合，对于安全策略相同的IP网段和IP地址，建议您使用IP地址组简化管理。</li></ul>                |

安全组配置示例

您可以在安全组内放通指定IP地址，允许指定IP地址访问安全组内实例，或者在某个安全组内放通另外一个安全组，实现不同安全组内的实例内网互通。通过安全组规则，

您可以灵活控制组网内流量的走向，以确保您的网络安全，以下为您提供典型的安  
全组应用示例。

说明

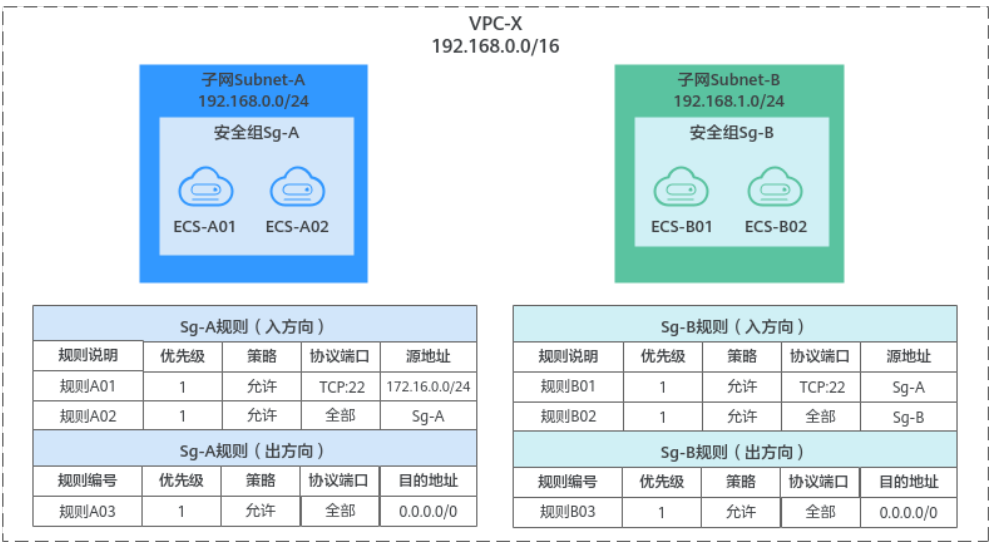
更多安全组规则配置示例，请参见[安全组配置示例](#)。

控制外部指定 IP 地址或安全组对实例的访问

如图8-7所示，在VPC-X中有两个子网Subnet-A和Subnet-B，Subnet-A中的ECS承载同  
一类业务，需要相同的网络连接请求，因此均关联至安全组Sg-A。同理，Subnet-B中  
的ECS均关联至另外一个安全组Sg-B。

- 安全组Sg-A入方向规则A01允许从指定IP地址 (172.16.0.0/24)访问安全组内实例  
的SSH(22)端口，用于远程登录安全组内的Linux云服务器。
- 安全组Sg-A入方向规则A02允许安全组内的实例可使用任何协议和端口互相通  
信，即子网Subnet-A内的ECS网络互通。
- 安全组Sg-B入方向规则B01允许Sg-A内的实例访问Sg-B内实例的SSH(22)端口，  
即通过子网Subnet-A的ECS可远程登录Subnet-B内的ECS。
- 安全组Sg-B入方向规则B02允许安全组内的实例可使用任何协议和端口互相通  
信，即子网Subnet-B内的ECS网络互通。
- 两个安全组的出方向规则允许所有流量从安全组内实例流出。

图 8-7 控制外部指定 IP 地址或安全组对实例的访问



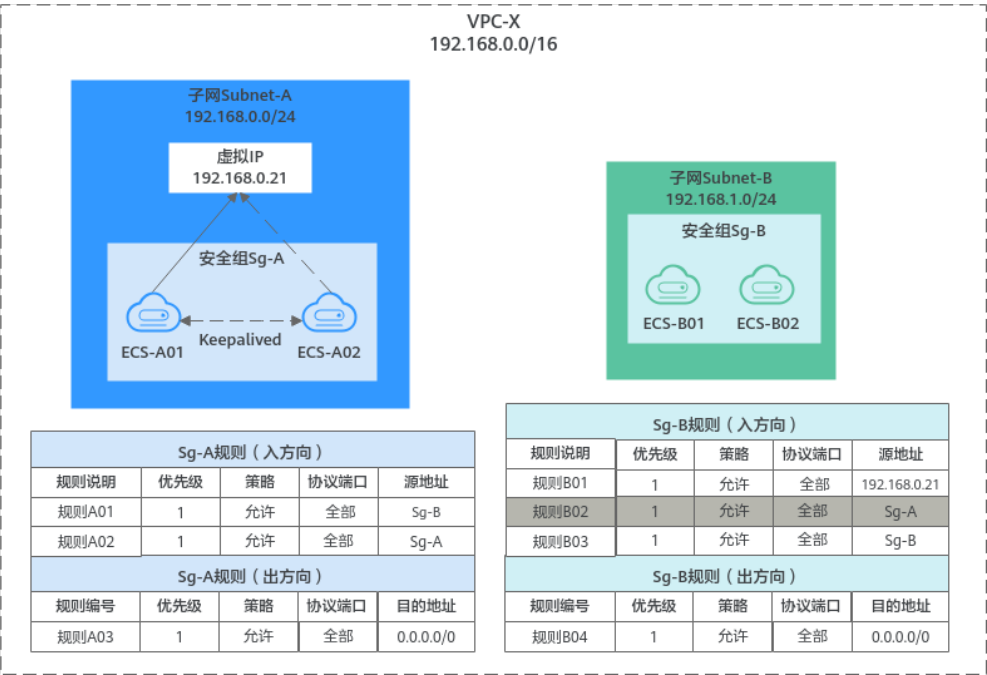
控制虚拟 IP 访问安全组内实例

如果您通过中间网络实例在不同子网的实例之间转发流量，比如图8-8中，子网  
Subnet-A的ECS通过虚拟IP和子网Subnet-B的ECS互相通信。由于存在中间网络实例，  
此时安全组规则的源地址选择实例所在的安全组时，无法放通中间网络实例转发的流  
量，源地址必须设置成中间网络实例的私有IP地址或者子网网段。

在VPC-X中有两个子网Subnet-A和Subnet-B，Subnet-A中的ECS关联至安全组Sg-A，  
Subnet-B中的ECS关联至安全组Sg-B。通过虚拟IP将Subnet-A中的ECS搭建成  
Keepalived高可用集群，后端服务器ECS-A01和ECS-A02形成主备模式，对外使用虚拟  
IP进行通信。

- 安全组Sg-A入方向规则A01允许Sg-B内的实例使用任何协议和端口访问Sg-A内的实例。
- 安全组Sg-B入方向规则说明如下：
  - 规则B02：允许Sg-A内的实例使用私有IP地址访问Sg-B内实例，但是当前组网下，Sg-A内的实例和Sg-B内的实例通信需要经过虚拟IP，此时虚拟IP的流量无法流入Sg-B内的实例，该规则不适用于当前组网。
  - 规则B01：允许虚拟IP(192.168.0.21)使用任何协议和端口访问Sg-B内的实例。当前组网中，您还可以将源地址设置成子网Subnet-A的网段192.168.0.0/24。

图 8-8 控制虚拟 IP 访问安全组内实例



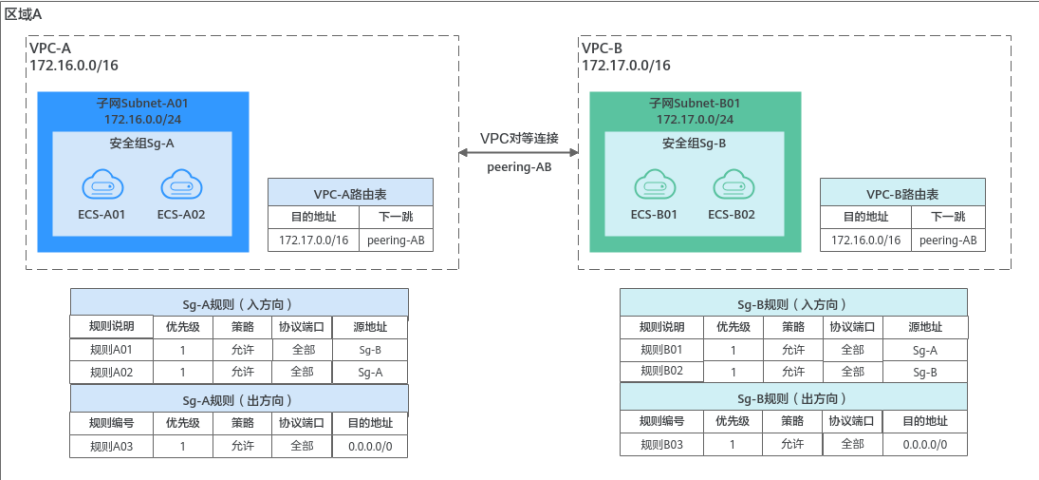
控制对等连接两端 VPC 内的实例互访

如图8-9所示，在区域A内，通过VPC对等连接连通VPC-A和VPC-B之间的网络。对等连接路由配置完成后，子网Subnet-A01和子网Subnet-B01之间网络已连通。但是由于两个子网内的ECS分别关联了不同的安全组，此时ECS之间仍然网络不通，您还需要放通安全组Sg-A和Sg-B的网络，才可以实现对等连接两端的ECS网络互通。

- 在安全组Sg-A中，规则A01允许来自Sg-B内实例的流量访问Sg-A内的实例，源地址为安全组Sg-B。
- 在安全组Sg-B中，规则B01允许来自Sg-A内实例的流量访问Sg-B内的实例，源地址为安全组Sg-A。



图 8-9 控制对等连接两端 VPC 内的实例互访



安全组配置指引

如果您第一次使用安全组，建议您按照如下步骤操作：

表 8-5 安全组配置指引

| 操作场景       | 场景说明                                                                      | 参考文档                                                                                       |
|------------|---------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| 创建安全组      | 如果默认安全组和已有自定义安全组均不满足业务需要，您可以单独创建安全组。                                      | <a href="#">创建安全组</a><br><b>说明</b><br>创建ECS实例时，支持使用预设规则快速创建安全组，请参考 <a href="#">新建安全组</a> 。 |
| 配置安全组规则    | 安全组创建完成后，如果安全组中的规则不能满足业务要求，您可以根据需要增删入方向规则和出方向规则，修改已有安全组规则的策略、优先级、协议端口等信息。 | <a href="#">配置安全组规则</a>                                                                    |
| ECS实例关联安全组 | 创建ECS实例时，至少关联一个安全组，实例的出入流量受到安全组的保护。如果不满足业务需要，您可以调整ECS实例已关联的安全组。           | <a href="#">加入安全组</a><br><a href="#">移出安全组</a><br><a href="#">更改安全组</a>                    |

安全组的使用限制

- 为了确保良好的网络性能体验，建议一个实例最多关联5个安全组。
- 建议一个安全组关联的实例数量不应超过6000个，否则会引起安全组性能下降。
- 在一个安全组中，对于入方向规则来说，源地址是安全组的规则数量+源地址是IP地址组的规则数量+端口是不连续端口号的规则数量 ≤ 120条，否则超过数量的安全组规则将不生效。当同时存在IPv4和IPv6类型的安全组规则时，两种类型的安全组规则单独计算，即IPv4规则和IPv6规则可以各有120条。  
对于安全组出方向规则来说，目的地址和端口存在一样的限制。

以安全组Sg-A的入方向IPv4规则为例，表8-6中提供了部分符合限制条件的规则供您参考。其中，当一条安全组规则同时符合多个限制时，比如规则A02即使用了不连续端口，又使用了安全组作为源地址，此时只占用一条配额。

表 8-6 入方向安全组规则示例

| 规则编号  | 策略 | 类型   | 协议端口          | 源地址                  |
|-------|----|------|---------------|----------------------|
| 规则A01 | 允许 | IPv4 | 全部            | 当前安全组：Sg-A           |
| 规则A02 | 允许 | IPv4 | TCP: 22,25,27 | 其他安全组：Sg-B           |
| 规则A03 | 允许 | IPv4 | TCP: 80-82    | IP地址组：ipGroup-A      |
| 规则A04 | 允许 | IPv4 | TCP: 22-24,25 | IP地址: 192.168.0.0/16 |

- 如果您添加安全组规则时，使用IP地址组或者不连续端口，那么该安全组规则对不同规格云服务器的生效情况存在差异，为了避免您的安全组规则不生效，请您查看表8-7了解详情。

表 8-7 安全组规则限制

| 安全组规则                           | 云服务器类型                                                                                                                                                                                            |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 添加安全组规则时，“源地址”和“目的地址”可选择“IP地址组” | 不支持的X86云服务器规格如下： <ul style="list-style-type: none"><li>通用计算型（S1型、C1型、C2型）</li><li>内存优化型（M1型）</li><li>高性能计算型（H1型）</li><li>磁盘增强型（D1型）</li><li>GPU加速型（G1型、G2型）</li><li>超大内存型（E1型、E2型、ET2型）</li></ul> |
| 添加安全组规则时，“协议端口”可配置为不连续端口号       | 不支持的X86云服务器规格如下： <ul style="list-style-type: none"><li>通用计算型（S1型、C1型、C2型）</li><li>内存优化型（M1型）</li><li>高性能计算型（H1型）</li><li>磁盘增强型（D1型）</li><li>GPU加速型（G1型、G2型）</li><li>超大内存型（E1型、E2型、ET2型）</li></ul> |



| 安全组规则 | 云服务器类型                                                                                                                                                                     |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <p>所有鲲鹏云服务器规格不支持配置不连续端口。</p> <p>如果您在鲲鹏云服务器中添加安全组规则时，使用了不连续端口号，那么除了该条规则不会生效，该规则后的其他规则也不会生效。比如：</p> <p>您先配置了安全组规则A（不连续端口号22,24），再配置了下一条安全组规则B（独立端口号9096），则安全组规则A和B均不会生效。</p> |

说明

- X86云服务器规格详情，请参见[规格清单（X86）](#)。
- 鲲鹏云服务器规格详情，请参见[规格清单（鲲鹏）](#)。
- 当您的组网中存在以下情况时，来自ELB和VPCEP的流量不受网络ACL和安全组规则的限制。
  - ELB实例的监听器开启“获取客户端IP”功能时，不受限制。  
比如规则已明确拒绝来自ELB实例的流量进入后端云服务器，此时该规则无法拦截来自ELB的流量，流量依然会抵达后端云服务器。
  - VPCEP实例类型为“专业型”时，不受限制。

实践建议

- 请您遵循白名单原则配置安全组规则，即安全组内实例默认拒绝所有外部的访问请求，通过添加允许规则放通指定的网络流量。
- 添加安全组规则时，请遵循最小授权原则。例如，放通22端口用于远程登录云服务器时，建议仅允许指定的IP地址登录，谨慎使用0.0.0.0/0（所有IP地址）。
- 请您尽量保持单个安全组内规则的简洁，通过不同的安全组来管理不同用途的实例。如果您使用一个安全组管理您的所有业务实例，可能会导致单个安全组内的规则过于冗余复杂，增加维护管理成本。
- 您可以将实例按照用途加入到不同的安全组内。例如，当您具有面向公网提供网站访问的业务时，建议您将运行公网业务的Web服务器加入到同一个安全组，此时仅需要放通对外部提供服务的特定端口，例如80、443等，默认拒绝外部其他的访问请求。同时，请避免在运行公网业务的Web服务器上运行内部业务，例如MySQL、Redis等，建议您将内部业务部署在不需要连通公网的服务器上，并将这些服务器关联至其他安全组内。
- 对于安全策略相同的多个IP地址，您可以将其添加到一个IP地址组内统一管理，并在安全组内添加针对该IP地址组的授权规则。当IP地址发生变化时，您只需要在IP地址组内修改IP地址，那么IP地址组对应的安全组规则将会随之变更，无需逐次修改安全组内的规则，降低了安全组管理的难度，提升效率。具体方法，请参见[使用IP地址组提升安全组规则管理效率](#)。
- 请您尽量避免直接修改已运行业务的安全组规则。如果您需要修改使用中的安全组规则，建议您先克隆一个测试安全组，然后在测试安全组上进行调试，确保测试安全组内实例网络正常后，再修改使用中的安全组规则，减少对业务的影响。具体方法，请参见[克隆安全组](#)。
- 您在安全组内新添加实例，或者修改安全组的规则后，此时不需要重启实例，安全组规则会自动生效。

如果您的安全组规则配置完未生效，请参考[为什么配置的安全组规则不生效？](#)。

## 相关链接

- [默认安全组和规则](#)
- [安全组配置示例](#)
- [ECS常用端口](#)
- [配置安全组规则](#)
- [更改安全组](#)
- [加入安全组](#)
- [移出安全组](#)
- [查看安全组](#)
- [Windows云服务器访问公网不通应如何处理？](#)
- [防火墙设置](#)

### 8.2.2 默认安全组和规则

如果您未创建任何安全组，那么您在首次使用安全组时，系统会自动为您创建一个默认安全组。

- 默认安全组名称为default，为了区分默认安全组和您自己创建的安全组，不支持修改默认安全组名称。
- 您无法删除默认安全组，可以在默认安全组内修改已有规则或者添加新的规则。
- 默认安全组仅确保安全组内实例互通，默认拒绝所有外部请求进入实例，如果您需要登录默认安全组关联的实例，请参见[通过本地服务器远程登录云服务器](#)添加安全组规则放通指定端口。
- 如果实际业务对不同用途实例的安全要求存在差异，那么建议您创建自定义安全组，并将实例按照用途加入到不同的安全组内。

#### 说明

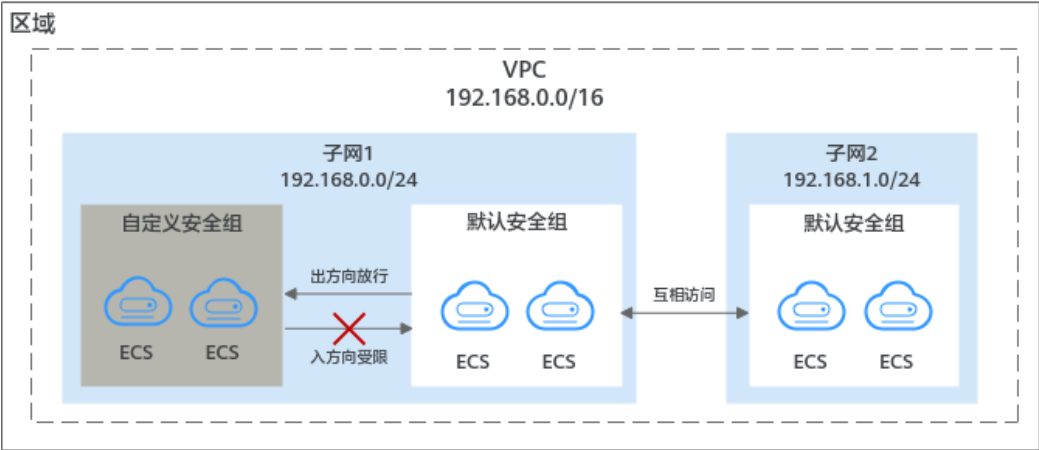
您可以免费使用安全组资源，当前不收取任何费用。

默认安全组规则说明如下：

- **入方向规则：**入方向流量受限，只允许安全组内实例互通，拒绝来自安全组外部的所有请求进入实例。
- **出方向规则：**出方向流量放行，允许所有请求从安全组内实例流出。

如[图8-10](#)所示。

图 8-10 默认安全组



默认安全组规则如表8-8所示：

表 8-8 默认安全组规则

| 方向  | 策略 | 类型       | 协议<br>端口 | 源地址/目的<br>地址                 | 描述                                               |
|-----|----|----------|----------|------------------------------|--------------------------------------------------|
| 入方向 | 允许 | IPv<br>4 | 全部       | 源地址：默认<br>安全组<br>( default ) | 针对全部IPv4协议，允许安全组内的实例可使用任何协议和端口互相通信，确保安全组内实例网络互通。 |
| 入方向 | 允许 | IPv<br>6 | 全部       | 源地址：默认<br>安全组<br>( default ) | 针对全部IPv6协议，允许安全组内的实例可使用任何协议和端口互相通信，确保安全组内实例网络互通。 |
| 出方向 | 允许 | IPv<br>4 | 全部       | 目的地址：<br>0.0.0.0/0           | 针对全部IPv4协议，允许所有流量从安全组内实例流出，即实例可访问外部任意IP和端口。      |
| 出方向 | 允许 | IPv<br>6 | 全部       | 目的地<br>址： ::/0               | 针对全部IPv6协议，允许所有流量从安全组内实例流出，即实例可访问外部任意IP和端口。      |

首次创建弹性云服务器时，系统会自动新建虚拟私有云vpc-default，同时对安全组进行如下操作：

- 新增Sys-WebServer安全组
- 新增Sys-FullAccess安全组
- 在默认安全组default中新增安全组规则

表 8-9 默认 default 安全组规则

| 规则方向  | 策略 | 类型   | 协议端口      | 源地址/目的地址               | 描述                                                |
|-------|----|------|-----------|------------------------|---------------------------------------------------|
| 入方向规则 | 允许 | IPv4 | TCP: 3389 | 源地址: 0.0.0.0/0         | 针对全部IPv4协议，允许所有IP地址通过默认Windows远程桌面连接到Windows云服务器。 |
| 入方向规则 | 允许 | IPv4 | TCP: 22   | 源地址: 0.0.0.0/0         | 针对全部IPv4协议，允许所有IP地址通过SSH远程连接到Linux云服务器。           |
| 入方向规则 | 允许 | IPv4 | 全部        | 源地址: 默认安全组 ( default ) | 针对全部IPv4协议，允许本安全组内实例的请求进入，即该条规则确保安全组内的实例网络互通。     |
| 入方向规则 | 允许 | IPv6 | 全部        | 源地址: 默认安全组 ( default ) | 针对全部IPv6协议，允许本安全组内实例的请求进入，即该条规则确保安全组内的实例网络互通。     |
| 出方向规则 | 允许 | IPv4 | 全部        | 目的地址: 0.0.0.0/0        | 针对全部IPv4协议，允许安全组内的实例可访问外部IP的所有端口。                 |
| 出方向规则 | 允许 | IPv6 | 全部        | 目的地址: ::/0             | 针对全部IPv6协议，允许安全组内的实例可访问外部IP的所有端口。                 |

表 8-10 Sys-WebServer 安全组规则

| 规则方向  | 策略 | 类型   | 协议端口      | 目的地址/源地址                  | 描述                                                |
|-------|----|------|-----------|---------------------------|---------------------------------------------------|
| 入方向规则 | 允许 | IPv4 | ICMP: 全部  | 源地址: 0.0.0.0/0            | 针对全部IPv4协议，允许在云服务器上使用ping命令验证网络的连通性。              |
| 入方向规则 | 允许 | IPv4 | 全部        | 源地址: 当前安全组(Sys-WebServer) | 针对全部IPv4协议，允许本安全组内实例的请求进入，即该条规则确保安全组内的实例网络互通。     |
| 入方向规则 | 允许 | IPv4 | TCP: 443  | 源地址: 0.0.0.0/0            | 针对全部IPv4协议，允许所有IP地址通过HTTPS协议访问云服务器上搭建的网站。         |
| 入方向规则 | 允许 | IPv4 | TCP: 80   | 源地址: 0.0.0.0/0            | 针对全部IPv4协议，允许所有IP地址通过HTTP协议访问云服务器上搭建的网站。          |
| 入方向规则 | 允许 | IPv4 | TCP: 22   | 源地址: 0.0.0.0/0            | 针对全部IPv4协议，允许所有IP地址通过SSH远程连接到Linux云服务器。           |
| 入方向规则 | 允许 | IPv4 | TCP: 3389 | 源地址: 0.0.0.0/0            | 针对全部IPv4协议，允许所有IP地址通过默认Windows远程桌面连接到Windows云服务器。 |

| 规则方向  | 策略 | 类型   | 协议端口 | 目的地址/源地址                 | 描述                                            |
|-------|----|------|------|--------------------------|-----------------------------------------------|
| 入方向规则 | 允许 | IPv6 | 全部   | 源地址：当前安全组(Sys-WebServer) | 针对全部IPv6协议，允许本安全组内实例的请求进入，即该条规则确保安全组内的实例网络互通。 |
| 出方向规则 | 允许 | IPv4 | 全部   | 目的地址：0.0.0.0/0           | 针对全部IPv4协议，允许安全组内的实例可访问外部IP的所有端口。             |
| 出方向规则 | 允许 | IPv6 | 全部   | 目的地址：::/0                | 针对全部IPv6协议，允许安全组内的实例可访问外部IP的所有端口。             |

表 8-11 Sys-FullAccess 安全组规则

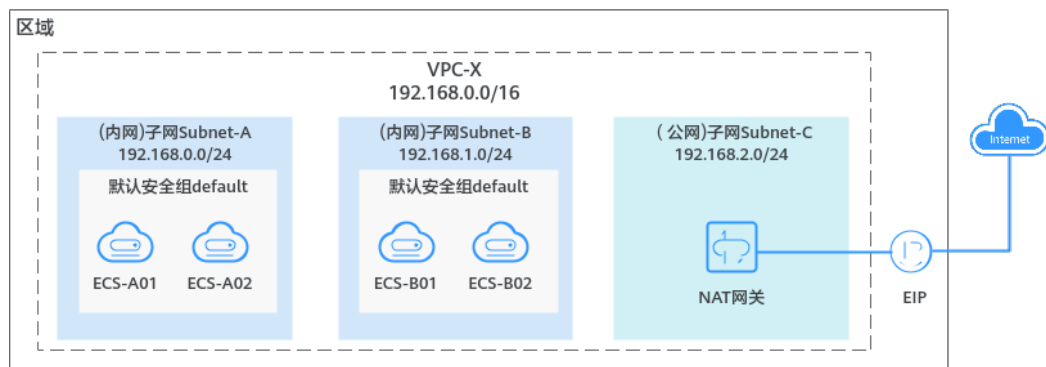
| 规则方向  | 策略 | 类型   | 协议端口 | 目的地址/源地址                  | 说明                                            |
|-------|----|------|------|---------------------------|-----------------------------------------------|
| 入方向规则 | 允许 | IPv4 | 全部   | 源地址：当前安全组(Sys-FullAccess) | 针对全部IPv4协议，允许本安全组内实例的请求进入，即该条规则确保安全组内的实例网络互通。 |
| 入方向规则 | 允许 | IPv6 | 全部   | 源地址：当前安全组(Sys-FullAccess) | 针对全部IPv6协议，允许本安全组内实例的请求进入，即该条规则确保安全组内的实例网络互通。 |
| 入方向规则 | 允许 | IPv4 | 全部   | 源地址：0.0.0.0/0             | 针对全部IPv4协议，允许所有入站流量的数据报文通过。                   |
| 入方向规则 | 允许 | IPv6 | 全部   | 源地址：::/0                  | 针对全部IPv6协议，允许所有入站流量的数据报文通过。                   |
| 出方向规则 | 允许 | IPv4 | 全部   | 目的地址：0.0.0.0/0            | 针对全部IPv4协议，允许安全组内的实例可访问外部IP的所有端口。             |
| 出方向规则 | 允许 | IPv6 | 全部   | 目的地址：::/0                 | 针对全部IPv6协议，允许安全组内的实例可访问外部IP的所有端口。             |

默认安全组应用示例

如图8-11所示，VPC-X内有三个子网，其中子网Subnet-A和Subnet-B中的ECS均关联默认安全组，默认安全组仅确保安全组内实例互通，默认拒绝所有外部请求进入实例。ECS-A01、ECS-A02、ECS-B01和ECS-B02之间内网网络互通，但是无法接受来自NAT网关的流量。

如果您需要放通NAT网关的流量，您可以在默认安全组中添加对应的规则，或者创建新的安全组，并关联给实例使用。

图 8-11 默认安全组应用示例



### 8.2.3 安全组配置示例

当您在VPC子网内创建实例（云服务器、云容器、云数据库等）时，您可以使用系统提供的**默认安全组default**，您也可以创建其他安全组。无论是默认安全组，还是您创建的安全组，您均可以**在安全组内设置出方向和入方向规则**，以此控制出入实例的流量。以下为您介绍一些常用的安全组的配置示例：

- [通过本地服务器远程登录云服务器](#)
- [在本地服务器远程连接云服务器上传或者下载文件（FTP）](#)
- [在云服务器上搭建网站对外提供Web服务](#)
- [使用ping命令验证网络连通性](#)
- [实现不同安全组的实例内网网络互通](#)
- [云服务器提供数据库访问服务](#)
- [限制云服务器访问外部网站](#)

#### 须知

如果您的安全组规则配置完成后不生效，请您参考[为什么配置的安全组规则不生效](#)排查可能原因，或者[提交工单](#)联系客服处理。

### 使用须知

在配置安全组规则之前，您需要先了解以下信息：

- 不同安全组之间的实例默认网络隔离，无法互相访问。
- 安全组默认拒绝所有来自外部的请求，即本安全组内的实例网络互通，外部无法访问安全组内的实例。  
您需要遵循白名单原则添加安全组入方向规则，允许来自外部的特定请求访问安全组内的实例。
- 安全组入方向规则的源地址设置为0.0.0.0/0或::/0，表示允许或拒绝所有外部IP地址访问您的实例，如果将“22、3389、8848”等[高危端口](#)暴露到公网，可能导致网络入侵，造成业务中断、数据泄露或数据勒索等严重后果。建议您将安全组规则设置为仅允许已知的IP地址访问。
- 安全组的出方向规则一般默认全部放通，即允许安全组内的实例访问外部。

如果出方向规则被删除，将会导致安全组内实例无法正常访问外部，您可以参考[表8-12](#)重新添加规则。

表 8-12 安全组默认出方向规则

| 方向  | 优先级 | 策略 | 类型   | 协议端口 | 目的地址      | 描述                                |
|-----|-----|----|------|------|-----------|-----------------------------------|
| 出方向 | 1   | 允许 | IPv4 | 全部   | 0.0.0.0/0 | 针对全部IPv4协议，允许安全组内的实例可访问外部任意IP和端口。 |
| 出方向 | 1   | 允许 | IPv6 | 全部   | ::/0      | 针对全部IPv6协议，允许安全组内的实例可访问外部任意IP和端口。 |

通过本地服务器远程登录云服务器

安全组默认拒绝所有来自外部的请求，如果您需要通过本地服务器远程登录安全组内的云服务器，那么需要根据您的云服务器操作系统类型，在安全组入方向添加对应的规则。

- 通过SSH远程登录Linux云服务器，需要放通SSH(22)端口，请参见[表8-13](#)。
- 通过RDP远程登录Windows云服务器，需要放通RDP(3389)端口，请参见[表8-14](#)。

表 8-13 通过 SSH 远程登录 Linux 云服务器

| 方向  | 优先级 | 策略 | 类型   | 协议端口       | 源地址             |
|-----|-----|----|------|------------|-----------------|
| 入方向 | 1   | 允许 | IPv4 | 自定义TCP: 22 | IP地址: 0.0.0.0/0 |

表 8-14 通过 RDP 远程登录 Windows 云服务器

| 方向  | 优先级 | 策略 | 类型   | 协议端口         | 源地址             |
|-----|-----|----|------|--------------|-----------------|
| 入方向 | 1   | 允许 | IPv4 | 自定义TCP: 3389 | IP地址: 0.0.0.0/0 |

 **注意**

源地址设置为0.0.0.0/0表示允许所有外部IP地址远程登录云服务器，如果将当前端口暴露到公网，可能存在网络安全风险，建议您将源IP设置为已知的IP地址，配置示例请参见[表8-15](#)。



表 8-15 通过已知 IP 地址远程登录云服务器

| 云服务器类型      | 方向  | 优先级 | 策略 | 类型   | 协议端口         | 源地址                  |
|-------------|-----|-----|----|------|--------------|----------------------|
| Linux云服务器   | 入方向 | 1   | 允许 | IPv4 | 自定义TCP: 22   | IP地址: 192.168.0.0/24 |
| Windows云服务器 | 入方向 | 1   | 允许 | IPv4 | 自定义TCP: 3389 | IP地址: 10.10.0.0/24   |

在本地服务器远程连接云服务器上传或者下载文件（FTP）

安全组默认拒绝所有来自外部的请求，如果您需要在本地服务器远程连接云服务器上传或者下载文件，那么您需要开通FTP(20、21)端口。

表 8-16 通过任意服务器远程连接云服务器上传或者下载文件

| 方向  | 优先级 | 策略 | 类型   | 协议端口          | 源地址             |
|-----|-----|----|------|---------------|-----------------|
| 入方向 | 1   | 允许 | IPv4 | 自定义TCP: 20-21 | IP地址: 0.0.0.0/0 |

 **注意**

- 源地址设置为0.0.0.0/0表示允许所有外部IP地址远程连接云服务器上传或者下载文件，如果将当前端口暴露到公网，可能存在网络安全风险，建议您将源IP设置为已知的IP地址，配置示例请参见表8-17。
- 您需要在弹性云服务器上先安装FTP服务器程序，再查看20、21端口是否正常工作。安装FTP服务器的操作请参见[搭建FTP站点（Windows）](#)、[搭建FTP站点（Linux）](#)。

表 8-17 通过已知的服务器远程连接云服务器上传或者下载文件

| 方向  | 优先级 | 策略 | 类型   | 协议端口          | 源地址                  |
|-----|-----|----|------|---------------|----------------------|
| 入方向 | 1   | 允许 | IPv4 | 自定义TCP: 20-21 | IP地址: 192.168.0.0/24 |

在云服务器上搭建网站对外提供 Web 服务

安全组默认拒绝所有来自外部的请求，如果您在云服务器上搭建了可供外部访问的网站，则您需要在安全组入方向添加对应的规则，放通对应的端口，例如HTTP(80)、HTTPS(443)。



表 8-18 在云服务器上搭建网站对外提供 Web 服务

| 方向  | 优先级 | 策略 | 类型   | 协议端口        | 源地址             |
|-----|-----|----|------|-------------|-----------------|
| 入方向 | 1   | 允许 | IPv4 | 自定义TCP: 80  | IP地址: 0.0.0.0/0 |
| 入方向 | 1   | 允许 | IPv4 | 自定义TCP: 443 | IP地址: 0.0.0.0/0 |

使用 ping 命令验证网络连通性

ICMP协议用于网络消息的控制和传递，因此在进行一些基本测试操作之前，需要开通ICMP协议访问端口。比如，您需要在某台个人PC上使用ping命令来验证云服务器的网络连通性，则您需要在云服务器所在安全组的入方向添加以下规则，放通ICMP端口。

表 8-19 使用 ping 命令验证网络连通性

| 方向  | 优先级 | 策略 | 类型   | 协议端口     | 源地址             |
|-----|-----|----|------|----------|-----------------|
| 入方向 | 1   | 允许 | IPv4 | ICMP: 全部 | IP地址: 0.0.0.0/0 |
| 入方向 | 1   | 允许 | IPv6 | ICMP: 全部 | IP地址: ::/0      |

实现不同安全组的实例内网网络互通

同一个VPC内，位于不同安全组内的实例网络不通。如果您需要在同一个VPC内的实例之间共享数据，比如安全组sg-A内的云服务器访问安全组sg-B内的MySQL数据库，您需要通过在安全组sg-B中添加一条入方向规则，允许来自安全组sg-A内云服务器的内网请求进入。

表 8-20 实现不同安全组的实例网络互通

| 方向  | 优先级 | 策略 | 类型   | 协议端口         | 源地址       |
|-----|-----|----|------|--------------|-----------|
| 入方向 | 1   | 允许 | IPv4 | 自定义TCP: 3306 | 安全组: sg-A |

须知

如果您通过中间网络实例在不同子网的实例之间转发流量，如[安全组应用示例](#)中的“控制虚拟IP访问安全组内实例”，子网Subnet-A的ECS通过虚拟IP和子网Subnet-B的ECS互相通信。由于存在中间网络实例，此时安全组规则的源地址选择实例所在的安全组时，无法放通中间网络实例转发的流量，源地址必须设置成中间网络实例的私有IP地址或者子网网段。

云服务器提供数据库访问服务

安全组默认拒绝所有来自外部的请求，如果您在云服务器上部署了数据库服务，允许其他实例通过内网访问数据库服务，则您需要在部署数据库服务器所在的安全组内，添加加入方向规则，放通对应的端口，实现其他实例通过内网获取数据库数据的请求。常见的数据库类型及其对应的端口如下：

- MySQL(3306)
- Oracle(1521)
- MS SQL(1433)
- PostgreSQL(5432)
- Redis(6379)

本示例中源地址提供的配置仅供参考，请您根据实际需求设置源地址。

表 8-21 云服务器提供数据库访问服务

| 方向  | 优先级 | 策略 | 类型   | 协议端口             | 源地址                         | 描述                                                |
|-----|-----|----|------|------------------|-----------------------------|---------------------------------------------------|
| 入方向 | 1   | 允许 | IPv4 | 自定义<br>TCP: 3306 | 安全组：<br>sg-A                | 允许安全组sg-A内云服务器访问MySQL数据库服务。                       |
| 入方向 | 1   | 允许 | IPv4 | 自定义<br>TCP: 1521 | 安全组：<br>sg-B                | 允许安全组sg-B内云服务器访问Oracle数据库服务。                      |
| 入方向 | 1   | 允许 | IPv4 | 自定义<br>TCP: 1433 | IP地址：<br>172.16.3.2<br>1/32 | 允许私网IP地址为172.16.3.21的云服务器访问MS SQL数据库服务。           |
| 入方向 | 1   | 允许 | IPv4 | 自定义<br>TCP: 5432 | IP地址：<br>192.168.0.<br>0/24 | 允许私网IP地址属于192.168.0.0/24网段的云服务器访问PostgreSQL数据库服务。 |
| 入方向 | 1   | 允许 | IPv4 | 自定义<br>TCP: 6379 | IP地址组：<br>ipGroup-A         | 允许私网IP地址属于IP地址组ipGroup-A范围内的云服务器访问Redis数据库服务。     |

限制云服务器访问外部网站

安全组的出方向规则一般默认全部放通，默认规则如表8-23所示。如果您需要限制服务器只能访问特定网站，则按照如下要求配置：

1. 首先，您需要遵循白名单规则，在安全组出方向规则中添加指定的端口和IP地址。

表 8-22 限制云服务器访问外部网站

| 方向  | 优先级 | 策略 | 类型    | 协议端口         | 目的地址                | 描述                                                   |
|-----|-----|----|-------|--------------|---------------------|------------------------------------------------------|
| 出方向 | 1   | 允许 | IP v4 | 自定义 TCP: 80  | IP地址: 132.15.XX.XX  | 允许安全组内云服务器访问指定的外部网站，网站地址为 http://132.15.XX.XX:80。    |
| 出方向 | 1   | 允许 | IP v4 | 自定义 TCP: 443 | IP地址: 145.117.XX.XX | 允许安全组内云服务器访问指定的外部网站，网站地址为 https://145.117.XX.XX:443。 |

2. 其次，删除安全组出方向中原有放通全部流量的规则，如表8-23所示。

表 8-23 安全组默认出方向规则

| 方向  | 优先级 | 策略 | 类型    | 协议端口 | 目的地址      | 描述                                |
|-----|-----|----|-------|------|-----------|-----------------------------------|
| 出方向 | 1   | 允许 | IPv 4 | 全部   | 0.0.0.0/0 | 针对全部IPv4协议，允许安全组内的实例可访问外部任意IP和端口。 |
| 出方向 | 1   | 允许 | IPv 6 | 全部   | ::/0      | 针对全部IPv6协议，允许安全组内的实例可访问外部任意IP和端口。 |

相关链接

- [ECS常用端口](#)

8.2.4 创建安全组

操作场景

安全组是一个逻辑上的分组，为具有相同安全保护需求并相互信任的ECS实例提供访问策略，控制流入/流出ECS实例的流量。本文介绍创建安全组的操作。

常见的安全组应用场景包括：允许或者拒绝特定来源的网络流量、允许或拒绝特定协议的网络流量、屏蔽不需要开放的端口、以及配置实例的特定访问权限等。

创建ECS时必须将ECS加入一个安全组，如果此前您还未创建任何安全组，那么系统会自动为您创建[默认安全组](#)并关联至该实例。除了默认安全组，您还可以参考以下操作创建自定义安全组，并配置安全组规则控制特定流量的访问请求。了解安全组的更多信息，请参见[安全组概述](#)。

安全组预设规则说明

创建安全组的时候，您可以选择系统预设规则。安全组预设规则中预先配置了入方向规则和出方向规则，您可以根据业务选择所需的预设规则，快速完成安全组的创建。安全组预设规则的详细说明如表8-24所示。

表 8-24 预设安全组规则说明

| 预设规则     | 方向    | 类型和协议端口          | 源地址/目的地址  | 规则说明                                                             | 适用场景                                                                                                                                 |
|----------|-------|------------------|-----------|------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| 通用Web服务器 | 入方向规则 | TCP: 22 (IPv4)   | 0.0.0.0/0 | 针对TCP(IPv4)协议，允许外部所有IP访问安全组内实例的SSH(22)端口，用于远程登录Linux实例。          | <ul style="list-style-type: none"><li>外部远程登录安全组内实例（如ECS）</li><li>外部使用ping命令验证安全组内实例的网络连通性</li><li>安全组内实例用作Web服务器对外提供网站访问服务</li></ul> |
|          |       | TCP: 3389 (IPv4) | 0.0.0.0/0 | 针对TCP(IPv4)协议，允许外部所有IP访问安全组内实例的RDP(3389)端口，用于远程登录Windows实例。      |                                                                                                                                      |
|          |       | TCP: 80 (IPv4)   | 0.0.0.0/0 | 针对TCP(IPv4)协议，允许外部所有IP访问安全组内实例的HTTP(80)端口，用于通过HTTP协议访问网站。        |                                                                                                                                      |
|          |       | TCP: 443 (IPv4)  | 0.0.0.0/0 | 针对TCP(IPv4)协议，允许外部所有IP访问安全组内实例的HTTPS(443)端口，用于通过HTTPS协议访问网站。     |                                                                                                                                      |
|          |       | ICMP: 全部 (IPv4)  | 0.0.0.0/0 | 针对ICMP(IPv4)协议，允许外部所有IP访问安全组内实例的所有端口，用于外部使用ping命令验证安全组内实例的网络连通性。 |                                                                                                                                      |
|          |       | 全部 (IPv4)        | 当前安全组     | 针对全部协议，允许安全组内实例通过内网网络相互通信。                                       |                                                                                                                                      |
|          |       | 全部 (IPv6)        |           |                                                                  |                                                                                                                                      |
|          | 出方向规则 | 全部 (IPv4)        | 0.0.0.0/0 | 针对全部协议，允许所有流量从安全组内实例流出，用于访问外部。                                   |                                                                                                                                      |
|          |       | 全部 (IPv6)        | ::/0      |                                                                  |                                                                                                                                      |

| 预设规则   | 方向    | 类型和协议端口   | 源地址/目的地址  | 规则说明                                         | 适用场景                                                   |
|--------|-------|-----------|-----------|----------------------------------------------|--------------------------------------------------------|
| 开放全部端口 | 入方向规则 | 全部 (IPv4) | 0.0.0.0/0 | 针对全部协议，允许外部所有IP访问安全组内实例的所有端口，即任意流量可流入安全组内实例。 | 开放全部端口即允许任意流量出入安全组内的实例，此操作存在一定安全风险，请您谨慎选择。             |
|        |       | 全部 (IPv6) | ::/0      |                                              |                                                        |
|        |       | 全部 (IPv4) | 当前安全组     | 针对全部协议，允许安全组内实例通过内网网络相互通信。                   |                                                        |
|        |       | 全部 (IPv6) |           |                                              |                                                        |
|        | 出方向规则 | 全部 (IPv4) | 0.0.0.0/0 | 针对全部协议，允许所有流量从安全组内实例流出，用于访问外部。               |                                                        |
|        |       | 全部 (IPv6) | ::/0      |                                              |                                                        |
| 自定义    | 入方向规则 | 全部 (IPv4) | 当前安全组     | 针对全部协议，允许安全组内实例通过内网网络相互通信。                   | 该预设规则的入方向未放通任何端口，即外部任意流量均无法流入安全组内实例。请您根据业务需求自行添加安全组规则。 |
|        |       | 全部 (IPv6) |           |                                              |                                                        |
|        | 出方向规则 | 全部 (IPv4) | 0.0.0.0/0 | 针对全部协议，允许所有流量从安全组内实例流出，用于访问外部。               |                                                        |
|        |       | 全部 (IPv6) | ::/0      |                                              |                                                        |

操作步骤

1. 登录管理控制台，进入弹性云服务器的[安全组](#)列表页面。
2. 在安全组列表右上方，单击“创建安全组”。  
进入“创建安全组”页面。
3. 根据界面提示，配置安全组基本信息。

图 8-12 配置基本信息

<

创建安全组

基本信息

区域

不同区域的云服务产品之间内网互不相通；请就近选择靠近您业务的区域，可减少网络时延，提高访问速度。

名称

企业项目 ?

请选择

Q

新建企业项目

标签(可选)

如果您需要使用同一标签标识多种云资源，即所有服务均可在标签输入框下拉选择同一标签，建议在TMS中 [创建预定义标签](#)

+ 添加标签

您还可以添加20个标签。

描述(可选)

请输入

0/255

表 8-25 基本信息参数说明

| 参数 | 参数说明                                                                                                                                                            | 取值样例   |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|
| 区域 | 必选参数。<br>不同区域的云服务产品之间内网互不相通，请就近选择靠近您业务的区域，可减少网络时延，提高访问速度。<br>安全组和实例必须位于同一个区域内，才可以将实例添加到安全组内。                                                                    | 华东-上海一 |
| 名称 | 必选参数。<br>安全组的名称。要求如下： <ul style="list-style-type: none"><li>长度范围为1~64位。</li><li>名称由中文、英文字母、数字、下划线（_）、中划线（-）、点（.）组成。</li></ul> <b>说明</b><br>安全组名称创建后可以修改，建议不要重名。 | sg-AB  |

| 参数   | 参数说明                                                                                                                                                      | 取值样例                           |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|
| 企业项目 | 必选参数。<br>创建安全组时，可以将安全组加入已启用的企业项目。<br>企业项目管理提供了一种按企业项目管理云资源的方式，帮助您实现以企业项目为基本单元的资源及人员的统一管理，默认项目为default。<br>关于创建和管理企业项目的详情，请参见《 <a href="#">企业管理用户指南</a> 》。 | default                        |
| 标签   | 可选参数。<br>您可以在创建安全组的时候为安全组绑定标签，标签用于标识安全组资源，可通过标签实现对安全组资源的分类和搜索。<br>关于标签更详细的说明，请参见 <a href="#">标签概述</a> 。                                                   | “标签键”：<br>test<br>“标签值”：<br>01 |
| 描述   | 可选参数。<br>安全组的描述信息。<br>描述信息内容不能超过255个字符，且不能包含“<”和“>”。                                                                                                      | -                              |

4. 根据界面提示，配置安全组规则。
- a. 选择预设规则

图 8-13 配置规则

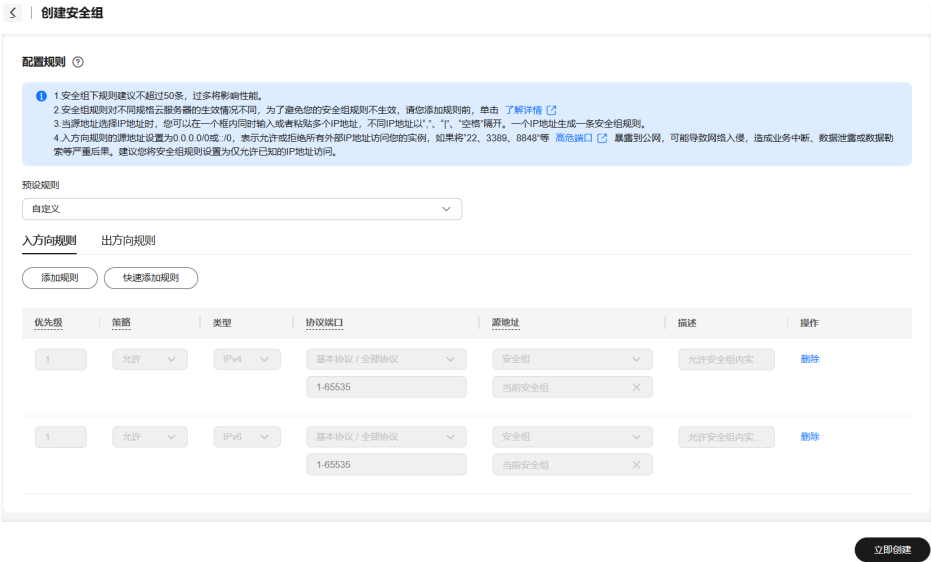


表 8-26 配置规则参数说明

| 参数   | 参数说明                                                                                                                                                                                                                                                             | 取值样例     |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| 预设规则 | <p>必选参数。</p> <p>支持三种预设规则，预先配置了不同的入方向和出方向规则，方便您快速完成安全组的创建。</p> <ul style="list-style-type: none"><li>通用Web服务器：默认配置放通22、3389、80、443端口和ICMP协议。</li><li>开放全部端口：开放全部端口有一定安全风险，请谨慎选择。</li><li>自定义：未放通任何端口，需要用户自定义安全组规则。</li></ul> <p>安全组预设规则的详细说明和适用场景，具体请参见表8-24。</p> | 通用Web服务器 |

b. 修改安全组规则

如果预设规则无法满足业务需要，您可以新增安全组规则或对预设规则进行删除、修改等操作。

须知

- 入方向规则的参数说明请参见表8-30，出方向规则的参数说明请参见表8-31。
- 入方向规则中，源地址为当前安全组的规则不支持修改，如果您删除该规则，将会导致安全组内实例的内网网络无法互通，请谨慎操作。
- 出方向规则中，目的地址为0.0.0.0/0和::/0的规则不支持修改，如果您删除该规则，将会导致安全组内实例无法访问外部网络，请谨慎操作。

5. 规则设置完成后，单击“立即创建”，完成创建。
6. 进入弹性云服务器的安全组列表页面，单击安全组名称，查看安全组详细信息。

8.2.5 配置安全组规则

操作场景

安全组规则实际是网络流量访问策略，由入方向规则和出方向规则共同组成，用来控制流入/流出安全组内ECS实例的流量。本文介绍安全组规则的添加、修改等操作。

配置安全组规则前，请您规划好安全组内实例的访问策略。常见安全组规则配置案例请参见安全组配置示例，默认安全组规则请参见默认安全组和规则，安全组常用端口请参见ECS常用端口。

常见的安全组规则应用场景如下：

- 如果实例需要对外提供服务，则应添加入方向规则，允许外部请求访问安全组内实例。



- 如果实例遇到外部网络攻击，则应添加入方向规则，拒绝有安全风险的外部请求访问安全组内实例。
- 如果实例需要访问外部网络，则应添加出方向规则，允许内部请求访问外部。
- 如果不再需要管控某些入方向或出方向流量时，可删除对应的安全组规则，以精简规则配置。
- 如果需要复制其他安全组内的规则，可使用导入/导出安全组规则或者克隆安全组功能。

使用须知

- 当您配置安全组规则前，请您务必了解该操作可能带来的影响，避免误操作造成网络中断或者引入不必要的网络安全问题。
- 安全组的规则数量有限制，请您尽量保持安全组内规则的简洁，详细约束请参见安全组的使用限制。
- 在安全组规则中放开某个端口后，您还需要确保实例内对应的端口也已经放通，安全组规则才会对实例生效，具体请参见检查安全组规则是否生效。
- 安全组入方向规则的源地址设置为0.0.0.0/0或::/0，表示允许或拒绝所有外部IP地址访问您的实例，如果将“22、3389、8848”等高危端口暴露到公网，可能导致网络入侵，造成业务中断、数据泄露或数据勒索等严重后果。建议您将安全组规则设置为仅允许已知的IP地址访问。
- 安全组规则遵循白名单原理，当在规则中没有明确定义允许或拒绝某条流量时，安全组一律拒绝该流量流入或者流出实例。
  - 在入方向中，表8-27中的入方向规则，确保安全组内实例的内网网络互通，不建议您修改或删除该安全组规则。
  - 在出方向中，表8-27中的出方向规则，允许所有流量从安全组内实例流出。如果您修改或删除该安全组规则，可能导致安全组内的实例无法访问外部，请您谨慎操作。

表 8-27 安全组规则说明

| 方向  | 策略 | 类型   | 协议端口 | 源地址/目的地址       |
|-----|----|------|------|----------------|
| 入方向 | 允许 | IPv4 | 全部   | 源地址：当前安全组      |
| 入方向 | 允许 | IPv6 | 全部   | 源地址：当前安全组      |
| 出方向 | 允许 | IPv4 | 全部   | 目的地址：0.0.0.0/0 |
| 出方向 | 允许 | IPv6 | 全部   | 目的地址：::/0      |

- 通常情况下，同一个安全组内的实例默认网络互通。当同一个安全组内实例网络不通时，可能情况如下：
  - 当实例属于同一个VPC时，请您检查入方向规则中，是否删除了同一个安全组内实例互通对应的规则，规则详情如表8-27所示。
  - 不同VPC的网络不通，所以当实例属于同一个安全组，但属于不同VPC时，网络不通。  
您可以通过VPC对等连接连通不同区域的VPC。

进入安全组规则配置页面

1. 进入[弹性云服务器列表](#)页面。
2. 在待配置安全组规则的弹性云服务器的“操作”列，单击“更多 > 网络/安全组 > 安全组规则配置”。
3. 在“安全组规则配置”页面的安全组列表中，单击待配置安全组规则的安全组“操作”列的“配置规则”。

图 8-14 配置规则



配置安全组规则

请根据业务需要，查看并执行对应的操作步骤。

添加入方向规则

1. 在“入方向规则”页签，单击“添加规则”。

弹出“添加入方向规则”对话框。
2. 根据界面提示，设置入方向规则参数。

单击⊕，可以依次增加多条入方向规则。

图 8-15 添加安全组入方向规则



表 8-28 入方向规则参数说明

| 参数   | 说明                                                                                                                                                                                                                                     | 取值样例                  |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| 优先级  | 安全组规则优先级。<br>优先级可选范围为1-100，默认值为1，即最高优先级。优先级数字越小，规则优先级级别越高。                                                                                                                                                                             | 1                     |
| 策略   | 安全组规则策略，支持的策略如下： <ul style="list-style-type: none"><li>如果“策略”设置为允许，表示允许源地址访问安全组内云服务器的指定端口。</li><li>如果“策略”设置为拒绝，表示拒绝源地址访问安全组内云服务器的指定端口。</li></ul> 安全组规则匹配流量时，首先按照优先级进行排序，其次按照策略排序，拒绝策略高于允许策略，更多信息请参见 <a href="#">流量匹配安全组规则的顺序</a> 。     | 允许                    |
| 类型   | 源地址支持的IP地址类型，如下： <ul style="list-style-type: none"><li>IPv4</li><li>IPv6</li></ul>                                                                                                                                                     | IPv4                  |
| 协议端口 | 安全组规则中用来匹配流量的网络协议类型，目前支持TCP、UDP、ICMP和GRE协议。                                                                                                                                                                                            | TCP                   |
|      | 安全组规则中用来匹配流量的目的端口，取值范围为：1～65535。<br>在入方向规则中，表示外部访问安全组内实例的指定端口。<br>端口填写支持下格式： <ul style="list-style-type: none"><li>单个端口：例如22</li><li>连续端口：例如22-30</li><li>多个端口：例如22,23-30，一次最多支持20个不连续端口组，端口组之间不能重复。</li><li>全部端口：为空或1-65535</li></ul> | 22或22-30<br>或20,22-30 |

| 参数  | 说明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 取值样例                                 |
|-----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
| 源地址 | <p>在入方向规则中，用来匹配外部请求的源地址，支持以下格式：</p> <ul style="list-style-type: none"><li>● IP地址：表示源地址为某个固定的IP地址。当源地址选择IP地址时，您可以在一个框内同时输入或者粘贴多个IP地址，不同IP地址以“,”隔开。一个IP地址生成一条安全组规则。<ul style="list-style-type: none"><li>- 单个IP地址：IP地址/掩码。<br/>单个IPv4地址示例为192.168.10.10/32。<br/>单个IPv6地址示例为2002:50::44/128。</li><li>- IP网段：IP地址/掩码。<br/>IPv4网段示例为192.168.52.0/24。<br/>IPv6网段示例为2407:c080:802:469::/64。</li><li>- 所有IP地址：<br/>0.0.0.0/0表示匹配所有IPv4地址。<br/>::/0表示匹配所有IPv6地址。</li></ul></li><li>● 安全组：表示源地址为另外一个安全组，您可以在下拉列表中，选择同一个区域内的其他安全组。当安全组A内有实例a，安全组B内有实例b，在安全组A的入方向规则中，放通源地址为安全组B的流量，则来自实例b的内网访问请求被允许进入实例a。</li><li>● IP地址组：表示源地址为一个IP地址组，IP地址组是一个或者多个IP地址的集合。您可以在下拉列表中，选择可用的IP地址组。对于安全策略相同的IP网段和IP地址，此处建议您使用IP地址组简化管理。<br/>如果没有可用的IP地址组，请您参见<a href="#">创建IP地址组</a>进行创建。</li></ul> | IP地址：<br>192.168.52.0/24,10.0.0.0/24 |
| 描述  | <p>安全组规则的描述信息，非必填项。<br/>描述信息内容不能超过255个字符，且不能包含“&lt;”和“&gt;”。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | -                                    |

3. 入方向规则设置完成后，单击“确定”。  
返回入方向规则列表，可以查看添加的入方向规则。

## 添加出方向规则

1. 在“出方向规则”页签，单击“添加规则”。  
弹出“添加出方向规则”页签。
2. 根据界面提示，设置出方向规则参数。  
单击，可以依次增加多条出方向规则。

图 8-16 添加安全组出方向规则

添加出方向规则 教我设置

安全组 sg-xxxxxx

安全组规则对不同规格云服务器的生效情况不同。为了避免您的安全组规则不生效，请您添加规则前，单击[此处](#)了解详情。  
当目的地址选择IP地址时，您可以在一个IP地址框内同时输入多个IP地址，一个IP地址对应一条安全组规则。

如您要添加多条规则，建议单击 导入规则 以进行批量导入。

| 优先级   | 策略 | 类型   | 协议端口      | 目的地址    | 描述 | 操作    |
|-------|----|------|-----------|---------|----|-------|
| 1-100 | 允许 | IPv4 | 基本协议/全部协议 | IP地址    |    | 复制 删除 |
|       |    |      | 1-65535   | 0.0.0.0 |    |       |

增加1条规则

取消 确定

表 8-29 出方向规则参数说明

| 参数   | 说明                                                                                                                                                                                                                                       | 取值样例              |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|
| 优先级  | 安全组规则优先级。<br>优先级可选范围为1-100，默认值为1，即最高优先级。优先级数字越小，规则优先级级别越高。                                                                                                                                                                               | 1                 |
| 策略   | 安全组规则策略，支持的策略如下： <ul style="list-style-type: none"><li>如果“策略”设置为允许，表示允许安全组内的云服务器访问目的地址的指定端口。</li><li>如果“策略”设置为拒绝，表示拒绝安全组内的云服务器访问目的地址的指定端口。</li></ul> 安全组规则匹配流量时，首先按照优先级进行排序，其次按照策略排序，拒绝策略高于允许策略，更多信息请参见 <a href="#">流量匹配安全组规则的顺序</a> 。   | 允许                |
| 类型   | 目的地址支持的IP地址类型，如下： <ul style="list-style-type: none"><li>IPv4</li><li>IPv6</li></ul>                                                                                                                                                      | IPv4              |
| 协议端口 | 安全组规则中用来匹配流量的网络协议类型，目前支持TCP、UDP、ICMP和GRE协议。                                                                                                                                                                                              | TCP               |
|      | 安全组规则中用来匹配流量的目的端口，取值范围为：1～65535。<br>在出方向规则中，表示安全组内实例访问外部地址的指定端口。<br>端口填写支持下格式： <ul style="list-style-type: none"><li>单个端口：例如22</li><li>连续端口：例如22-30</li><li>多个端口：例如22,23-30，一次最多支持20个不连续端口组，端口组之间不能重复。</li><li>全部端口：为空或1-65535</li></ul> | 22或22-30或20,22-30 |

| 参数   | 说明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 取值样例                                 |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
| 目的地址 | <p>在出方向规则中，用来匹配内部请求的目的地址。支持以下格式：</p> <ul style="list-style-type: none"><li>● IP地址：表示目的地址为某个固定的IP地址。当目的地址选择IP地址时，您可以在一个框内同时输入或者粘贴多个IP地址，不同IP地址以“,” 隔开。一个IP地址生成一条安全组规则。<ul style="list-style-type: none"><li>- 单个IP地址：IP地址/掩码。<br/>单个IPv4地址示例为192.168.10.10/32。<br/>单个IPv6地址示例为2002:50::44/128。</li><li>- IP网段：IP地址/掩码。<br/>IPv4网段示例为192.168.52.0/24。<br/>IPv6网段示例为2407:c080:802:469::/64。</li><li>- 所有IP地址：<br/>0.0.0.0/0表示匹配所有IPv4地址。<br/>::/0表示匹配所有IPv6地址。</li></ul></li><li>● 安全组：表示目的地址为另外一个安全组，您可以在下拉列表中，选择当前账号下，同一个区域内的其他安全组。当安全组A内有实例a，安全组B内有实例b，在安全组A的出方向规则放通目的地址为安全组B的流量，则实例a访问实例b的内网请求被允许流出。</li><li>● IP地址组：表示目的地址为一个IP地址组，IP地址组是一个或者多个IP地址的集合。您可以在下拉列表中，选择可用的IP地址组。对于安全策略相同的IP网段和IP地址，此处建议您使用IP地址组简化管理。<br/>如果没有可用的IP地址组，请您参见<a href="#">创建IP地址组</a>进行创建。</li></ul> | IP地址：<br>192.168.52.0/24,10.0.0.0/24 |
| 描述   | <p>安全组规则的描述信息，非必填项。<br/>描述信息内容不能超过255个字符，且不能包含“&lt;”和“&gt;”。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | -                                    |

3. 出方向规则设置完成后，单击“确定”。  
返回出方向规则列表，可以查看添加的出方向规则。

## 修改入方向规则

1. 选择“入方向规则”页签。  
进入安全组规则列表页面。
2. 在安全组规则列表中，单击目标规则所在行的操作列下的“修改”。
3. 根据界面提示，修改安全组规则信息。

表 8-30 入方向规则参数说明

| 参数   | 说明                                                                                                                                                                                                                                     | 取值样例                  |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| 优先级  | 安全组规则优先级。<br>优先级可选范围为1-100，默认值为1，即最高优先级。优先级数字越小，规则优先级级别越高。                                                                                                                                                                             | 1                     |
| 策略   | 安全组规则策略，支持的策略如下： <ul style="list-style-type: none"><li>如果“策略”设置为允许，表示允许源地址访问安全组内云服务器的指定端口。</li><li>如果“策略”设置为拒绝，表示拒绝源地址访问安全组内云服务器的指定端口。</li></ul> 安全组规则匹配流量时，首先按照优先级进行排序，其次按照策略排序，拒绝策略高于允许策略，更多信息请参见 <a href="#">流量匹配安全组规则的顺序</a> 。     | 允许                    |
| 类型   | 源地址支持的IP地址类型，如下： <ul style="list-style-type: none"><li>IPv4</li><li>IPv6</li></ul>                                                                                                                                                     | IPv4                  |
| 协议端口 | 安全组规则中用来匹配流量的网络协议类型，目前支持TCP、UDP、ICMP和GRE协议。                                                                                                                                                                                            | TCP                   |
|      | 安全组规则中用来匹配流量的目的端口，取值范围为：1～65535。<br>在入方向规则中，表示外部访问安全组内实例的指定端口。<br>端口填写支持下格式： <ul style="list-style-type: none"><li>单个端口：例如22</li><li>连续端口：例如22-30</li><li>多个端口：例如22,23-30，一次最多支持20个不连续端口组，端口组之间不能重复。</li><li>全部端口：为空或1-65535</li></ul> | 22或22-30<br>或20,22-30 |

| 参数  | 说明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 取值样例                                 |
|-----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
| 源地址 | <p>在入方向规则中，用来匹配外部请求的源地址，支持以下格式：</p> <ul style="list-style-type: none"><li>● IP地址：表示源地址为某个固定的IP地址。当源地址选择IP地址时，您可以在一个框内同时输入或者粘贴多个IP地址，不同IP地址以“,”隔开。一个IP地址生成一条安全组规则。<ul style="list-style-type: none"><li>- 单个IP地址：IP地址/掩码。<br/>单个IPv4地址示例为192.168.10.10/32。<br/>单个IPv6地址示例为2002:50::44/128。</li><li>- IP网段：IP地址/掩码。<br/>IPv4网段示例为192.168.52.0/24。<br/>IPv6网段示例为2407:c080:802:469::/64。</li><li>- 所有IP地址：<br/>0.0.0.0/0表示匹配所有IPv4地址。<br/>::/0表示匹配所有IPv6地址。</li></ul></li><li>● 安全组：表示源地址为另外一个安全组，您可以在下拉列表中，选择同一个区域内的其他安全组。当安全组A内有实例a，安全组B内有实例b，在安全组A的入方向规则中，放通源地址为安全组B的流量，则来自实例b的内网访问请求被允许进入实例a。</li><li>● IP地址组：表示源地址为一个IP地址组，IP地址组是一个或者多个IP地址的集合。您可以在下拉列表中，选择可用的IP地址组。对于安全策略相同的IP网段和IP地址，此处建议您使用IP地址组简化管理。<br/>如果没有可用的IP地址组，请您参见<a href="#">创建IP地址组</a>进行创建。</li></ul> | IP地址：<br>192.168.52.0/24,10.0.0.0/24 |
| 描述  | <p>安全组规则的描述信息，非必填项。<br/>描述信息内容不能超过255个字符，且不能包含“&lt;”和“&gt;”。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | -                                    |

4. 单击“确认”，完成入方向规则修改。

## 修改出方向规则

1. 选择“出方向规则”页签。  
进入安全组规则列表页面。
2. 在安全组规则列表中，单击目标规则所在行的操作列下的“修改”。
3. 根据界面提示，修改安全组规则信息。



表 8-31 出方向规则参数说明

| 参数   | 说明                                                                                                                                                                                                                                       | 取值样例                  |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| 优先级  | 安全组规则优先级。<br>优先级可选范围为1-100，默认值为1，即最高优先级。优先级数字越小，规则优先级级别越高。                                                                                                                                                                               | 1                     |
| 策略   | 安全组规则策略，支持的策略如下： <ul style="list-style-type: none"><li>如果“策略”设置为允许，表示允许安全组内的云服务器访问目的地址的指定端口。</li><li>如果“策略”设置为拒绝，表示拒绝安全组内的云服务器访问目的地址的指定端口。</li></ul> 安全组规则匹配流量时，首先按照优先级进行排序，其次按照策略排序，拒绝策略高于允许策略，更多信息请参见 <a href="#">流量匹配安全组规则的顺序</a> 。   | 允许                    |
| 类型   | 目的地址支持的IP地址类型，如下： <ul style="list-style-type: none"><li>IPv4</li><li>IPv6</li></ul>                                                                                                                                                      | IPv4                  |
| 协议端口 | 安全组规则中用来匹配流量的网络协议类型，目前支持TCP、UDP、ICMP和GRE协议。                                                                                                                                                                                              | TCP                   |
|      | 安全组规则中用来匹配流量的目的端口，取值范围为：1～65535。<br>在出方向规则中，表示安全组内实例访问外部地址的指定端口。<br>端口填写支持下格式： <ul style="list-style-type: none"><li>单个端口：例如22</li><li>连续端口：例如22-30</li><li>多个端口：例如22,23-30，一次最多支持20个不连续端口组，端口组之间不能重复。</li><li>全部端口：为空或1-65535</li></ul> | 22或22-30<br>或20,22-30 |

| 参数   | 说明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 取值样例                                 |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
| 目的地址 | <p>在出方向规则中，用来匹配内部请求的目的地址。支持以下格式：</p> <ul style="list-style-type: none"><li>● IP地址：表示目的地址为某个固定的IP地址。当目的地址选择IP地址时，您可以在一个框内同时输入或者粘贴多个IP地址，不同IP地址以“,” 隔开。一个IP地址生成一条安全组规则。<ul style="list-style-type: none"><li>- 单个IP地址：IP地址/掩码。<br/>单个IPv4地址示例为192.168.10.10/32。<br/>单个IPv6地址示例为2002:50::44/128。</li><li>- IP网段：IP地址/掩码。<br/>IPv4网段示例为192.168.52.0/24。<br/>IPv6网段示例为2407:c080:802:469::/64。</li><li>- 所有IP地址：<br/>0.0.0.0/0表示匹配所有IPv4地址。<br/>::/0表示匹配所有IPv6地址。</li></ul></li><li>● 安全组：表示目的地址为另外一个安全组，您可以在下拉列表中，选择当前账号下，同一个区域内的其他安全组。当安全组A内有实例a，安全组B内有实例b，在安全组A的出方向规则放通目的地址为安全组B的流量，则实例a访问实例b的内网请求被允许流出。</li><li>● IP地址组：表示目的地址为一个IP地址组，IP地址组是一个或者多个IP地址的集合。您可以在下拉列表中，选择可用的IP地址组。对于安全策略相同的IP网段和IP地址，此处建议您使用IP地址组简化管理。<br/>如果没有可用的IP地址组，请您参见<a href="#">创建IP地址组</a>进行创建。</li></ul> | IP地址：<br>192.168.52.0/24,10.0.0.0/24 |
| 描述   | <p>安全组规则的描述信息，非必填项。<br/>描述信息内容不能超过255个字符，且不能包含“&lt;”和“&gt;”。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | -                                    |

4. 单击“确认”，完成出方向规则修改。

## 检查安全组规则是否生效

在安全组规则中放开某个端口后，您还需要确保实例内对应的端口也已经放通，安全组规则才会对实例生效。

假设您在某台ECS上部署了网站，希望用户能通过HTTP(80)端口访问到您的网站，则您需要先在ECS所在安全组的入方向中，添加[表8-32](#)中的规则，放通HTTP(80)端口。

表 8-32 安全组规则示例

| 方向  | 优先级 | 策略 | 类型   | 协议端口       | 源地址             |
|-----|-----|----|------|------------|-----------------|
| 入方向 | 1   | 允许 | IPv4 | 自定义TCP: 80 | IP地址: 0.0.0.0/0 |

安全组规则添加完成后，您需要执行以下操作，检查云服务器内端口开放情况，并验证配置是否生效。

1. 登录云服务器，检查云服务器端口开放情况。
- 检查Linux云服务器端口

执行以下命令，查看TCP 80端口是否被监听。

**netstat -an | grep 80**

若回显类似图8-17，说明80端口已开通。

图 8-17 Linux TCP 80 端口验证结果



- 检查Windows云服务器端口
- i. 通过“开始菜单 > 运行 > cmd”，打开命令执行窗口。

ii. 执行以下命令，查看TCP 80端口是否被监听。

**netstat -an | findstr 80**

若回显类似图8-18，说明TCP 80端口已开通。

图 8-18 Windows TCP 80 端口验证结果



2. 打开浏览器，在地址栏里输入“http://云服务器的弹性公网IP地址”。
- 如果访问成功，说明安全组规则已经生效。

相关链接

- 为什么配置的安全组规则不生效？

8.2.6 更改安全组

操作场景

ECS实例关联安全组时，是将ECS实例的网卡关联到安全组。关联安全组后，实例的流入和流出流量受安全组规则限制。您可以根据业务需要，随时调整ECS实例的网卡与安全组的关联关系。多个安全组的生效规则请参考[安全组及规则的工作原理](#)。

本节操作介绍当弹性云服务器的网卡需要变更所属安全组时的操作步骤。

支持对一台或多台弹性云服务器进行更改安全组的操作：

- 更改安全组（单台云服务器）**：适用于对弹性云服务器指定网卡的安全组进行操作。
- 更改安全组（多台云服务器）**：适用于对弹性云服务器主网卡的安全组进行操作。

约束限制

- 更改安全组操作会覆盖弹性云服务器原有的安全组设置。
- 使用多个安全组可能会影响弹性云服务器的网络性能，建议您选择安全组的数量不多于5个。
- 批量更改安全组仅支持对弹性云服务器主网卡的安全组进行操作。

更改安全组（单台云服务器）

1. 登录管理控制台。
  2. 单击“”，选择“计算 > 弹性云服务器”。
  3. 在弹性云服务器列表中，单击“操作”列下的“更多 > 网络/安全组 > 更改安全组”。
- 系统弹窗显示“更改安全组”页面。

图 8-19 更改安全组



4. 根据界面提示，在下拉列表中选择待更改安全组的网卡，并重新选择安全组。  
您可以同时勾选多个安全组，安全组序号按照勾选顺序依次排序，安全组序号越小，表示优先级越高。在已选安全组列表的“操作”列，单击“上移”或“下移”调整安全组的优先级。  
如需创建新的安全组，请单击“新建安全组”。

说明

使用多个安全组可能会影响弹性云服务器的网络性能，建议您选择安全组的数量不多于5个。

5. 单击“确定”。

更改安全组（多台云服务器）

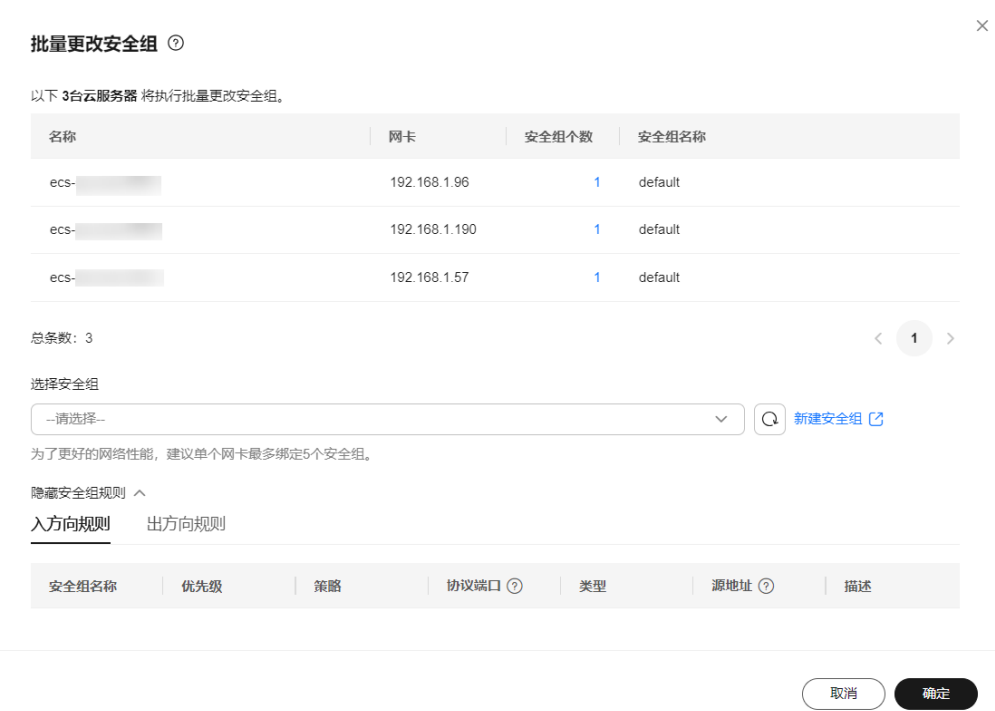
1. 登录管理控制台。

2. 单击“”，选择“计算 > 弹性云服务器”。

3. 在弹性云服务器列表中，勾选待更改安全组的云服务器。

4. 单击列表上方的“更多 > 安全组 > 更改安全组”。
- 进入“批量更改安全组”页面。

图 8-20 批量更改安全组



5. 根据界面提示，在下拉列表中选择待更改的安全组，为所选云服务器变更主网卡所属的安全组。
- 您可以同时勾选多个安全组，安全组序号按照勾选顺序依次排序，安全组序号越小，表示优先级越高。在已选安全组列表的“操作列”，单击“上移”或“下移”调整安全组的优先级。
- 如需创建新的安全组，请单击“新建安全组”。

说明

使用多个安全组可能会影响弹性云服务器的网络性能，建议您选择安全组的数量不多于5个。

6. 单击“确定”。

查看 ECS 实例关联的安全组信息

1. 进入[弹性云服务器列表](#)页面。

2. 单击待查询安全组规则的弹性云服务器的实例名称，进入实例详情页。

3. 单击“安全组”页签。

4. 在下拉框中选择网卡，查看网卡关联的全部安全组和安全组规则。

## 8.2.7 加入安全组

### 操作场景

ECS实例关联安全组时，是将ECS实例的网卡关联到安全组。关联安全组后，实例的流入和流出流量受安全组规则限制。您可以根据业务需要，随时调整ECS实例的网卡与安全组的关联关系。多个安全组的生效规则请参考[安全组及规则的工作原理](#)。

本节操作介绍当弹性云服务器的网卡需要增加所属安全组时的操作步骤。

支持对一台或多台弹性云服务器进行增加所属安全组的操作：

- **加入安全组（单台云服务器）**：适用于对弹性云服务器指定网卡的安全组进行操作。
- **加入安全组（多台云服务器）**：适用于对弹性云服务器主网卡的安全组进行操作。

### 约束限制

- 加入安全组操作对弹性云服务器原有所属安全组设置无影响。
- 使用多个安全组可能会影响弹性云服务器的网络性能，建议您为弹性云服务器设置的安全组总数量不多于5个。
- 批量加入安全组仅支持对弹性云服务器主网卡的安全组进行操作。

### 加入安全组（单台云服务器）

1. 登录管理控制台。
  2. 单击“”，选择“计算 > 弹性云服务器”。
  3. 在弹性云服务器列表中，单击“操作”列下的“更多 > 网络/安全组 > 加入安全组”。
- 系统弹窗显示“加入安全组”页面。

图 8-21 加入安全组

加入安全组

以下 1 台云服务器 将执行加入安全组。

| 名称   | 网卡           | 安全组个数 | 安全组名称   |
|------|--------------|-------|---------|
| ecs- | 192.168.1.96 | 1     | default |

总条数: 1

网卡

192.168.1.96 (主)

选择安全组

- 请选择 -

新建安全组

为了更好的网络性能，建议单个网卡最多绑定5个安全组。若选择的安全组已经关联目标实例，则不会重复加入。

选择新安全组的插入位置

置于顶部

置于底部

隐藏安全组规则

入方向规则

出方向规则

| 安全组名称 | 优先级 | 策略 | 协议端口 | 类型 | 源地址 | 描述 |
|-------|-----|----|------|----|-----|----|
|-------|-----|----|------|----|-----|----|

取消

确定

4. 根据界面提示，为所选云服务器的指定网卡增加一个或多个安全组。
- a. 在网卡下拉列表中选择待增加安全组的网卡。

b. （可选）如需创建新的安全组，请单击“新建安全组”。

c. 勾选所有待新增安全组。  
新增多个安全组时，安全组序号按照勾选顺序依次排序，安全组序号越小，表示优先级越高。

d. 选择新增安全组的插入位置。  
“置于顶部”表示将所有新增安全组插入安全组列表首位，优先级最高。  
“置于底部”表示将所有新增安全组插入安全组列表末尾，优先级最低。

说明

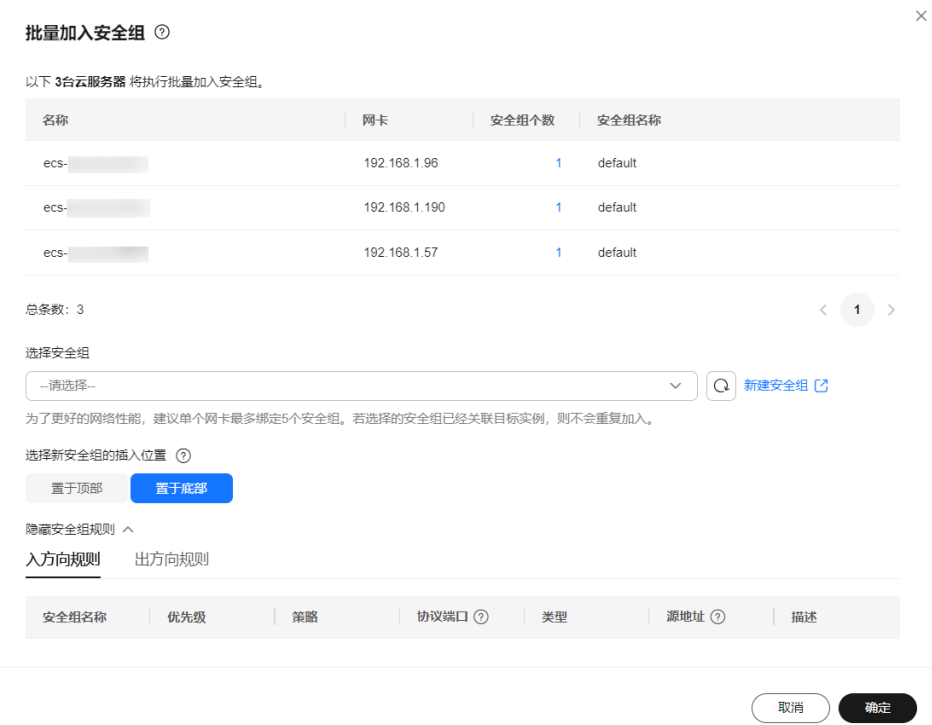
- 若选择的安全组已经关联目标实例，则不会重复加入，且在安全组列表中的优先级保持不变。
- 使用多个安全组可能会影响弹性云服务器的网络性能，建议您为弹性云服务器设置的安全组总数量不多于5个。

5. 单击“确定”。

加入安全组（多台云服务器）

1. 登录管理控制台。
2. 单击“”，选择“计算 > 弹性云服务器”。
3. 在弹性云服务器列表中，勾选待增加安全组的云服务器。
4. 单击列表上方的“更多 > 安全组 > 加入安全组”。
- 进入“批量加入安全组”页面。

图 8-22 批量加入安全组



5. 根据界面提示，为所选云服务器的主网卡增加一个或多个安全组。
- a. （可选）如需创建新的安全组，请单击“新建安全组”。
- b. 勾选所有待新增安全组。  
新增多个安全组时，安全组序号按照勾选顺序进行排序，安全组序号越小，表示优先级越高。
- c. 选择新增安全组的插入位置。  
“置于顶部”表示将所有新增安全组插入安全组列表首位，优先级最高。  
“置于底部”表示将所有新增安全组插入安全组列表末尾，优先级最低。

说明

- 若选择的安全组已经关联目标实例，则不会重复加入，且在安全组列表中的优先级保持不变。
  - 使用多个安全组可能会影响弹性云服务器的网络性能，建议您为弹性云服务器设置的安全组总数量不多于5个。
6. 单击“确定”。

查看 ECS 实例关联的安全组信息

1. 进入弹性云服务器列表页面。
2. 单击待查询安全组规则的弹性云服务器的实例名称，进入实例详情页。
3. 单击“安全组”页签。
4. 在下拉框中选择网卡，查看网卡关联的全部安全组和安全组规则。



## 8.2.8 移出安全组

### 操作场景

ECS实例关联安全组时，是将ECS实例的网卡关联到安全组。关联安全组后，实例的流入和流出流量受安全组规则限制。您可以根据业务需要，随时调整ECS实例的网卡与安全组的关联关系。多个安全组的生效规则请参考[安全组及规则的工作原理](#)。

本节操作介绍当弹性云服务器的网卡需要移出所属安全组时的操作步骤。

支持对一台或多台弹性云服务器进行移出所属安全组的操作：

- **移出安全组（单台云服务器）**：适用于对弹性云服务器指定网卡的安全组进行操作。
- **移出安全组（多台云服务器）**：适用于对弹性云服务器主网卡的安全组进行操作。

### 约束限制

- 使用多个安全组可能会影响弹性云服务器的网络性能，建议您为弹性云服务器设置的安全组总数量不多于5个。
- 批量移出安全组仅支持对弹性云服务器主网卡的安全组进行操作。
- 实例必须加入一个安全组，如果您需要更换安全组，可以先将实例加入新的安全组，然后再将实例从原有安全组移出。

### 移出安全组（单台云服务器）

1. 登录管理控制台。
2. 单击“”，选择“计算 > 弹性云服务器”。
3. 在弹性云服务器列表中，单击“操作”列下的“更多 > 网络/安全组 > 移出安全组”。

系统弹窗显示“移出安全组”页面。

图 8-23 移出安全组



4. 根据界面提示，在下拉列表中选择待移出安全组的网卡，并选择安全组。  
您可以同时勾选多个安全组，且安全组包含在弹性云服务器所属安全组内，否则移出操作无效。
5. 单击“确定”。

移出安全组（多台云服务器）

1. 登录管理控制台。
2. 单击“≡”，选择“计算 > 弹性云服务器”。
3. 在弹性云服务器列表中，勾选待移出安全组的云服务器。
4. 单击列表上方的“更多 > 安全组 > 移出安全组”。  
进入“批量移出安全组”页面。

图 8-24 批量移出安全组



5. 根据界面提示，在下拉列表中选择待移出的安全组，为所选云服务器移出主网卡所属的安全组。  
您可以同时勾选多个安全组，且安全组包含在弹性云服务器所属安全组内，否则移出操作无效。
6. 单击“确定”。

查看 ECS 实例关联的安全组信息

1. 进入[弹性云服务器列表](#)页面。
2. 单击待查询安全组规则的弹性云服务器的实例名称，进入实例详情页。
3. 单击“安全组”页签。
4. 在下拉框中选择网卡，查看网卡关联的全部安全组和安全组规则。

8.3 主机安全

什么是主机安全

企业主机安全服务（Host Security Service，HSS）是以工作负载为中心的安全产品，集成了主机安全、容器安全和网页防篡改，旨在解决混合云、多云数据中心基础架构中服务器工作负载的独特保护要求。HSS通过对主机、容器进行系统完整性的保护、应用程序控制、行为监控和基于主机的入侵防御等，保护工作负载免受攻击。

主机安全是旨在增强主机整体安全性的服务，通过主机管理、风险防御、入侵检测、安全运营、网页防篡改功能等功能，能够全面识别并管理主机内的信息资产，实时监测主机中潜在风险，并阻止非法入侵行为，帮助企业构建服务器安全体系，降低服务器所面临的安全威胁。主机安全工作原理请参考[什么是企业主机安全](#)。

使用主机安全需要在云服务器中安装Agent。安装Agent后，您的云服务器将受到HSS云端防护中心全方位的安全保障，在安全控制台可视化界面上，您可以统一查看并管理同一区域内所有主机的防护状态和主机安全风险。

## 计费说明

- 企业主机安全提供包年/包月、按需计费两种计费模式，以满足不同场景下的用户需求。详细介绍请参见[HSS计费模式概述](#)。
- 当ECS关机后，HSS按需计费的防护配额将停止计费。

## 怎样开启主机安全服务

针对新创建的云服务器和已有的云服务器提供不同的开启方式。

### 新创建云服务器开启主机安全

购买弹性云服务器，选择部分操作系统的公共镜像时，系统推荐您配套使用主机安全服务（Host Security Service, HSS）。

开启“主机安全”需要设置“安全防护”参数：

- 免费试用一个月主机安全基础防护：开启后，免费体验HSS基础版30天，为您的主机提供操作系统漏洞检测、弱口令检测、暴力破解检测等功能。

#### 说明

主机安全基础防护免费使用期限结束后，该防护配额将自动释放，停止相应的实时防护能力。

如您需要保留或升级原有安全防护能力，建议您购买高阶防护。详细情况，请参见主机安全的[免费试用HSS基础版到期后怎么办？](#)。

购买弹性云服务器时，默认设置该选项。

- 购买高阶防护：高阶防护支持基础版、企业版、旗舰版和网页防篡改版，需付费使用。

购买后您可以在主机安全服务控制台切换不同版本。各版本之间的差异请参考[服务版本差异](#)。

- 不使用安全防护：若您不需要进行安全防护，可选择此选项。

选择主机安全后系统自动安装主机安全Agent，开启账号防御，启用主机安全服务的功能。

若基础版或企业版不满足要求，您可以[购买其他版本配额](#)，在主机安全服务控制台[切换不同版本](#)，获取更高级的防护，且不需要重新安装Agent。

图 8-25 开通主机安全



### 已创建的云服务器开启主机安全

对于已经创建完成的弹性云服务器，可能由于创建时尚未支持主机安全服务或未设置“安全防护”参数而暂未开启主机安全服务。开启主机安全的流程如下：

表 8-33 开启主机安全流程说明

| 序号 | 步骤            | 说明                                                                                                                                                                                                                                                                   |
|----|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | 购买防护配额        | 企业主机安全HSS提供基础版、专业版、企业版、旗舰版、网页防篡改版和容器版供您选择，每个版本支持的功能特性存在差异，您需要根据对主机的防护需求，购买对应的防护版本。HSS各版本的区别请参见 <a href="#">产品功能</a> 。                                                                                                                                                |
| 2  | 为华为云主机安装Agent | Agent是企业主机安全提供的一款软件，安装在云服务器上，用于与企业主机安全的云端防护中心进行数据交互，实现对主机的安全检测和防护。安装Agent后，您才能使用企业主机安全。                                                                                                                                                                              |
| 3  | 开启防护          | 完成购买防护配额、安装Agent后，HSS还未对云服务器进行防护，您需要为云服务器开启防护。                                                                                                                                                                                                                       |
| 4  | (可选) 开启告警通知   | 默认情况下，HSS在防护主机/容器过程中发现的安全风险展示在管理控制台，您需要登录管理控制台查看。如果您需要及时了解主机/容器的安全风险，可以开启告警通知，开启后，HSS会将安全风险通过短信或邮件的方式发送给您。                                                                                                                                                           |
| 5  | (可选) 常用安全配置   | 您可以根据实际业务需求，配置如下云服务器安全保护项，提升云服务器安全性： <ul style="list-style-type: none"><li>● 主机登录保护：配置常用登录地、常用登录IP、SSH登录IP白名单，对使用非常用登录地、登录IP进行登录的行为进行告警，拒绝白名单以外的IP登录。</li><li>● 双因子认证：双因素身份验证机制，结合短信/邮箱验证码，对登录云服务器行为进行二次认证。</li><li>● 恶意程序隔离查杀：对识别出的后门、木马、蠕虫等恶意程序进行自动隔离查杀。</li></ul> |

怎样查看主机安全状态

- 在云服务器的列表页，您可以查看当前区域下的云服务器的主机安全状态。
- 建议您定期查看主机防护状态，及时处理主机中存在的安全风险，避免威胁入侵造成您的财产损失或防护中断导致您的主机暴露在风险中。
1. 登录管理控制台。
  2. 单击“”，选择“安全与合规 > 主机安全服务”。
  3. 在“资产管理 > 主机管理”的“云服务器”页签，查看服务器的防护状态。

图 8-26 查看主机安全状态



表 8-34 状态说明

| 参数      | 说明                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Agent状态 | <ul style="list-style-type: none"><li>未安装：未安装Agent，或Agent已安装但未成功启动。</li><li>在线：Agent运行正常。</li><li>离线：Agent已经安装完成，但当前Agent与HSS远端防护中心的连接中断，无法通信。此时，HSS无法提供安全防护功能。<br/>单击“离线”，您可以查看Agent不在线的华为云主机列表，并查看“离线原因”。解决办法请参见<a href="#">Agent状态异常应如何处理？</a></li><li>安装失败：在尝试安装过程中遇到错误或问题，导致安装未能完成。<br/>单击安装失败状态旁边的<sup>?</sup>查看具体原因，解决办法请参见<a href="#">Agent安装失败应如何处理？</a></li><li>安装中：当前正在进行Agent安装。</li></ul> |
| 风险状态    | <p>服务器当前的风险情况（数据存在24小时延迟）。</p> <ul style="list-style-type: none"><li>有风险：主机存在风险。<br/>鼠标悬停在风险分布图标上方，可查看风险分布详情；单击数值可跳转至风险详情页面查看详细信息。</li><li>无风险：主机暂未发现风险。</li><li>未检测：主机未开启防护。</li></ul>                                                                                                                                                                                                                |
| 防护状态    | <ul style="list-style-type: none"><li>防护中：HSS为该服务器提供全面的安全防护。</li><li>未防护：目标未开启防护。<br/>Agent安装完成后，单击“操作”列“开启防护”可以开启防护。</li><li>防护中断：HSS防护服务器中断，未正常防护服务器，可能是服务器关机、Agent离线或Agent被卸载导致防护中断。<br/>您可以将鼠标悬停在“防护中断”旁边的<sup>?</sup>查看具体原因。</li></ul>                                                                                                                                                            |

更多关于主机安全服务的使用，请参见[主机安全服务](#)。

常见问题

Agent安装失败常见问题请参见[Agent安装失败应如何处理？](#)

8.4 云堡垒机

什么是云堡垒机

云堡垒机（Cloud Bastion Host，CBH）是华为云的一款4A统一安全管控平台，为企业提供集中的账号（Account）、授权（Authorization）、认证（Authentication）和审计（Audit）管理服务。

云堡垒机提供云计算安全管控的系统 and 组件，包含部门、用户、资源、策略、运维、审计等功能模块，集单点登录、统一资产管理、多终端访问协议、文件传输、会话协同等功能于一体。通过统一运维登录入口，基于协议正向代理技术和远程访问隔离技术，实现对服务器、云主机、数据库、应用系统等云上资源的集中管理和运维审计。

快速配置云堡垒机

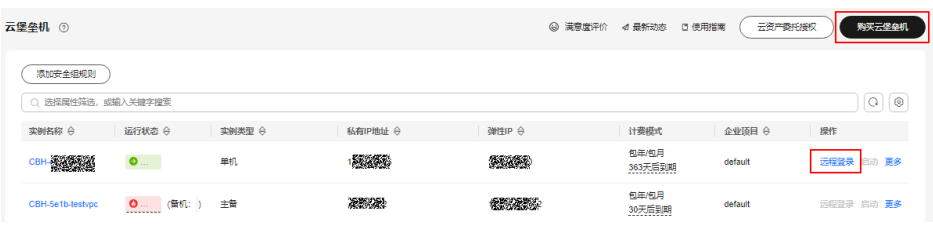
配置后可以实时收集和监控网络环境中每个组成部分的系统状态、安全事件和网络活动，保障网络和数据不受来自外部或内部用户的入侵和破坏，便于集中报警、及时处理及审计定责。

- 步骤1 [登录管理控制台](#)。
- 步骤2 在控制台页面中选择“安全与合规 > 云堡垒机 CBH”，进入服务在右上角单击[购买云堡垒机](#)，购买后在实例“操作”列单击“远程登录”进入云堡垒机登录页面。

说明

- 首次以系统管理员admin登录系统，登录密码为购买实例时配置密码。系统管理员admin是系统默认用户，即第一个可登录用户，拥有系统最高操作权限，且无法删除和更改权限配置。
- 系统所有用户首次登录系统后，请按照提示修改密码和绑定手机号码。

图 8-27 登录云堡垒机



- 步骤3 登录云堡垒机系统后，选择“用户 > 用户管理”，右上角单击“新建”，根据实际需求和界面提示[创建运维用户](#)。

说明

- 角色划分用户系统操作权限，默认有系统管理员、策略管理员、审计管理员和运维员四种角色。admin可以[自定义角色](#)，分配系统操作权限。
- “登录名”在整个CBH系统是唯一的，不能重复。
- 创建用户成功后，可通过修改用户配置，配置用户登录云堡垒机系统的[多因子认证](#)。

图 8-28 新建运维用户

新建用户

\* 登录名

长度1-64个字符，以字母或者数字开头，不支持的字符:\[]:|!+,\*?<>@\*以及空格

\* 认证类型

本地

\* 密码

\* 确认密码

长度为8-32个字符，密码只能包含大写字母、小写字母、数字和特殊字符(!@\$%^\_-=+[]:;./?~#\*)且至少包含四种字符中的三种，不能包含用户名或倒序用户名

\* 姓名

长度为1-255个汉字或字符，允许输入汉字、字母、数字、“@”、“.”、“\_”或“-”

\* 手机

手机号十分重要，请输入正确的手机号码。  
若是国际号码，请输入：“+”+国家代码+手机号码

确定

取消

**步骤4** 运维用户创建成功后，选择“资源 > 主机管理”，右上角单击“新建”，[配置主机](#)基本信息和网络参数。

说明

- “主机地址”为主机与云堡垒机网络通畅的IP地址，可选择主机的EIP地址或私有IP地址，建议优先选择可用的私有IP地址。
- 增强版支持以主机方式运维数据库，支持四种数据库类型MySQL、SQL Server、Oracle和DB2。
- 应用发布资源是通过Windows远程访问应用实现运维，需先[配置应用发布服务器](#)。
- 创建资源成功后，需添加资源账户才能登录资源运维。资源账户的登录方式可选择以下几种：

自动登录：系统纳管资源账户名和密码，再次登录资源时无需输入账户名和密码。

手动登录：自动生成一个Empty账户。登录资源时，需手工输入资源账户名和密码进行登录。

提权登录：当用户登录提权资源账户时，自动切换身份到特权帐号。



图 8-29 新建主机

新建主机

\* 主机名称

长度为1-128个汉字或字符

\* 协议类型

请选择协议类型

\* 主机地址

请输入有效的IP地址或域名

\* 端口

请输入1-65535之间的有效数字

系统类型

请选择系统类型

更多选项

☒ 文件管理

☒ X11转发

☒ 上行剪切板

☒ 下行剪切板

\* 所属部门

总部

标签

取消

下一步

- 步骤5 单击“下一步”，配置运维主机账户信息，单击“确认”完成配置。
- 步骤6 运维用户和主机资源创建成功后，选择“策略 > 访问控制策略”，右上角单击“新建”配置访问控制权限。

说明

- 访问控制策略用于关联用户和资源，并赋予用户访问和操作资源的具体权限。CBH系统用户被赋予了资源访问控制权限，才能运维资源。
- IP限制”是设置用户本地IP地址，用于限制或允许该IP地址的用户访问资源。

图 8-30 新建控制策略

新建访问控制策略

\* 策略名称

长度1-64个汉字或字符，允许输入英文字母、数字、或“-”

有效期

生效时间

失效时间

文件传输

☒ 上传

☒ 下载

更多选项

☒ 文件管理

☒ 上行剪切板

☒ 下行剪切板

☐ 显示水印

登录时段限制

☒ 允许登录

☐ 禁止登录

周一

周二

周三

周四

周五

周六

周日

0

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

IP限制

黑名单

取消

下一步

**步骤7** 单击“下一步”，关联运维用户和主机资源，单击“确认”完成配置。

**步骤8** 访问控制策略配置成功后，使用运维用户登录云堡垒机系统，选择“运维 > 主机运维”。

**步骤9** 选择目标主机资源，单击“登录”，[登录主机资源](#)进行运维操作。

#### 说明

- SSH、TELNET和Rlogin协议类型主机资源，可使用SSH客户端运维资源。
- FTP、SFTP和SCP协议类型主机资源，需使用FTP/SFTP/SCP客户端运维资源。
- MySQL、SQL Server、Oracle和DB2协议类型的主机资源，需提前配置SSO单点登录工具和数据库管理工具。通过SSO单点登录工具调用数据库客户端，实现SSO单点客户端运维资源。
- SSH、RDP、VNC和TELNET协议类型主机资源，支持直接通过Web浏览器运维；应用发布资源仅能通过Web浏览器远程访问进行运维。

----结束

## 8.5 管理项目和企业项目

### 创建项目并授权

- **创建项目**

进入管理控制台页面，单击右上方的用户名，在下拉列表中选择“统一身份认证”，进入统一身份认证服务页面。选择左侧导航中的“项目”，单击“创建项目”，选择区域并输入项目名称。

- **授权**

通过为用户组授予权限（包括资源集和操作集），实现项目 and 用户组的关联。将用户加入到用户组，使用户具有用户组中的权限，从而精确地控制用户所能访问的项目，以及所能操作的资源。具体步骤如下：

- 在“用户组”页面，选择目标用户组，单击操作列的“授权”，进入“选择策略”环节。
- 在列表中勾选策略，完成用户组的“策略”设置。
- 单击“下一步”，将“选择授权范围方案”设置为“指定区域项目资源”。
- 在区域项目列表中，选择具体的项目，单击“确定”。完成对用户组的授权。
- 在“用户”页面，选择目标用户，单击操作列的“授权”，进入“选择授权方式”环节。
- 勾选“继承所选用户组的策略”，并在“已有用户组”列表中勾选[步骤1](#)中进行了策略授权的用户组。
- 单击“确定”，将用户加入到用户组。

### 创建企业项目并授权

- **创建企业项目**

进入管理控制台页面，单击右上方的“企业 > 企业管理”，进入企业项目管理页面。单击“创建企业项目”，完成企业项目的创建。

## 说明

开通了企业项目的客户，或者权限为企业主账号的客户才可以看到控制台页面上方的“企业”入口。如需使用该功能，请联系客服申请开通。

- **授权**

通过为企业项目添加用户组，并设置策略，实现企业项目和用户组的关联。将用户加入到用户组，使用户具有用户组中的权限，从而精确地控制用户所能访问的项目，以及所能操作的资源。具体步骤如下：

- a. 在企业项目管理页面，单击企业项目的名称，进入企业项目详情页面。
- b. 在“权限管理”页签，单击“用户组授权”，系统跳转至IAM的用户组页面，在“用户组”页签中为企业项目关联用户组并授权。

详细操作，请参见[创建用户组并授权](#)。

- **关联资源与企业项目**

企业项目可以将云资源按企业项目统一管理。

- 购买弹性云服务器时选择企业项目

在购买页面，“企业项目”下拉列表中选择目标企业项目，实现资源与企业项目关联。

- 资源迁入

对于账号下的存量弹性云服务器，您可以在“企业项目管理”页面将资源迁入目标企业项目。

“default”为默认企业项目，账号下原有资源和未选择企业项目的资源均在默认企业项目内。

更多信息，请参阅《[企业管理用户指南](#)》。

## 8.6 敏感操作保护

### 操作场景

弹性云服务器支持敏感操作保护，在控制台进行敏感操作时，需要输入一种能证明身份的凭证，身份验证通过后方可进行相关操作。为了账号安全，建议开启操作保护功能，该功能对账号以及账号下的用户都生效。

目前支持：关机、重启、删除、重置密码、卸载磁盘、解绑弹性公网IP。

### 约束与限制

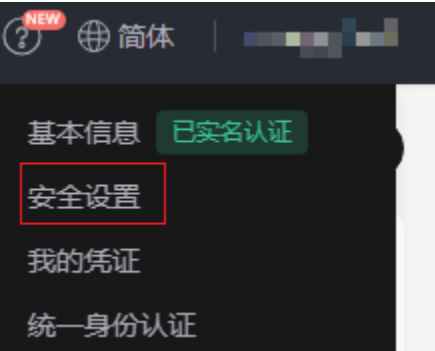
敏感操作保护仅影响通过管理控制台进行操作的用户，对通过“华为云”手机应用程序进行操作的用户无影响。

### 开启操作保护

操作保护默认关闭，您可以参考以下步骤开启操作保护。

1. 登录管理控制台。
2. 在“控制台”页面，鼠标移动至右上方的用户名，在下拉列表中选择“安全设置”。

图 8-31 安全设置



3. 在“安全设置”页面中，选择“敏感操作 > 操作保护 > 立即启用”。

图 8-32 敏感操作



4. 在“操作保护设置”页面中，选择“开启”，单击“确定”后，开启操作保护。开启后，您以及账号中的IAM用户进行敏感操作时，例如删除弹性云服务器资源，需要输入验证码进行验证，避免误操作带来的风险和损失。

说明

- 用户如果进行敏感操作，将进入“操作保护”页面，选择认证方式，包括邮箱、手机和虚拟MFA三种认证方式。
  - 如果用户只绑定了手机，则认证方式只能选择手机。
  - 如果用户只绑定了邮箱，则认证方式只能选择邮件。
  - 如果用户未绑定邮箱、手机和虚拟MFA，进行敏感操作时，华为云将提示用户绑定邮箱、手机或虚拟MFA。
- 如需修改验证手机、邮箱、虚拟MFA设备，请在[基本信息](#)中修改。

操作保护验证

当您已经开启操作保护，在进行敏感操作时，系统会先进行操作保护验证：

- 若您绑定了邮箱，需输入邮箱验证码。
- 若您绑定了手机，需输入手机验证码。
- 若您绑定了虚拟MFA，需输入MFA设备上的6位动态验证码。

当尝试关机弹性云服务器时，弹出以下验证框，选择一种验证方式：

图 8-33 操作确认

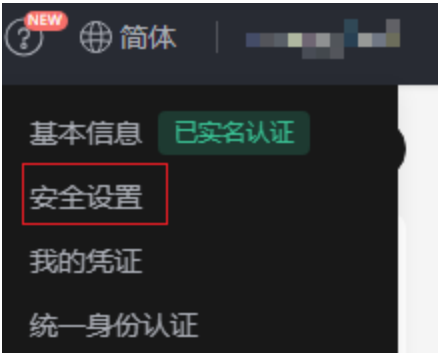


关闭操作保护

如需关闭操作保护，请参考以下步骤操作。

- 1. 登录管理控制台。
- 2. 在“控制台”页面，鼠标移动至右上方的用户名，在下拉列表中选择“安全设置”。

图 8-34 安全设置



- 3. 在“安全设置”页面中，选择“敏感操作 > 操作保护 > 立即修改”。

图 8-35 修改敏感操作



4. 在“操作保护设置”页面中，选择“关闭”，单击“确定”后，关闭操作保护。

## 相关链接

- 华为云密钥管理服务（Key management Service，简称KMS）[如何绑定虚拟MFA设备？](#)
- [如何获取MFA验证码？](#)

# 9 备份管理

---

## 9.1 云备份概述

### 什么是云备份

云备份（Cloud Backup and Recovery, CBR）可以为云服务器、云硬盘提供简单易用的备份服务，当发生病毒入侵、人为误删除、软硬件故障等事件时，可将数据恢复到任意备份点。

云备份保障用户数据的安全性和正确性，确保业务安全。

### 视频帮助

[什么是云备份？三分钟带你快速了解什么是云备份服务。](#)

### 备份、快照、镜像有什么区别？

备份分为云服务器备份和云硬盘备份。

镜像分为系统盘镜像、数据盘镜像、整机镜像。

| 备份类型   | 备份对象                   | 适用场景                                                                                                                                                                                                                                                                                                                    | 区别和优势                                                                              | 备份方法     | 恢复方法                                                                                                     |
|--------|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|----------|----------------------------------------------------------------------------------------------------------|
| 云服务器备份 | 弹性云服务器中的所有云硬盘（系统盘和数据盘） | <ul style="list-style-type: none"><li>● <b>云服务器受到攻击或病毒入侵</b><br/>通过云服务器备份，可立即恢复到最近一次没有受黑客攻击或病毒入侵的备份时间点。</li><li>● <b>数据被误删</b><br/>通过云服务器备份，可立即恢复到删除前的备份时间点，找回被删除的数据。</li><li>● <b>应用程序更新出错</b><br/>通过云服务器备份，可立即恢复到应用程序更新前的备份时间点，使系统正常运行。</li><li>● <b>云服务器宕机</b><br/>通过云服务器备份，可立即恢复到宕机之前的备份时间点，使云服务器能再次正常启动。</li></ul> | 备份的同一个云服务器下的所有云硬盘数据具有一致性，即同时对所有云硬盘进行备份，不存在因备份创建时间差带来的数据不一致问题。<br>且云备份支持根据备份策略自动备份。 | 创建云服务器备份 | <ul style="list-style-type: none"><li>● 使用云服务器备份恢复数据（恢复至原服务器）</li><li>● 使用云服务器备份恢复数据（创建新的云服务器）</li></ul> |



| 备份类型  | 备份对象                 | 适用场景                                                                                                                                                                                                                                    | 区别和优势                                                          | 备份方法                    | 恢复方法                                                                                                                                |
|-------|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| 云硬盘备份 | 指定的单个或多个云硬盘（系统盘或数据盘） | <ul style="list-style-type: none"><li>● <b>系统盘没有个人数据，因而只需要对部分的数据盘进行备份</b><br/>当云硬盘出现故障或云硬盘中的数据发生逻辑错误时（如误删数据、遭遇黑客攻击或病毒危害等），可快速恢复数据。</li><li>● <b>备份作为基线数据</b><br/>设置备份策略，根据策略自动对云硬盘进行数据备份，通过定期创建的备份作为基线数据，用来创建新的云硬盘或者恢复数据到云硬盘。</li></ul> | 备份数据则存储在对象存储（OBS）中，可以实现在云硬盘存储损坏情况下的数据恢复<br><br>保证数据安全的同时降低备份成本 | <a href="#">创建云硬盘备份</a> | <ul style="list-style-type: none"><li>● <a href="#">使用云硬盘备份恢复数据（恢复至原磁盘）</a></li><li>● <a href="#">使用云硬盘备份恢复数据（创建新的磁盘）</a></li></ul> |

| 备份类型 | 备份对象                 | 适用场景                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 区别和优势                                                                                                                                        | 备份方法                 | 恢复方法                     |
|------|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|----------------------|--------------------------|
| 快照   | 指定的单个或多个云硬盘（系统盘或数据盘） | <ul style="list-style-type: none"><li>● <b>日常备份数据</b><br/>通过对云硬盘定期创建快照，实现数据的日常备份，可以应对由于误操作、病毒以及黑客攻击等导致数据丢失或不一致的情况。</li><li>● <b>快速恢复数据</b><br/>应用软件升级或业务数据迁移等重大操作前，您可以创建一份或多份快照，一旦升级或迁移过程中出现问题，可以通过快照及时将业务恢复到快照创建点的数据状态。<br/>例如，当由于云服务器A的系统盘A发生故障而无法正常开机时，此时您可以使用系统盘A已有的快照新建一块云硬盘B并挂载至正常运行的云服务器B上，从而云服务器B能够通过云硬盘B读取原系统盘A的数据。</li><li>● <b>快速部署多个业务</b><br/>通过同一个快照可以快速创建出多个具有相同数据的云硬盘，从而可以同时为多种业务提供数据资源。例如数据挖掘、报表查询和开发测试等业务。<br/>这种方式既保护了原始数据，又能通过快照创建的新云硬盘快速部署其他业务，满足企业对业务数据的多元化需求。</li></ul> <p><b>说明</b></p> <ul style="list-style-type: none"><li>● 只支持回滚快照数据至原云硬盘，不支持快照回滚到其他云硬盘。</li><li>● 重装操作系统或切换操作系统后，系统盘快照会自动删除；数据盘快照不受影响，可以照常使用。</li></ul> | <ul style="list-style-type: none"><li>● 快照数据与云硬盘数据存储在 一起，可以支持快速备份和恢复</li><li>● 快速保存指定时刻云硬盘的数据，同时还可以通过快照创建新的云硬盘，这样云硬盘在初始状态就具有快照中的数据</li></ul> | <a href="#">创建快照</a> | <a href="#">使用快照回滚数据</a> |

| 备份类型  | 备份对象   | 适用场景                                                                                                                                                                                                                            | 区别和优势                                            | 备份方法                    | 恢复方法                                                                                                                             |
|-------|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------|-------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| 系统盘镜像 | 系统盘    | <ul style="list-style-type: none"><li>● <b>快速恢复系统</b><br/>更换操作系统、应用软件升级或业务数据迁移等重大操作前，将系统盘创建成系统盘镜像，一旦迁移过程中出现问题，可以通过系统盘镜像切换操作系统，或重新创建新的云服务器。</li><li>● <b>快速部署多个业务</b><br/>通过同一个系统盘镜像可以快速创建出多个具有相同操作系统的云服务器，从而快速部署多个业务。</li></ul> | 系统盘镜像可以实现在云服务器操作系统损坏情况下快速切换至损坏前的操作系统。            | <a href="#">创建系统盘镜像</a> | <ul style="list-style-type: none"><li>● <a href="#">使用系统盘镜像切换故障云服务器的操作系统</a></li><li>● <a href="#">使用系统盘镜像创建新的云服务器</a></li></ul> |
| 数据盘镜像 | 指定的数据盘 | <b>快速复制数据</b><br>通过同一个数据盘镜像可以快速创建出多个具有相同数据的云硬盘，再将新创建的云硬盘挂载到其他服务器上，从而可以同时为多种业务提供数据资源。                                                                                                                                            | 数据盘镜像可以复制全盘的数据并创建新的云硬盘挂载到其他服务器上，实现云服务器数据盘的复制和共享。 | <a href="#">创建数据盘镜像</a> | <a href="#">使用数据盘镜像创建数据盘</a>                                                                                                     |

| 备份类型 | 备份对象                   | 适用场景                                                                                                                                                                                                                                     | 区别和优势            | 备份方法          | 恢复方法                  |
|------|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|---------------|-----------------------|
| 整机镜像 | 弹性云服务器中的所有云硬盘（系统盘和数据盘） | <ul style="list-style-type: none"><li>● <b>快速恢复系统</b><br/>更换操作系统、应用软件升级或业务数据迁移等重大操作前，将云服务器的系统盘和数据盘创建成整机镜像，一旦迁移过程中出现问题，可以通过整机镜像切换操作系统，或重新创建新的云服务器。</li><li>● <b>快速部署多个业务</b><br/>通过同一个整机镜像可以快速创建出多个具有相同操作系统和数据的云服务器，从而快速部署多个业务。</li></ul> | 通过整机镜像实现业务的整理迁移。 | <b>创建整机镜像</b> | <b>使用整机镜像创建新的云服务器</b> |

云备份产品架构

云备份由备份、存储库和策略组成。

- **备份：**  
备份即一个备份对象执行一次备份任务产生的备份数据，包括备份对象恢复所需要的全部数据。
  - 云服务器备份：云服务器备份提供对弹性云服务器和裸金属服务器的基于多云硬盘一致性快照技术的数据保护。同时，未部署数据库等应用的服务器产生的备份为服务器备份，部署数据库等应用的服务器产生的备份为数据库服务器备份。
  - 云硬盘备份：云硬盘备份提供对云硬盘的基于快照技术的数据保护。
- **存储库**  
云备份使用存储库来存放备份。创建备份前，需要先创建至少一个存储库，并将服务器或磁盘绑定至存储库。服务器或磁盘产生的备份则会存放至绑定的存储库中。  
存储库分为备份存储库和复制存储库两种。备份存储库用于存放备份对象产生的备份，复制存储库用于存放复制操作产生的备份。  
不同类型的备份对象产生的备份需要存放在不同类型的存储库中。
- **策略**  
策略分为备份策略和复制策略。
  - 备份策略：需要对备份对象执行自动备份操作时，可以设置备份策略。通过在策略中设置备份任务执行的时间、周期以及备份数据的保留规则，将备份存储库绑定到备份策略，可以为存储库执行自动备份。
  - 复制策略：需要对备份或存储库执行自动复制操作时，可以设置复制策略。通过在策略中设置复制任务执行的时间、周期以及备份数据的保留规则，将备份存储库绑定到复制策略，可以为存储库执行自动复制。复制产生的备份需要存放在复制存储库中。

备份机制

首次备份为全量备份，备份云服务器/磁盘已使用空间。

示例：某磁盘大小为100GB，已使用空间为40GB，则备份的是40GB的已使用空间。

后续备份均为增量备份，备份上次备份后变化的数据，缩短备份时长、节约备份空间。

删除备份时，仅删除不被其他备份依赖的数据块，不影响使用其他备份进行恢复。无论是全量还是增量备份，都可以快速、方便地将数据恢复至备份所在时刻的状态。

云备份会在备份过程中自动创建快照并且为每个磁盘保留最新的快照。如果该磁盘已备份，再次备份后会自动将旧快照删除，保留最新的快照。

云备份通过云服务器/磁盘与对象存储服务的结合，将数据备份到对象存储中，高度保障用户的备份数据安全。

备份的方式及适用场景

云备份提供两种配置方式，一次性备份和周期性备份。一次性备份是指用户手动创建的一次性备份任务。周期性备份是指用户通过创建备份策略并绑定存储库的方式创建的周期性备份任务。

表 9-1 备份的方式及适用场景

| 对比项  | 一次性备份                                                  | 周期性备份                                        |
|------|--------------------------------------------------------|----------------------------------------------|
| 备份策略 | 不需要                                                    | 需要                                           |
| 备份次数 | 手动执行一次性备份                                              | 根据备份策略进行周期性备份                                |
| 备份名称 | 支持自定义，默认为“manualbk_xxxx”                               | 系统自动生成，默认为“autobk_xxxx”                      |
| 备份方式 | 默认首次全量备份，后续增量备份                                        | 默认首次全量备份，后续增量备份                              |
| 适用场景 | 资源进行操作系统补丁安装、升级，应用升级等操作之前，以便安装或者升级失败之后，能够快速恢复到变更之前的状态。 | 资源的日常备份保护，以便发生不可预见的故障而造成数据丢失时，能够使用邻近的备份进行恢复。 |

9.2 备份弹性云服务器

操作场景

云备份提供申请即用的备份服务，使您的数据更加安全可靠。例如，当云服务器或磁盘出现故障或者人为错误导致数据误删时，可以自助快速恢复数据。本节操作介绍备份云服务器和云硬盘的操作步骤。

您可以通过[云备份产品架构](#)、[备份机制（全量备份和增量备份）](#)、[备份的方式及适用场景](#)了解更多产品详情。

目前弹性云服务器备份可以通过“云服务器备份”和“云硬盘备份”功能实现：

- 云服务器备份（推荐）：如果是对弹性云服务器中的所有云硬盘（系统盘和数据盘）进行备份，推荐使用云服务器备份功能，同时对所有云硬盘进行备份，避免因备份创建时间差带来的数据不一致问题。
- 云硬盘备份：如果对指定的单个或多个云硬盘（系统盘或数据盘）进行备份，推荐使用云硬盘备份功能，在保证数据安全的同时降低备份成本。

## 云服务器备份操作步骤

1. 登录管理控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”。
4. 在弹性云服务器的“操作”列下，单击“更多 > 磁盘/备份 > 创建云服务器备份”。
- 如果云服务器已绑定存储库，则根据界面提示，配置备份信息。
  - 云服务器列表：默认已勾选待备份的云服务器
  - 名称：用户自定义云备份名称。
  - 描述：输入待创建的备份的描述。
  - 执行全量备份：勾选后，系统会为绑定的云服务器执行全量备份，备份所占存储容量也会相应增加。
- 如果云服务器未绑定存储库，请先购买存储库，配置备份信息。  
详细操作请参考[购买云服务器备份存储库](#)。
5. 单击“确定”。系统会自动为云服务器创建备份。  
在“备份副本”页签，产生的备份的“备份状态”为“可用”时，表示备份任务执行成功。  
云服务器备份在执行备份过程中，若备份进度已经超过10%可重启云服务器。但为了保证数据完整性，建议备份完成后再次执行重启。  
执行备份成功后，后续可以使用云服务器备份恢复服务器数据或创建镜像，详情请参见[使用云服务器备份恢复数据](#)和[使用备份创建镜像](#)。

## 云硬盘备份操作步骤

1. 登录管理控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”。
4. 在弹性云服务器的“操作”列下，单击“更多 > 磁盘/备份 > 创建云硬盘备份”。
- 如果云服务器已绑定存储库，则根据界面提示，配置备份信息。
  - 服务器列表：默认已勾选待备份的云服务器，单击  查看云服务器挂载的磁盘。并选择待备份的磁盘。
  - 名称：用户自定义云备份名称。

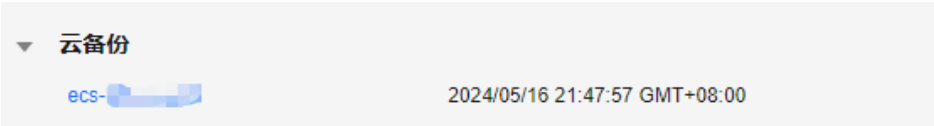
- 描述：输入待创建的备份的描述。
  - 执行全量备份：勾选后，系统会为绑定的磁盘执行全量备份，备份所占存储容量也会相应增加。
- 如果云服务器未绑定存储库，请先购买存储库，再配置备份信息。  
详细操作请参考[购买云硬盘备份存储库](#)。
5. 单击“确定”。系统会自动为磁盘创建备份。
- 根据界面提示，跳转至云备份控制台的“备份副本”页签，当产生的备份的“备份状态”为“可用”时，表示备份任务执行成功。
- 如果在备份过程中对磁盘的数据进行删除等操作，被删除的文件可能不会被备份成功。为了保证数据完整性，建议备份完成后对数据再进行操作。
- 执行备份成功后，后续可以使用云硬盘备份恢复磁盘数据，详情请参见[使用云硬盘备份恢复数据](#)。

后续操作

备份成功后，您可以查看云服务器的云备份信息以及备份详情。

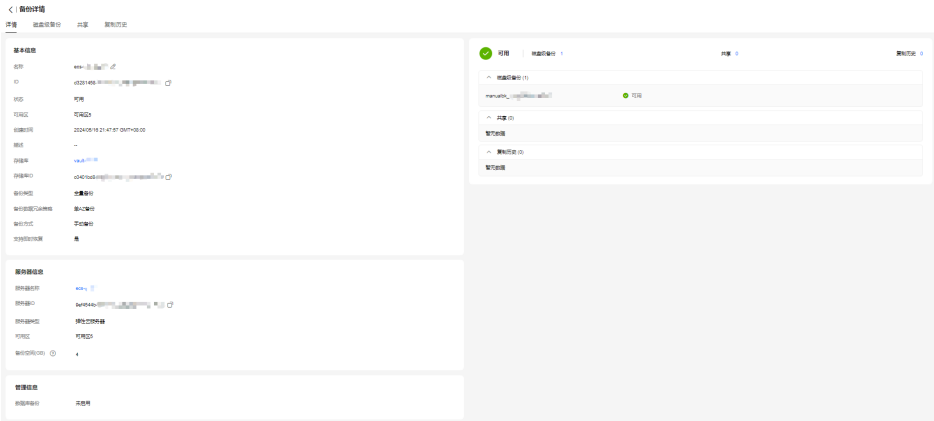
1. 登录管理控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。
3. 单击“≡”，选择“计算 > 弹性云服务器”。
4. 在云服务器列表中，单击待查看的弹性云服务器名称，进入详情页。
5. 查看备份详情。
  - a. 在云服务器详情页“基本信息”页签右下角的“云备份”区域，可以看到具体的备份及时间信息。

图 9-1 云备份区域



- b. 单击具体的备份，跳转至云备份控制台的“备份详情”页面。

图 9-2 备份详情



通过备份详情，可以查看备份的名称、ID、状态、可用区、创建时间、存储库等信息，还可以查看备份相关的云服务器信息。

更多关于备份详情的详细操作，请参见[备份管理](#)。

6. 在云服务器详情页，单击“云备份”页签，查看云备份的基本信息和付费信息。

图 9-3 云备份信息





# 10 密码和密钥对管理

## 10.1 重置 ECS 密码

### 10.1.1 密码使用场景介绍

密码用于登录弹性云服务器，如果您在购买弹性云服务器时选择的“登录凭证”方式为“密码”，即可通过用户名和密码进行登录。弹性云服务器系统密码涉及到客户重要的私人信息，提醒您妥善保管密码。

如果您遇到以下情况，可以通过重置密码的方式修改或获取弹性云服务器的密码。

- 忘记密码
- 密码过期
- 购买弹性云服务器时选择的“登录凭证”方式为“创建后设置”
- 通过“快速购买”方式购买弹性云服务器，该场景下“登录凭证”默认设置为“创建后设置”
- Windows

弹性云服务器的重置密码场景如表10-1所示。

表 10-1 重置密码场景

| 操作场景                             | 前提条件                                                                                                                             |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| 在控制台重置ECS密码                      | 已安装重置密码插件。<br>说明 <ul style="list-style-type: none"><li>• 使用公共镜像的弹性云服务器默认已安装一键式重置密码插件。</li><li>• Windows/Linux操作系统的云服务器</li></ul> |
| 未安装重置密码插件且忘记密码时，如何重置密码(Windows)? | 未安装重置密码插件。                                                                                                                       |
| 未安装重置密码插件且忘记密码时，如何重置密码(Linux)?   | 未安装重置密码插件。                                                                                                                       |

背景知识

弹性云服务器的密码规则包含创建ECS和重置密码两个场景，如表10-2所示。

表 10-2 密码设置规则

| 密码设置规则 | 创建ECS时                                                                                                                                            | 重置密码时                                                                                                                                                                                                                                                                           |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 长度规则   | 密码长度范围为8到26位。                                                                                                                                     | 密码长度范围为8到26位。                                                                                                                                                                                                                                                                   |
| 字符规则   | 密码至少包含支持的4种字符中的3种。                                                                                                                                | 密码至少包含支持的4种字符中的3种。                                                                                                                                                                                                                                                              |
| 安全性规则  | <ul style="list-style-type: none"><li>密码不能包含用户名或用户名的逆序。</li><li>Windows操作系统的云服务器，不能包含用户名中超过两个连续字符的部分。</li></ul>                                   | <ul style="list-style-type: none"><li>密码不能包含用户名或用户名的逆序。</li><li>Windows操作系统的云服务器，不能包含用户名中超过两个连续字符的部分。</li></ul>                                                                                                                                                                 |
| 其他约束   | 无                                                                                                                                                 | Windows操作系统的云服务器，不能以“/”为密码首字符。                                                                                                                                                                                                                                                  |
| 支持的字符  | 大写字母                                                                                                                                              | 大写字母                                                                                                                                                                                                                                                                            |
|        | 小写字母                                                                                                                                              | 小写字母                                                                                                                                                                                                                                                                            |
|        | 数字                                                                                                                                                | 数字                                                                                                                                                                                                                                                                              |
|        | <ul style="list-style-type: none"><li>Linux操作系统ECS支持的特殊字符：!@\$%^-_=+[{ } ;,:./~#*</li><li>Windows操作系统ECS支持的特殊字符：!@\$%^-_=+[{ } ;,:./~#*</li></ul> | <ul style="list-style-type: none"><li>在线修改密码方式：<br/>Linux操作系统ECS支持的特殊字符：!@\$%^-_=+[{ } ;,:./~#*<br/>Windows操作系统ECS支持的特殊字符：!@\$%^-_=+[{ } ;,:./~#*</li><li>离线修改密码方式：<br/>Linux操作系统ECS支持的特殊字符：!@\$%^-_=+[{ } ;,:./~#*<br/>Windows操作系统ECS支持的特殊字符：!@\$%^-_=+[{ } ;,:./~#*</li></ul> |

10.1.2 在控制台重置 ECS 密码

操作场景

如果在创建弹性云服务器时未设置密码，或密码丢失、过期，可以参考本节操作重置密码。

ECS支持在线重置密码和离线重置密码两种方式。

约束与限制

表 10-3 重置密码约束与限制

| 约束项   | 在线重置密码                                                                                                                       | 离线重置密码                                                                                                                                                                                                                                               |
|-------|------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 服务依赖  | 依赖云运维中心（Cloud Operations Center，简称COC），需开通并授权COC服务。<br><br>对于IAM用户，需额外配置COC资源操作类权限，详细内容，请参见 <a href="#">配置ECS自助运维自定义策略</a> 。 | 不涉及                                                                                                                                                                                                                                                  |
| 插件依赖  | 依赖UniAgent。UniAgent是统一数据采集Agent，支持脚本下发和执行。<br><br>若ECS未安装UniAgent，则无法在线重置密码，详细内容，请参见 <a href="#">为ECS安装UniAgent</a> 。        | 依赖一键式重置密码插件。<br><br>使用公共镜像创建的弹性云服务器默认已安装一键式重置密码插件。<br><br>若ECS未安装一键式重置密码插件或插件已失效，则无法离线重置密码，详细内容，请参见 <a href="#">安装单台ECS的一键式重置密码插件（单台操作）</a> 。                                                                                                        |
| 支持的状态 | 运行中                                                                                                                          | <ul style="list-style-type: none"><li>运行中</li><li>关机</li></ul>                                                                                                                                                                                       |
| 生效时间  | 修改后立即生效                                                                                                                      | 新密码的生效时间与ECS的状态有关： <ul style="list-style-type: none"><li>运行中：ECS重启后生效。<br/><b>须知</b><ul style="list-style-type: none"><li>离线重置密码时如果选择“自动重启”，可能会导致数据丢失，建议您先关机再重置密码。</li><li>重启ECS，可能会导致业务中断，建议您选择非业务高峰期进行操作。</li></ul></li><li>关机：ECS开机后生效。</li></ul> |

## 前提条件

- 密码丢失或过期前，已安装密码重置插件。
  - 公共镜像创建的弹性云服务器默认已安装一键式重置密码插件。
  - 私有镜像创建的云服务器且未安装密码重置插件，可参考[未安装重置密码插件且忘记密码时，如何重置密码\(Windows\)?](#)和[未安装重置密码插件且忘记密码时，如何重置密码\(Linux\)?](#)。
- 请勿删除重置密码进程CloudResetPwdAgent和CloudResetPwdUpdateAgent，否则，会导致一键式重装密码功能不可用。
- 使用SUSE 11 SP4镜像创建的弹性云服务器，内存需要大于等于4GiB时才能支持一键式重置密码功能。
- 弹性云服务器使用的VPC网络DHCP不能禁用。
- 弹性云服务器网络正常通行。
- 请确保一键式重置密码插件未被安全软件（如火绒软件等）阻止运行，否则重置密码功能无法使用。

## 操作步骤

重置密码包含在线重置密码和离线重置密码两种方式，您可以根据业务需要进行选择。

- 在线重置密码：依赖COC服务和AOM的UniAgent，修改立即生效，无需重启ECS。
- 离线重置密码：不依赖COC服务和AOM的UniAgent，ECS重启或开机后生效。

## 在线重置密码

1. 登录管理控制台，进入[弹性云服务器](#)列表页面。
2. 在ECS列表中，勾选待重置密码的ECS。

### 说明

如果勾选多台ECS，则可以为多台ECS重置密码，修改后多台ECS的密码相同。

3. 单击列表上方的“重置密码”。
4. 选择“在线重置密码”页签。
5. （可选）在“开通云运维中心并添加权限”页面，阅读服务声明并勾选后，单击“开通并授权”。

若当前账号未开通并授权COC服务，则会显示该页面。

6. 根据界面提示信息，完成相关参数配置。

### 须知

在线重置密码功能依赖UniAgent，如果提示未安装UniAgent或者安装失败，请参考[为ECS安装UniAgent](#)进行安装，否则无法在线重置密码。

图 10-1 在线重置密码

重置密码

在线重置密码

离线重置密码

1

如果执行过程中遇到权限问题，请确认是否已授予对应权限。[查看权限](#)

1

在线重置密码无需重启云服务器，修改后即可生效，您可使用新密码进行登录。

以下 1 台云服务器 将执行在线重置密码

| 名称   | ID | 操作系统  |
|------|----|-------|
| ECS- |    | Linux |

总条数: 1 < 1 >

登录名

root

新密码

确认密码

表 10-4 在线重置密码参数配置

| 参数  | 说明                                                                                                                             |
|-----|--------------------------------------------------------------------------------------------------------------------------------|
| 登录名 | ECS的登录名，系统默认设置，无需填写。 <ul style="list-style-type: none"><li>Linux操作系统ECS登录名：root</li><li>Windows操作系统登录名：Administrator</li></ul> |

| 参数   | 说明                                                                                                                                                                                                                                                                                                                                                                          |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 新密码  | 修改后的密码。<br>密码规则： <ul style="list-style-type: none"><li>8~26个字符。</li><li>密码至少包含以下4种字符中的3种：<ul style="list-style-type: none"><li>大写字母</li><li>小写字母</li><li>数字</li><li>特殊字符</li></ul>Linux操作系统ECS支持的特殊字符：@%-_+=[]:./^,{}?<br/>Windows操作系统ECS支持的特殊字符：\$@%-_+=[]:./,?<li>密码不能包含用户名或用户名的逆序。</li><li>Windows系统密码不能包含用户名中超过两个连续字符的部分。</li><li>Windows系统密码不能以“/”为首字符。</li></li></ul> |
| 确认密码 | 确认密码，需要与“新密码”保持一致。                                                                                                                                                                                                                                                                                                                                                          |

7. 单击“确定”，完成ECS的重置密码。

离线重置密码

1. 登录管理控制台，进入弹性云服务器列表页面。  
2. 在ECS列表中，勾选待重置密码的ECS。

说明

- 如果勾选多台ECS，则可以为多台ECS重置密码，修改后多台ECS的密码相同。
3. 单击列表上方的“重置密码”。
4. 选择“离线重置密码”页签，根据界面提示信息，完成相关参数配置。

图 10-2 离线重置密码

重置密码

在线重置密码

离线重置密码

弹性云服务器重启后，新密码自动生效。

以下 1 台云服务器 将执行离线重置密码

| 名称               | ID          | 登录名  |
|------------------|-------------|------|
| ecs- <div></div> | <div></div> | root |

总条数: 1 < 1 >

登录名

root

新密码

确认密码

☐ 运行中的云服务器，需重启后新密码才可生效

自动重启可能会导致数据丢失，建议您先关机再重置密码。

表 10-5 离线重置密码参数配置

| 参数  | 说明                                                                                                                             |
|-----|--------------------------------------------------------------------------------------------------------------------------------|
| 登录名 | ECS的登录名，系统默认设置，无需填写。 <ul style="list-style-type: none"><li>Linux操作系统ECS登录名：root</li><li>Windows操作系统登录名：Administrator</li></ul> |

| 参数   | 说明                                                                                                                                                                                                                                                                                                                                                                       |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 新密码  | 修改后的密码。<br>密码规则： <ul style="list-style-type: none"><li>8~26个字符。</li><li>密码至少包含以下4种字符中的3种：<ul style="list-style-type: none"><li>大写字母</li><li>小写字母</li><li>数字</li><li>特殊字符</li></ul>Linux操作系统ECS支持的特殊字符：!@%-_+=+[]:./?<br/>Windows操作系统ECS支持的特殊字符：!@%-_+=+[]:./?</li><li>密码不能包含用户名或用户名的逆序。</li><li>Windows系统密码不能包含用户名中超过两个连续字符的部分。</li><li>Windows系统密码不能以“/”为首字符。</li></ul> |
| 确认密码 | 确认密码，需要与“新密码”保持一致。                                                                                                                                                                                                                                                                                                                                                       |

5. 勾选“运行中的云服务器，需重启后新密码才可生效”。
- 当ECS处于“运行中”时，会显示该参数，且必须勾选，否则无法重置密码。
6. 单击“确定”，完成ECS的重置密码。

相关链接

- 一键重置密码后无法使用新密码登录弹性云服务器
- 业务端口被一键式重置密码插件占用
- ECS主机上执行UniAgent安装命令，下载安装脚本失败

10.2 管理 ECS 一键式重置密码插件

10.2.1 获取 ECS 一键式重置密码插件

操作场景

若弹性云服务器“重置密码”失败，有可能是由于未安装一键式重置密码插件或插件失效，您可以参考本章节获取一键式重置密码插件并校验其完整性。



## 获取并校验一键式重置密码插件完整性（Linux）

1. 以root用户登录弹性云服务器。
2. 执行以下命令，下载一键式重置密码插件及sha256校验码。  
您可以根据弹性云服务器所在区域、操作系统是32位还是64位，参考[表10-6](#)选择对应的下载地址。

### 说明

为了便于您通过内网下载一键式重置密码插件，我们提供了不同区域的下载地址，不同区域、相同操作系统的插件相同。

如果[表10-6](#)中不包含您的弹性云服务器所在区域，请您为弹性云服务器绑定EIP，然后选择就近区域进行下载。

绑定EIP的详细操作，请参见[绑定弹性公网IP](#)。

以“华北-北京一”区域的32位x86操作系统为例：

```
wget https://cn-north-1-cloud-reset-pwd.obs.cn-north-1.myhuaweicloud.com/linux/32/reset_pwd_agent/CloudResetPwdAgent.zip
```

```
wget https://cn-north-1-cloud-reset-pwd.obs.cn-north-1.myhuaweicloud.com/linux/32/reset_pwd_agent/CloudResetPwdAgent.zip.sha256
```

3. 执行以下命令，获取本地一键式重置密码插件的Hash值。  
**sha256sum {软件包本地目录}/CloudResetPwdAgent.zip**  
{软件包本地目录}：请根据实际下载目录进行替换，例如/root。
4. 将步骤2获取的sha256 Hash值和步骤3获取的Hash值进行比较。
  - 一致：通过校验。
  - 不一致：请重新下载对应版本的一键式重置密码插件，重复步骤2~步骤4进行校验。

## 获取并校验一键式重置密码插件完整性（Windows）

1. 登录弹性云服务器。
2. 下载一键式重置密码插件及sha256校验码。  
您可以根据弹性云服务器所在区域，参考[表10-6](#)选择对应的下载地址。

### 说明

如果[表10-6](#)中不包含您的弹性云服务器所在区域，请您为弹性云服务器绑定EIP，然后选择就近区域进行下载。

绑定EIP的详细操作，请参见[绑定弹性公网IP](#)。

3. 以管理员权限打开cmd，执行以下命令，获取本地一键式重置密码插件的Hash值。  
**certutil -hashfile {软件包本地目录}\CloudResetPwdAgent.zip SHA256**  
{软件包本地目录}：请根据实际下载目录进行替换。
4. 将步骤2获取的sha256 Hash值和步骤3获取的Hash值进行比较。
  - 一致：通过校验。
  - 不一致：请重新下载对应版本的一键式重置密码插件，重复步骤2~步骤4进行校验。

一键式重置密码插件及 sha256 校验码下载地址

表 10-6 一键式重置密码插件下载地址

| 区域     | 操作系统          | 文件名                    | 下载地址                                                                                                                           |
|--------|---------------|------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| 华北-北京一 | Linux(x86_32) | CloudResetPwdAgent.zip | https://cn-north-1-cloud-reset-pwd.obs.cn-north-1.myhuaweicloud.com/linux/32/reset_pwd_agent/CloudResetPwdAgent.zip            |
|        |               | sha256校验码              | https://cn-north-1-cloud-reset-pwd.obs.cn-north-1.myhuaweicloud.com/linux/32/reset_pwd_agent/CloudResetPwdAgent.zip.sha256     |
|        | Linux(x86_64) | CloudResetPwdAgent.zip | https://cn-north-1-cloud-reset-pwd.obs.cn-north-1.myhuaweicloud.com/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip            |
|        |               | sha256校验码              | https://cn-north-1-cloud-reset-pwd.obs.cn-north-1.myhuaweicloud.com/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip.sha256     |
|        | Linux(armv64) | CloudResetPwdAgent.zip | https://cn-north-1-cloud-reset-pwd.obs.cn-north-1.myhuaweicloud.com/arm/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip        |
|        |               | sha256校验码              | https://cn-north-1-cloud-reset-pwd.obs.cn-north-1.myhuaweicloud.com/arm/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip.sha256 |
| 华北-北京四 | Windows       | CloudResetPwdAgent.zip | https://cn-north-1-cloud-reset-pwd.obs.cn-north-1.myhuaweicloud.com/windows/reset_pwd_agent/CloudResetPwdAgent.zip             |
|        |               | sha256校验码              | https://cn-north-1-cloud-reset-pwd.obs.cn-north-1.myhuaweicloud.com/windows/reset_pwd_agent/CloudResetPwdAgent.zip.sha256      |
|        | Linux(x86_64) | CloudResetPwdAgent.zip | https://cn-north-4-cloud-reset-pwd.obs.cn-north-4.myhuaweicloud.com/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip            |
|        |               | sha256校验码              | https://cn-north-4-cloud-reset-pwd.obs.cn-north-4.myhuaweicloud.com/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip.sha256     |
|        | Windows       | CloudResetPwdAgent.zip | https://cn-north-4-cloud-reset-pwd.obs.cn-north-4.myhuaweicloud.com/windows/reset_pwd_agent/CloudResetPwdAgent.zip             |
|        |               | sha256校验码              | https://cn-north-4-cloud-reset-pwd.obs.cn-north-4.myhuaweicloud.com/windows/reset_pwd_agent/CloudResetPwdAgent.zip             |

| 区域     | 操作系统          | 文件名                    | 下载地址                                                                                                                                                                                                                                                                    |
|--------|---------------|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|        |               | sha256校验码              | <a href="https://cn-north-4-cloud-reset-pwd.obs.cn-north-4.myhuaweicloud.com/windows/reset_pwd_agent/CloudResetPwdAgent.zip.sha256">https://cn-north-4-cloud-reset-pwd.obs.cn-north-4.myhuaweicloud.com/windows/reset_pwd_agent/CloudResetPwdAgent.zip.sha256</a>       |
| 华东-上海二 | Linux(x86_32) | CloudResetPwdAgent.zip | <a href="https://cn-east-2-cloud-reset-pwd.obs.cn-east-2.myhuaweicloud.com/linux/32/reset_pwd_agent/CloudResetPwdAgent.zip">https://cn-east-2-cloud-reset-pwd.obs.cn-east-2.myhuaweicloud.com/linux/32/reset_pwd_agent/CloudResetPwdAgent.zip</a>                       |
|        |               | sha256校验码              | <a href="https://cn-east-2-cloud-reset-pwd.obs.cn-east-2.myhuaweicloud.com/linux/32/reset_pwd_agent/CloudResetPwdAgent.zip.sha256">https://cn-east-2-cloud-reset-pwd.obs.cn-east-2.myhuaweicloud.com/linux/32/reset_pwd_agent/CloudResetPwdAgent.zip.sha256</a>         |
|        | Linux(x86_64) | CloudResetPwdAgent.zip | <a href="https://cn-east-2-cloud-reset-pwd.obs.cn-east-2.myhuaweicloud.com/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip">https://cn-east-2-cloud-reset-pwd.obs.cn-east-2.myhuaweicloud.com/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip</a>                       |
|        |               | sha256校验码              | <a href="https://cn-east-2-cloud-reset-pwd.obs.cn-east-2.myhuaweicloud.com/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip.sha256">https://cn-east-2-cloud-reset-pwd.obs.cn-east-2.myhuaweicloud.com/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip.sha256</a>         |
|        | Linux(armv64) | CloudResetPwdAgent.zip | <a href="https://cn-east-2-cloud-reset-pwd.obs.cn-east-2.myhuaweicloud.com/arm/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip">https://cn-east-2-cloud-reset-pwd.obs.cn-east-2.myhuaweicloud.com/arm/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip</a>               |
|        |               | sha256校验码              | <a href="https://cn-east-2-cloud-reset-pwd.obs.cn-east-2.myhuaweicloud.com/arm/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip.sha256">https://cn-east-2-cloud-reset-pwd.obs.cn-east-2.myhuaweicloud.com/arm/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip.sha256</a> |
|        | Windows       | CloudResetPwdAgent.zip | <a href="https://cn-east-2-cloud-reset-pwd.obs.cn-east-2.myhuaweicloud.com/windows/reset_pwd_agent/CloudResetPwdAgent.zip">https://cn-east-2-cloud-reset-pwd.obs.cn-east-2.myhuaweicloud.com/windows/reset_pwd_agent/CloudResetPwdAgent.zip</a>                         |
|        |               | sha256校验码              | <a href="https://cn-east-2-cloud-reset-pwd.obs.cn-east-2.myhuaweicloud.com/windows/reset_pwd_agent/CloudResetPwdAgent.zip.sha256">https://cn-east-2-cloud-reset-pwd.obs.cn-east-2.myhuaweicloud.com/windows/reset_pwd_agent/CloudResetPwdAgent.zip.sha256</a>           |
| 华南-广州  | Linux(x86_32) | CloudResetPwdAgent.zip | <a href="https://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/linux/32/reset_pwd_agent/CloudResetPwdAgent.zip">https://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/linux/32/reset_pwd_agent/CloudResetPwdAgent.zip</a>                   |
|        |               | sha256校验码              | <a href="https://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/linux/32/reset_pwd_agent/CloudResetPwdAgent.zip.sha256">https://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/linux/32/reset_pwd_agent/CloudResetPwdAgent.zip.sha256</a>     |
|        | Linux(x86_64) | CloudResetPwdAgent.zip | <a href="https://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip">https://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip</a>                   |

| 区域    | 操作系统           | 文件名                    | 下载地址                                                                                                                                                                                                                                                                                |
|-------|----------------|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | Linux(aarch64) | sha256校验码              | <a href="https://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip.sha256">https://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip.sha256</a>                 |
|       |                | CloudResetPwdAgent.zip | <a href="https://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/arm/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip">https://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/arm/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip</a>                       |
|       |                | sha256校验码              | <a href="https://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/arm/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip.sha256">https://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/arm/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip.sha256</a>         |
|       | Windows        | CloudResetPwdAgent.zip | <a href="https://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/windows/reset_pwd_agent/CloudResetPwdAgent.zip">https://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/windows/reset_pwd_agent/CloudResetPwdAgent.zip</a>                                 |
|       |                | sha256校验码              | <a href="https://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/windows/reset_pwd_agent/CloudResetPwdAgent.zip.sha256">https://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/windows/reset_pwd_agent/CloudResetPwdAgent.zip.sha256</a>                   |
| 中国-香港 | Linux(x86_32)  | CloudResetPwdAgent.zip | <a href="https://ap-southeast-1-cloud-reset-pwd.obs.ap-southeast-1.myhuaweicloud.com/linux/32/reset_pwd_agent/CloudResetPwdAgent.zip">https://ap-southeast-1-cloud-reset-pwd.obs.ap-southeast-1.myhuaweicloud.com/linux/32/reset_pwd_agent/CloudResetPwdAgent.zip</a>               |
|       |                | sha256校验码              | <a href="https://ap-southeast-1-cloud-reset-pwd.obs.ap-southeast-1.myhuaweicloud.com/linux/32/reset_pwd_agent/CloudResetPwdAgent.zip.sha256">https://ap-southeast-1-cloud-reset-pwd.obs.ap-southeast-1.myhuaweicloud.com/linux/32/reset_pwd_agent/CloudResetPwdAgent.zip.sha256</a> |
|       | Linux(x86_64)  | CloudResetPwdAgent.zip | <a href="https://ap-southeast-1-cloud-reset-pwd.obs.ap-southeast-1.myhuaweicloud.com/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip">https://ap-southeast-1-cloud-reset-pwd.obs.ap-southeast-1.myhuaweicloud.com/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip</a>               |
|       |                | sha256校验码              | <a href="https://ap-southeast-1-cloud-reset-pwd.obs.ap-southeast-1.myhuaweicloud.com/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip.sha256">https://ap-southeast-1-cloud-reset-pwd.obs.ap-southeast-1.myhuaweicloud.com/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip.sha256</a> |
|       | Linux(aarch64) | CloudResetPwdAgent.zip | <a href="https://ap-southeast-1-cloud-reset-pwd.obs.ap-southeast-1.myhuaweicloud.com/arm/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip">https://ap-southeast-1-cloud-reset-pwd.obs.ap-southeast-1.myhuaweicloud.com/arm/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip</a>       |

| 区域    | 操作系统            | 文件名                    | 下载地址                                                                                                                                                                                                                                                                                        |
|-------|-----------------|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | Windows         | sha256校验码              | <a href="https://ap-southeast-1-cloud-reset-pwd.obs.ap-southeast-1.myhuaweicloud.com/arm/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip.sha256">https://ap-southeast-1-cloud-reset-pwd.obs.ap-southeast-1.myhuaweicloud.com/arm/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip.sha256</a> |
|       |                 | CloudResetPwdAgent.zip | <a href="https://ap-southeast-1-cloud-reset-pwd.obs.ap-southeast-1.myhuaweicloud.com/windows/reset_pwd_agent/CloudResetPwdAgent.zip">https://ap-southeast-1-cloud-reset-pwd.obs.ap-southeast-1.myhuaweicloud.com/windows/reset_pwd_agent/CloudResetPwdAgent.zip</a>                         |
|       |                 | sha256校验码              | <a href="https://ap-southeast-1-cloud-reset-pwd.obs.ap-southeast-1.myhuaweicloud.com/windows/reset_pwd_agent/CloudResetPwdAgent.zip.sha256">https://ap-southeast-1-cloud-reset-pwd.obs.ap-southeast-1.myhuaweicloud.com/windows/reset_pwd_agent/CloudResetPwdAgent.zip.sha256</a>           |
| 亚太-曼谷 | Linux(x86_32)   | CloudResetPwdAgent.zip | <a href="https://ap-southeast-2-cloud-reset-pwd.obs.ap-southeast-2.myhuaweicloud.com/linux/32/reset_pwd_agent/CloudResetPwdAgent.zip">https://ap-southeast-2-cloud-reset-pwd.obs.ap-southeast-2.myhuaweicloud.com/linux/32/reset_pwd_agent/CloudResetPwdAgent.zip</a>                       |
|       |                 | sha256校验码              | <a href="https://ap-southeast-2-cloud-reset-pwd.obs.ap-southeast-2.myhuaweicloud.com/linux/32/reset_pwd_agent/CloudResetPwdAgent.zip.sha256">https://ap-southeast-2-cloud-reset-pwd.obs.ap-southeast-2.myhuaweicloud.com/linux/32/reset_pwd_agent/CloudResetPwdAgent.zip.sha256</a>         |
|       | Linux(x86_64)   | CloudResetPwdAgent.zip | <a href="https://ap-southeast-2-cloud-reset-pwd.obs.ap-southeast-2.myhuaweicloud.com/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip">https://ap-southeast-2-cloud-reset-pwd.obs.ap-southeast-2.myhuaweicloud.com/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip</a>                       |
|       |                 | sha256校验码              | <a href="https://ap-southeast-2-cloud-reset-pwd.obs.ap-southeast-2.myhuaweicloud.com/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip.sha256">https://ap-southeast-2-cloud-reset-pwd.obs.ap-southeast-2.myhuaweicloud.com/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip.sha256</a>         |
|       | Linux(armv8_64) | CloudResetPwdAgent.zip | <a href="https://ap-southeast-2-cloud-reset-pwd.obs.ap-southeast-2.myhuaweicloud.com/arm/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip">https://ap-southeast-2-cloud-reset-pwd.obs.ap-southeast-2.myhuaweicloud.com/arm/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip</a>               |
|       |                 | sha256校验码              | <a href="https://ap-southeast-2-cloud-reset-pwd.obs.ap-southeast-2.myhuaweicloud.com/arm/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip.sha256">https://ap-southeast-2-cloud-reset-pwd.obs.ap-southeast-2.myhuaweicloud.com/arm/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip.sha256</a> |

| 区域 | 操作系统    | 文件名                    | 下载地址                                                                                                                              |
|----|---------|------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
|    | Windows | CloudResetPwdAgent.zip | https://ap-southeast-2-cloud-reset-pwd.obs.ap-southeast-2.myhuaweicloud.com/windows/reset_pwd_agent/CloudResetPwdAgent.zip        |
|    |         | sha256校验码              | https://ap-southeast-2-cloud-reset-pwd.obs.ap-southeast-2.myhuaweicloud.com/windows/reset_pwd_agent/CloudResetPwdAgent.zip.sha256 |

相关操作

获取完成后，您可以安装或更新一键式重置密码插件：

- [安装单台ECS的一键式重置密码插件（单台操作）](#)
- [更新单台ECS的一键式重置密码插件（单台操作）](#)
- [通过脚本批量更新ECS一键式重置密码插件（Linux）](#)
- [通过脚本批量更新ECS一键式重置密码插件（Windows）](#)

10.2.2 安装单台 ECS 的一键式重置密码插件（单台操作）

弹性云服务器提供一键式重置密码功能。当弹性云服务器的密码丢失或过期时，如果提前安装了一键式重置密码插件，则可以应用一键式重置密码功能，给弹性云服务器设置新密码。

该方法方便、有效，建议您成功创建、登录弹性云服务器后，安装密码重置插件，具体操作请参见本节内容。

 说明

使用公共镜像创建的弹性云服务器默认已安装一键式重置密码插件。检查是否已安装一键式重置密码插件，请参见[步骤1](#)。

安装须知

1. 用户自行决定是否安装一键式重置密码插件，使弹性云服务器具备一键式重置密码功能。
2. 安装完成后，请勿自行卸载插件，否则可能导致管理控制台判断失误，从而无法完成密码重置。
3. 重装/切换弹性云服务器操作系统后，一键式重置密码功能失效。如需继续使用该功能，请重新安装一键式重置密码插件。
4. 更换弹性云服务器系统盘后，一键式重置密码功能失效。如需继续使用该功能，请重新安装一键式重置密码插件。
5. CoreOS和KylinOS操作系统的弹性云服务器，不支持安装一键式重置密码插件。
6. 如果没有提前安装一键式重置密码插件，密码丢失或过期后，不能使用一键式重置密码功能。

- 弹性云服务器需绑定弹性公网IP，才能安装一键式重置密码插件。

## 前提条件

- 对于Windows弹性云服务器，需保证C盘可写入，且剩余空间大于300MB。
- 对于Linux弹性云服务器，需保证根目录可写入，且剩余空间大于300MB。
- 对于Linux弹性云服务器，若开启了selinux，请参考[关闭selinux](#)禁用selinux。
- 使用SUSE 11 SP4镜像创建的弹性云服务器，内存需要大于等于4GiB时才能支持一键式重置密码功能。
- 弹性云服务器使用的VPC网络DHCP不能禁用。
- 弹性云服务器网络正常通行。
- 设置弹性云服务器的网卡属性为DHCP，使弹性云服务器可以动态获取IP地址。

### 说明

Linux弹性云服务器的设置方法，请参见[设置网卡属性为DHCP（Linux）](#)。

Windows弹性云服务器的设置方法，请参见[设置网卡属性为DHCP（Windows）](#)。

- 弹性云服务器安全组出方向规则满足如下要求：

- 协议端口：TCP
- 端口范围：80
- 目的地址：169.254.0.0/16

如果您使用的是默认安全组出方向规则，则已经包括了如上要求，可以正常初始化。默认安全组出方向规则为：

- 协议端口：全部
- 端口范围：全部协议端口
- 目的地址：0.0.0.0/0

## Linux 弹性云服务器插件安装方法

**步骤1** 检查弹性云服务器是否已安装一键式重置密码插件。

- 以root用户登录弹性云服务器。
- 执行以下命令，查询是否已安装CloudResetPwdAgent。

```
ls -lh /Cloud*
```

图 10-3 查询是否已安装一键式重置密码插件

```
[root@ecs-test ~]# ls -lh /Cloud*
total 20K
drwx----- 2 root root 4.0K Jun 13 14:13 bin
drwxr-xr-x 2 root root 4.0K Jun 13 11:53 conf
drwx----- 3 root root 4.0K Jun 13 11:53 depend
drwx----- 2 root root 4.0K Jun 13 11:53 lib
drwx----- 2 root root 4.0K Jun 13 14:13 logs
[root@ecs-test ~]#
[root@ecs-test ~]#
```

检查结果是否如[图10-3](#)所示。

- 是，表示已安装一键式重置密码插件，结束。
- 否，表示未安装一键式重置密码插件，请继续执行如下操作进行安装。

**步骤2** 请参考[获取并校验一键式重置密码插件完整性（Linux）](#)，下载对应的一键式重置密码插件CloudResetPwdAgent.zip并完成完整性校验。

安装一键式重置密码插件对插件的具体放置目录无特殊要求，请您自定义。

**步骤3** 执行以下命令，解压软件包CloudResetPwdAgent.zip。

安装一键式重置密码插件对插件的解压目录无特殊要求，请您自定义。

**unzip -o -d 插件解压目录 CloudResetPwdAgent.zip**

示例：

假设插件解压的目录为/home/linux/test，则命令行如下：

**unzip -o -d /home/linux/test CloudResetPwdAgent.zip**

**步骤4** 安装一键式重置密码插件。

1. 执行以下命令，进入文件CloudResetPwdAgent.Linux。

**cd {插件解压目录}/CloudResetPwdAgent/CloudResetPwdAgent.Linux**

示例：

假设插件解压的目录为/home/linux/test，则命令行如下：

**cd /home/linux/test/CloudResetPwdAgent/CloudResetPwdAgent.Linux**

2. 执行以下命令，添加文件setup.sh的运行权限。

**chmod +x setup.sh**

3. 执行以下命令，安装插件。

**sudo sh setup.sh**

如果脚本执行成功打印“cloudResetPwdAgent install successfully.”，且未打印“Failed to start service cloudResetPwdAgent”，表示安装成功。

#### 说明

- 您也可以根据[步骤1](#)，检查密码重置插件是否安装成功。
- 如果密码重置插件安装失败，请检查安装环境是否符合要求，并重试安装操作。

**步骤5** 修改重置密码插件的文件权限。

**chmod 700 /CloudrResetPwdAgent/bin/cloudResetPwdAgent.script**

**chmod 700 /CloudrResetPwdAgent/bin/wrapper**

**chmod 600 /CloudrResetPwdAgent/lib/\***

----结束

## Windows 弹性云服务器插件安装方法

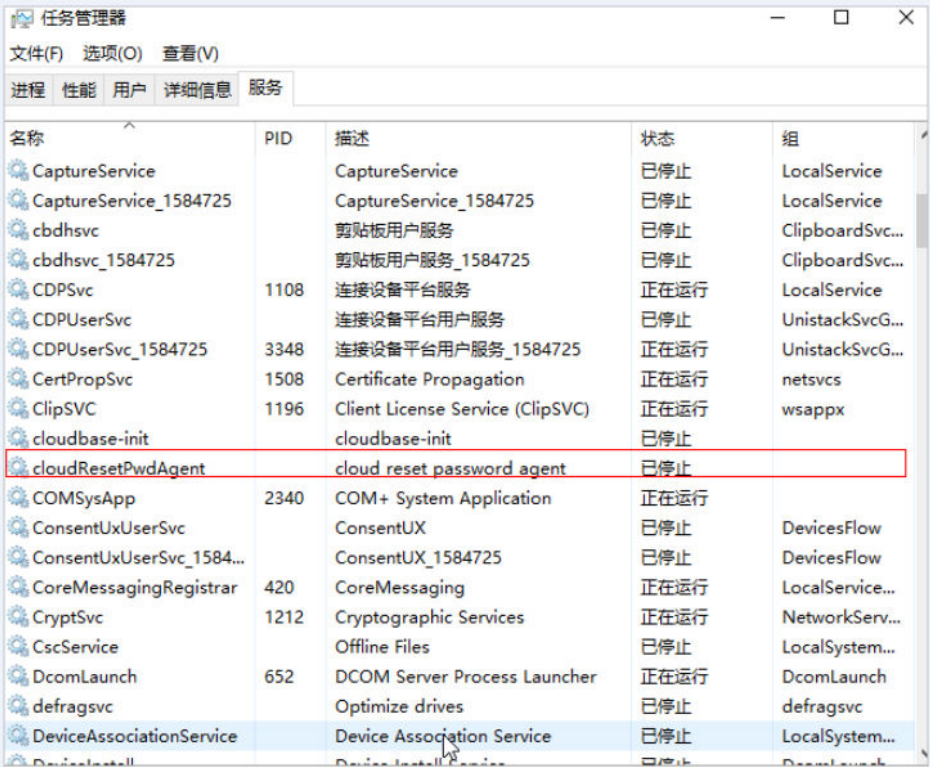
**步骤1** 登录弹性云服务器。

**步骤2** 检查弹性云服务器是否已安装密码重置插件CloudResetPwdAgent。检查方法如下：

查看任务管理器，如果找到cloudResetPwdAgent服务，如[图10-4](#)所示，表示弹性云服务器已安装密码重置插件。



图 10-4 安装插件成功



- 是，结束。
- 否，执行步骤3。

**步骤3** 请参考[获取并校验一键式重置密码插件完整性（Windows）](#)，下载对应的一键式重置密码插件CloudResetPwdAgent.zip并完成完整性校验。

安装一键式重置密码插件对插件的具体放置目录无特殊要求，请您自定义。

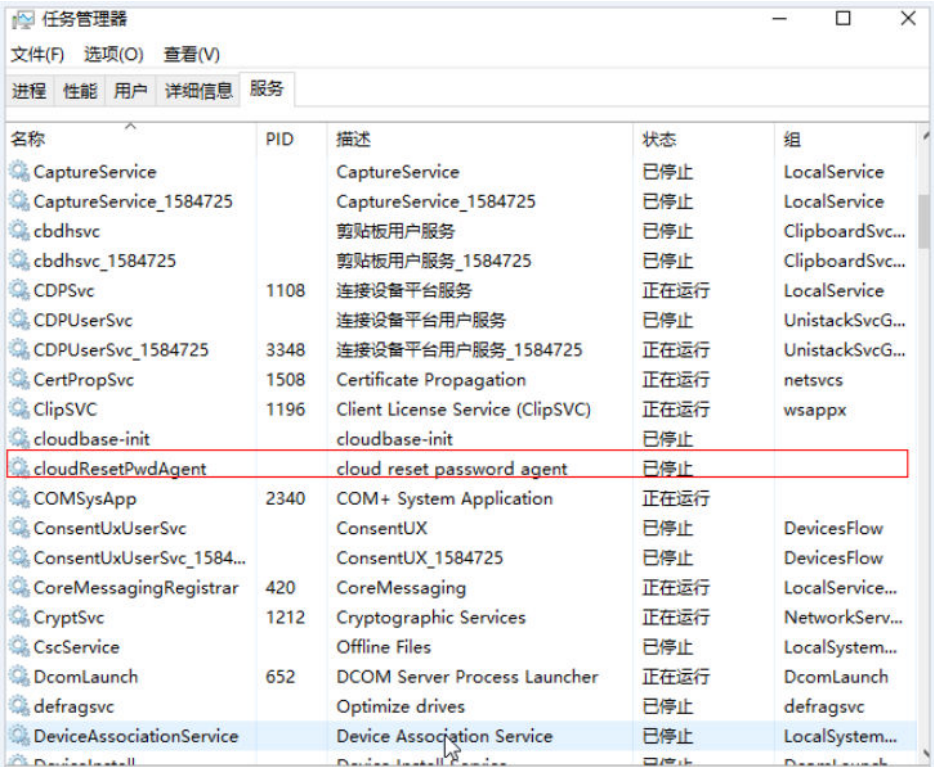
**步骤4** 解压软件包CloudResetPwdAgent.zip。

安装一键式重置密码插件对插件的解压目录无特殊要求，请您自定义。

**步骤5** 安装一键式重置密码插件。

1. 双击“CloudResetPwdAgent.Windows”文件夹下的“setup.bat”文件。  
安装密码重置插件。
2. 查看任务管理器，检查密码重置插件是否安装成功。  
如果在任务管理器中查找到了cloudResetPwdAgent服务，如[图10-5](#)所示，表示安装成功，否则安装失败。

图 10-5 安装插件成功



说明

如果密码重置插件安装失败，请检查安装环境是否符合要求，并重试安装操作。

----结束

后续处理

- 安装一键式重置密码插件后，如果无法通过弹性云服务器开机自动启动该插件，可以将其添加至开机启动项。具体方法请参见[一键式密码重置插件启动失败时如何操作？](#)。
- 一键式重置密码插件安装成功后，请勿删除重置密码进程CloudResetPwdAgent，否则，会导致一键式重装密码功能不可用。
- 华为云对一键式重置密码插件进行了升级，对于新创建的弹性云服务器，默认采用PIPE模式，不会占用端口。对于已创建云服务器，仍采用AUTO模式，随机占用31000~32999中的一个端口。占用端口的原则是：在该范围内，系统会按照自小到大的顺序，占用当前空闲的端口。

相关操作

下面介绍一键重置密码插件的卸载、停止和重启等相关操作。其中，Linux系统操作以CentOS 7.5版本为例进行介绍，更多版本的操作，请参考对应操作系统官网帮助文档。

- 卸载插件：**如果不再继续使用一键重置密码功能，您可以根据如下指导卸载插件。
  - Linux弹性云服务器

- i. 登录弹性云服务器。
  - ii. 执行以下命令，进入bin目录，删除服务cloudResetPwdAgent。  
**cd /CloudrResetPwdAgent/bin**  
**sudo ./cloudResetPwdAgent.script remove**
  - iii. 执行以下命令，删除插件。  
**sudo rm -rf /CloudrResetPwdAgent**
  - iv. 检查CloudResetPwdUpdateAgent是否存在，如果存在，进入bin目录，删除服务cloudResetPwdUpdateAgent。  
**cd /CloudResetPwdUpdateAgent/bin**  
**sudo ./cloudResetPwdUpdateAgent.script stop**  
**sudo ./cloudResetPwdUpdateAgent.script remove**
  - v. 执行以下命令，删除插件。  
**sudo rm -rf /CloudResetPwdUpdateAgent**
- Windows弹性云服务器
  - i. 卸载并删除CloudResetPwdAgent。
    - 1) 进入C:\CloudResetPwdAgent\bin文件夹。
    - 2) 双击“UninstallApp-NT.bat”。
    - 3) 删除C:\CloudResetPwdAgent的文件。
  - ii. （可选）卸载并删除CloudResetPwdUpdateAgent。  
不同Windows版本的弹性云服务器插件有差异，请检查CloudResetPwdUpdateAgent是否存在，如果存在，请执行本步骤卸载并删除；如果不存在，则跳过本步骤。
    - 1) 进入C:\CloudResetPwdUpdateAgent文件夹。
    - 2) 双击“UninstallApp-NT.bat”。
    - 3) 删除C:\CloudResetPwdUpdateAgent的文件。  
如果删除失败，请先通过“任务管理器”删除CloudResetPwdUpdateAgent进程后，再次删除C:\CloudResetPwdUpdateAgent文件夹。
- **停止插件：**如果暂时不需要使用一键重置密码功能，您可以根据如下指导停止插件。
  - Linux弹性云服务器
    - i. 登录弹性云服务器。
    - ii. 执行以下命令，进入bin目录，停止服务cloudResetPwdAgent。  
**cd /CloudrResetPwdAgent/bin**  
**sudo ./cloudResetPwdAgent.script stop**
    - iii. 检查CloudResetPwdUpdateAgent是否存在，如果存在，进入bin目录，停止服务cloudResetPwdUpdateAgent。  
**cd /CloudResetPwdUpdateAgent/bin**  
**sudo ./cloudResetPwdUpdateAgent.script stop**
  - Windows弹性云服务器
    - i. 停止CloudResetPwdAgent。

- 1) 登录弹性云服务器。
  - 2) 打开“任务管理器”。
  - 3) 在“服务”页签，找到“**CloudResetPwdAgent**”服务，右键单击菜单中的“停止”。
  - ii. （可选）停止**CloudResetPwdUpdateAgent**。  
不同Windows版本的弹性云服务器插件有差异，请检查**CloudResetPwdUpdateAgent**是否存在，如果存在，请执行本步骤停止；如果不存在，则跳过本步骤。
    - 1) 登录弹性云服务器。
    - 2) 打开“任务管理器”。
    - 3) 在“服务”页签，找到“**CloudResetPwdUpdateAgent**”服务，右键单击菜单中的“停止”。
- **重启插件**：如果一键重置密码功能异常，您可以根据如下指导重启插件。
    - Linux弹性云服务器
      - i. 登录弹性云服务器。
      - ii. 执行以下命令，进入bin目录，重启服务**cloudResetPwdAgent**。

```
cd /CloudResetPwdAgent/bin
sudo ./cloudResetPwdAgent.script reboot
```
      - iii. 检查**CloudResetPwdUpdateAgent**是否存在，如果存在，进入bin目录，重启服务**cloudResetPwdUpdateAgent**。

```
cd /CloudResetPwdUpdateAgent/bin
sudo ./cloudResetPwdUpdateAgent.script reboot
```
    - Windows弹性云服务器
      - i. 重启**CloudResetPwdAgent**。
        - 1) 登录弹性云服务器。
        - 2) 打开“任务管理器”。
        - 3) 在“服务”页签，找到“**CloudResetPwdAgent**”服务，右键单击菜单中的“重启”。
      - ii. （可选）重启**CloudResetPwdUpdateAgent**。  
不同Windows版本的弹性云服务器插件有差异，请检查**CloudResetPwdUpdateAgent**是否存在，如果存在，请执行本步骤重启；如果不存在，则跳过本步骤。
        - 1) 登录弹性云服务器。
        - 2) 打开“任务管理器”。
        - 3) 在“服务”页签，找到“**CloudResetPwdUpdateAgent**”服务，右键单击菜单中的“重启”。

### 10.2.3 更新单台 ECS 的一键式重置密码插件（单台操作）

弹性云服务器提供一键式重置密码功能。当弹性云服务器的密码丢失或过期时，如果提前安装了一键式重置密码插件，则可以应用一键式重置密码功能，给弹性云服务器设置新密码。

更新一键式重置密码插件的操作请参考本节内容。

## 安装须知

1. 弹性云服务器需绑定弹性公网IP，才能更新一键式重置密码插件。
2. 使用公共镜像创建的弹性云服务器默认已安装一键式重置密码插件，在更新前请先卸载一键式重置密码插件。

## 前提条件

- 对于Windows弹性云服务器，需保证C盘可写入，且剩余空间大于300MB。
- 对于Linux弹性云服务器，需保证根目录可写入，且剩余空间大于300MB。
- 对于Linux弹性云服务器，若开启了selinux，请参考[关闭selinux](#)禁用selinux。
- 使用SUSE 11 SP4镜像创建的弹性云服务器，内存需要大于等于4GiB时才能支持一键式重置密码功能。
- 弹性云服务器使用的VPC网络DHCP不能禁用。
- 弹性云服务器网络正常通行。
- 设置弹性云服务器的网卡属性为DHCP，使弹性云服务器可以动态获取IP地址。

### 说明

Linux弹性云服务器的设置方法，请参见[设置网卡属性为DHCP（Linux）](#)。

Windows弹性云服务器的设置方法，请参见[设置网卡属性为DHCP（Windows）](#)。

- 弹性云服务器安全组出方向规则满足如下要求：

- 协议端口：TCP
- 端口范围：80
- 目的地址：169.254.0.0/16

如果您使用的是默认安全组出方向规则，则已经包括了如上要求，可以正常初始化。默认安全组出方向规则为：

- 协议端口：全部
- 端口范围：全部协议端口
- 目的地址：0.0.0.0/0

## Linux 弹性云服务器插件更新方法

### 步骤1 卸载插件。

1. 登录弹性云服务器。
2. 执行以下命令，进入bin目录，删除服务cloudResetPwdAgent。  
**cd /CloudrResetPwdAgent/bin**  
**sudo ./cloudResetPwdAgent.script remove**
3. 执行以下命令，删除插件。  
**sudo rm -rf /CloudrResetPwdAgent**
4. 检查CloudResetPwdUpdateAgent是否存在，如果存在，进入bin目录，删除服务cloudResetPwdUpdateAgent。  
**cd /CloudResetPwdUpdateAgent/bin**  
**sudo ./cloudResetPwdUpdateAgent.script stop**  
**sudo ./cloudResetPwdUpdateAgent.script remove**

5. 执行以下命令，删除插件。

```
sudo rm -rf /CloudResetPwdUpdateAgent
```

**步骤2** 请参考[获取并校验一键式重置密码插件完整性（Linux）](#)，下载对应的一键式重置密码插件CloudResetPwdAgent.zip并完成完整性校验。

安装一键式重置密码插件对插件的具体放置目录无特殊要求，请您自定义。

**步骤3** 执行以下命令，解压软件包CloudResetPwdAgent.zip。

安装一键式重置密码插件对插件的解压目录无特殊要求，请您自定义。

```
unzip -o -d 插件解压目录 CloudResetPwdAgent.zip
```

示例：

假设插件解压的目录为/home/linux/test，则命令行如下：

```
unzip -o -d /home/linux/test CloudResetPwdAgent.zip
```

**步骤4** 安装一键式重置密码插件。

1. 执行以下命令，进入文件CloudResetPwdAgent.Linux。

```
cd {插件解压目录}/CloudResetPwdAgent/CloudResetPwdAgent.Linux
```

示例：

假设插件解压的目录为/home/linux/test，则命令行如下：

```
cd /home/linux/test/CloudResetPwdAgent/CloudResetPwdAgent.Linux
```

2. 执行以下命令，添加文件setup.sh的运行权限。

```
chmod +x setup.sh
```

3. 执行以下命令，安装插件。

```
sudo sh setup.sh
```

如果脚本执行成功打印“cloudResetPwdAgent install successfully.”，且未打印“Failed to start service cloudResetPwdAgent”，表示安装成功。

#### 说明

- 您也可以根据[步骤1](#)，检查密码重置插件是否安装成功。
- 如果密码重置插件安装失败，请检查安装环境是否符合要求，并重试安装操作。

**步骤5** 修改重置密码插件的文件权限。

```
chmod 700 /CloudResetPwdAgent/bin/cloudResetPwdAgent.script
```

```
chmod 700 /CloudResetPwdAgent/bin/wrapper
```

```
chmod 600 /CloudResetPwdAgent/lib/*
```

----结束

## Windows 弹性云服务器插件更新方法

**步骤1** 卸载插件。

1. 卸载并删除CloudResetPwdAgent。
  - a. 进入C:\CloudResetPwdAgent\bin文件夹。



- b. 双击“UninstallApp-NT.bat”。

c. 删除C:\CloudResetPwdAgent的文件。
2. （可选）卸载并删除CloudResetPwdUpdateAgent。  
不同Windows版本的弹性云服务器插件有差异，请检查CloudResetPwdUpdateAgent是否存在，如果存在，请执行本步骤卸载并删除；如果不存在，则跳过本步骤。

a. 进入C:\CloudResetPwdUpdateAgent文件夹。

b. 双击“UninstallApp-NT.bat”。

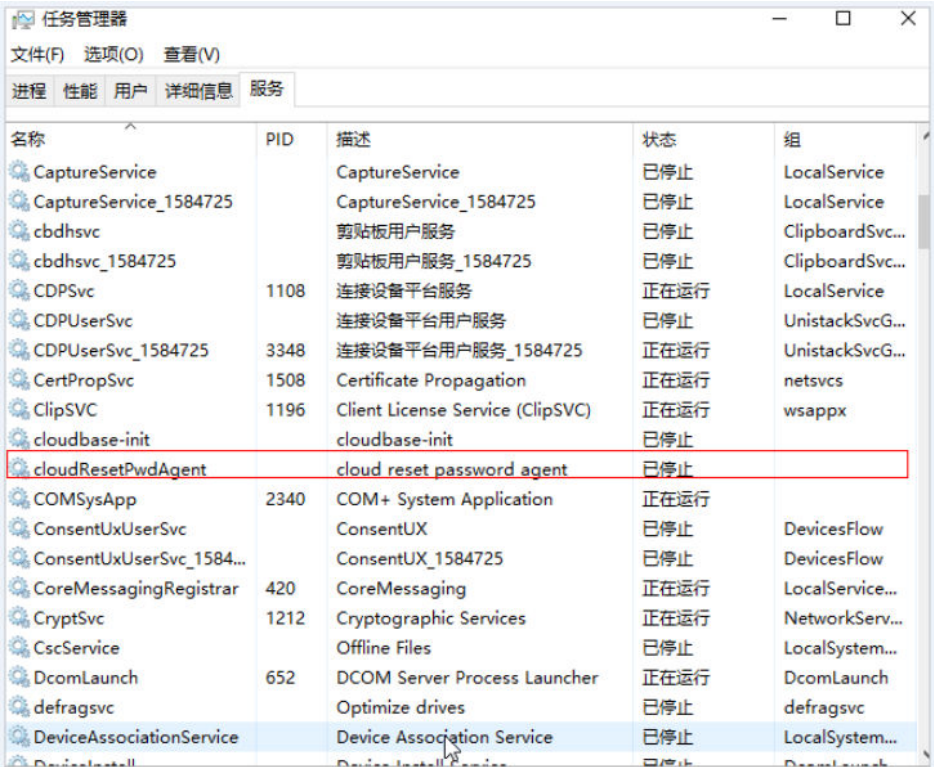
c. 删除C:\CloudResetPwdUpdateAgent的文件。

如果删除失败，请先通过“任务管理器”删除CloudResetPwdUpdateAgent进程后，再次删除C:\CloudResetPwdUpdateAgent文件夹。
- 步骤2 请参考[获取并校验一键式重置密码插件完整性（Windows）](#)，下载对应的一键式重置密码插件CloudResetPwdAgent.zip并完成完整性校验。  
安装一键式重置密码插件对插件的具体放置目录无特殊要求，请您自定义。
- 步骤3 解压软件包CloudResetPwdAgent.zip。  
安装一键式重置密码插件对插件的解压目录无特殊要求，请您自定义。
- 步骤4 安装一键式重置密码插件。

1. 双击“CloudResetPwdAgent.Windows”文件夹下的“setup.bat”文件。  
安装密码重置插件。

2. 查看任务管理器，检查密码重置插件是否安装成功。  
如果在任务管理器中查找到了cloudResetPwdAgent服务，如[图10-6](#)所示，表示安装成功，否则安装失败。

图 10-6 安装插件成功



### 📖 说明

如果密码重置插件安装失败，请检查安装环境是否符合要求，并重试安装操作。

----结束

## 后续处理

- 更新一键式重置密码插件后，如果无法通过弹性云服务器开机自动启动该插件，可以将其添加至开机启动项。具体方法请参见[一键式密码重置插件启动失败时如何操作？](#)。
- 一键式重置密码插件更新成功后，请勿删除重置密码进程CloudResetPwdAgent，否则，会导致一键式重装密码功能不可用。
- 华为云对一键式重置密码插件进行了升级，对于新创建的弹性云服务器，默认采用PIPE模式，不会占用端口。对于已创建云服务器，仍采用AUTO模式，随机占用31000~32999中的一个端口。占用端口的原则是：在该范围内，系统会按照自小到大的顺序，占用当前空闲的端口。

## 10.2.4 通过 AOM 批量更新 ECS 一键式重置密码插件

弹性云服务器提供一键式重置密码功能。当弹性云服务器的密码丢失或过期时，如果提前安装了一键式重置密码插件，则可以应用一键式重置密码功能，给弹性云服务器设置新密码。

应用运维管理（Application Operations Management，简称AOM）是云上应用的一站式立体化运维管理平台，AOM 2.0的统一数据采集Agent（简称UniAgent）支持更新一键式重置密码插件。

本章节介绍使用AOM 2.0 UniAgent方式更新一键式重置密码插件的操作指导。

## 约束与限制

AOM 2.0目前仅在部分区域上线，详细内容，请参见[开通AOM 2.0](#)。

## Linux 弹性云服务器插件更新方法

### 安装UniAgent

1. 登录[AOM华为云官网](#)。
2. 在AOM产品简介下方单击“AOM2.0控制台”，进入应用运维管理控制台。

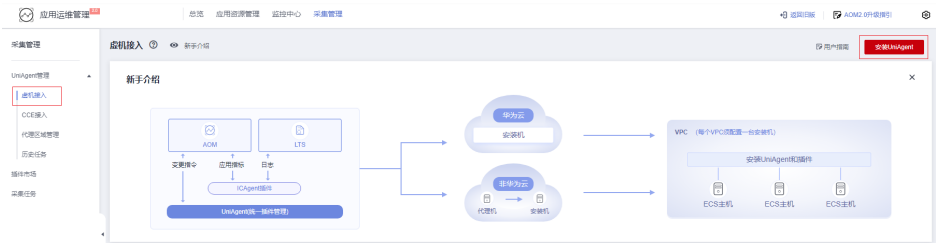
图 10-7 AOM 2.0 入口





3.
- 在应用运维管理控制台左侧导航栏，单击“采集管理”，进入采集管理控制台。

图 10-8 采集管理控制台



4.
- 在左侧导航栏选择“UniAgent管理 > 虚机接入”。
5.
- 单击“安装UniAgent”，在待更新重置密码插件的虚拟机中选择一台作为UniAgent的安装机。

说明

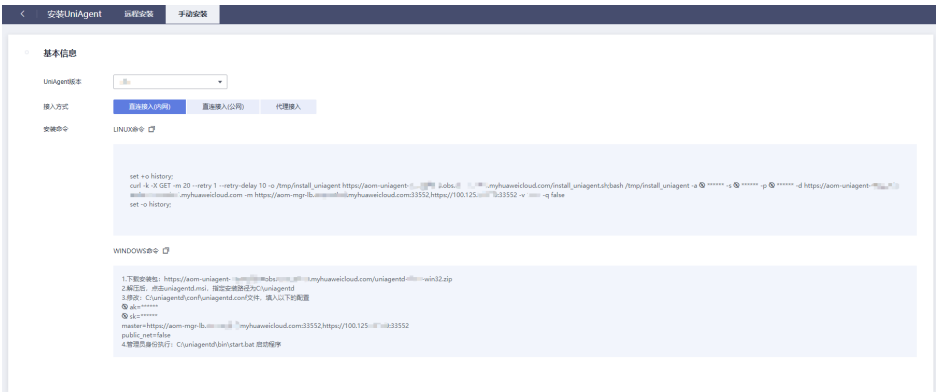
- 安装机是远程安装方式下命令的执行机。
- 首次安装UniAgent时，仅支持手动安装的方式。

请确保安装机与其余待安装机间网络互通，并且可通过SSH远程连接。

- 如果远程连接失败，请确认安全组规则入方向规则已添加安装机的IP网段，并且该网段允许SSH远程连接Linux弹性云服务器。
- 如果您的待更新机器在同一VPC下，继续执行后续步骤。
- 如果您的待更新机器属于不同VPC，建议您对每个VPC重复执行步骤5~步骤12，分VPC进行安装。
- 如果您想通过打通VPC的方式进行更新，请先完成“[如何实现跨VPC的网络互通？](#)”的相关配置，然后继续执行以下步骤。

6.
- 在安装UniAgent页面中，复制以下Linux安装命令。

图 10-9 安装 UniAgent（手动安装）



7.
- 登录待安装UniAgent的弹性云服务器，执行复制的Linux安装命令。  
若出现如下显示说明安装成功。

图 10-10 UniAgent 安装成功



安装完成后，在虚机接入界面可以看到已经安装成功的虚拟机。

图 10-11 安装成功的虚拟机

| 主机名称/IP地址              | 接入方式 | UniAgent状态 | 安装机名称 | 操作系统  | UniAgent版本 | UniAgent心跳          | ICAgent状态 | ICAgent版本 | 操作       |
|------------------------|------|------------|-------|-------|------------|---------------------|-----------|-----------|----------|
| ecs-01<br>172.16.0.132 | 直接接入 | 运行中        | -     | LINUX | 1.1.1      | 2024/06/25 15:50:28 | 未安装       | -         | 删除、设置安装机 |

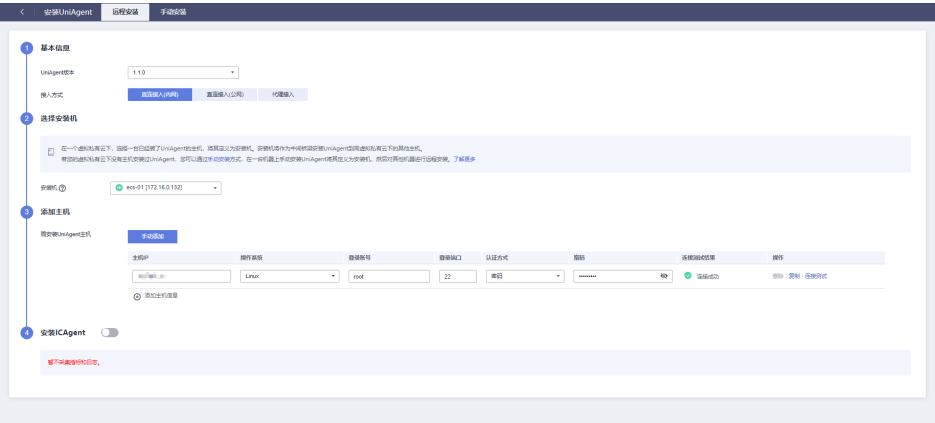
8. 在已安装成功的虚拟机“操作”列，单击“设置安装机”，将该虚拟机作为安装机。

图 10-12 设置安装机



9. 在虚机接入界面，单击“安装UniAgent”为其余虚拟机安装UniAgent。
10. 在UniAgent安装界面的上方，单击“远程安装”。

图 10-13 安装 UniAgent（远程安装）



11. 设置参数。
- a. 选择步骤7装好的虚拟机作为安装机。

b. 添加需安装UniAgent的主机。
- 单击“添加主机信息”可添加多个主机，最多支持添加100个主机。

说明

如果待安装主机在“虚机接入”页面列表的“UniAgent状态”为“运行中”，则无需执行后续步骤。

详细的参数设置，请参考[安装UniAgent](#)。

- 主机IP：主机的IP。

操作系统：主机的操作系统，例如Linux。

登录账号：登录主机的账号。建议使用root账号，可保证有足够的读写权限。

登录端口：访问主机的端口。

认证方式：认证方式为密码。

密码：登录主机的密码。

连接测试结果：测试安装机和需安装主机间的网络连通性以及密码正确性。

操作：删除、复制和连接测试。

12. 单击“立即安装”。

### 创建脚本

1. 在本地浏览器通过以下链接获取脚本，并复制内容。  
请根据云服务器所在区域选择脚本的下载地址：
  - 华北-北京一：[https://cn-north-1-cloud-reset-pwd.obs.cn-north-1.myhuaweicloud.com/linux/batch\\_update\\_resetpwd/update\\_log4j\\_version\\_for\\_resetpwdagent.sh](https://cn-north-1-cloud-reset-pwd.obs.cn-north-1.myhuaweicloud.com/linux/batch_update_resetpwd/update_log4j_version_for_resetpwdagent.sh)
  - 华北-北京四：[https://cn-north-4-cloud-reset-pwd.obs.cn-north-4.myhuaweicloud.com/linux/batch\\_update\\_resetpwd/update\\_log4j\\_version\\_for\\_resetpwdagent.sh](https://cn-north-4-cloud-reset-pwd.obs.cn-north-4.myhuaweicloud.com/linux/batch_update_resetpwd/update_log4j_version_for_resetpwdagent.sh)
  - 华东-上海二：[https://cn-east-2-cloud-reset-pwd.obs.cn-east-2.myhuaweicloud.com/linux/batch\\_update\\_resetpwd/update\\_log4j\\_version\\_for\\_resetpwdagent.sh](https://cn-east-2-cloud-reset-pwd.obs.cn-east-2.myhuaweicloud.com/linux/batch_update_resetpwd/update_log4j_version_for_resetpwdagent.sh)
  - 华南-广州：[https://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/linux/batch\\_update\\_resetpwd/update\\_log4j\\_version\\_for\\_resetpwdagent.sh](https://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/linux/batch_update_resetpwd/update_log4j_version_for_resetpwdagent.sh)
  - 中国-香港：[https://ap-southeast-1-cloud-reset-pwd.obs.ap-southeast-1.myhuaweicloud.com/linux/batch\\_update\\_resetpwd/update\\_log4j\\_version\\_for\\_resetpwdagent.sh](https://ap-southeast-1-cloud-reset-pwd.obs.ap-southeast-1.myhuaweicloud.com/linux/batch_update_resetpwd/update_log4j_version_for_resetpwdagent.sh)
2. 进入[云运维中心控制台](#)，在左侧导航栏单击“资源运维 > 自动化运维”。

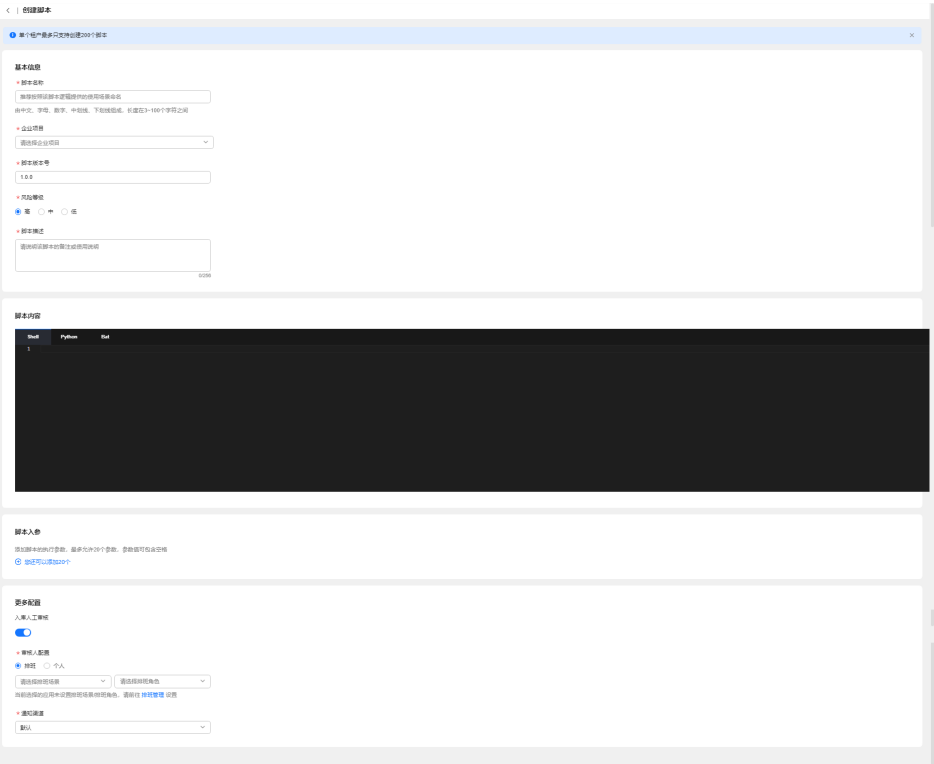
#### 说明

云运维中心处于公测阶段，需[申请公测](#)后才能使用。

3. 在自动化运维控制台，单击“脚本管理”。
4. 在脚本管理页面，单击“创建脚本”。

参数设置相关内容，请参见[创建自定义脚本](#)。

图 10-14 创建脚本



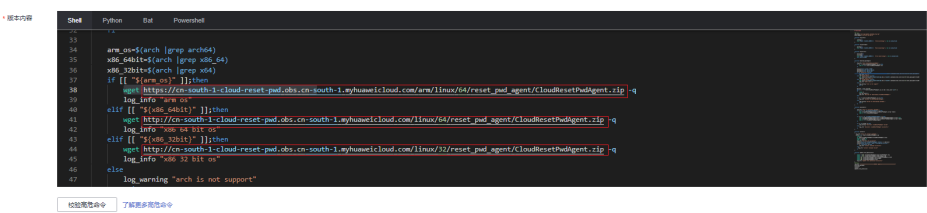
5. 将步骤1下载的脚本文件复制到“脚本内容”区域。

说明

请确认脚本内容wget URL之后带有参数-q，没有则需要手动添加，否则会导致下载软件包日志过多，影响性能。

6. 手动替换脚本中下载地址，下载对应操作系统架构的一键式重置密码插件包。  
仅未绑定弹性公网IP的弹性云服务器需要执行本步骤。若待更新的弹性云服务器均已绑定弹性公网IP，则跳过本步骤，无需操作。

图 10-15 脚本内容



如图10-15所示，图中红框内容为脚本中的插件下载地址，需要参考[获取一键式重置密码插件](#)进行替换。

以“华南-广州”区域为例：

- 32位操作系统，x86架构：  
**wget [http://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/linux/32/reset\\_pwd\\_agent/CloudResetPwdAgent.zip](http://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/linux/32/reset_pwd_agent/CloudResetPwdAgent.zip) -q**
- 64位操作系统，x86架构：

```
wget http://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip -q
```

– 64位操作系统，鲲鹏架构：

```
wget https://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/arm/linux/64/reset_pwd_agent/CloudResetPwdAgent.zip -q
```

📖 说明

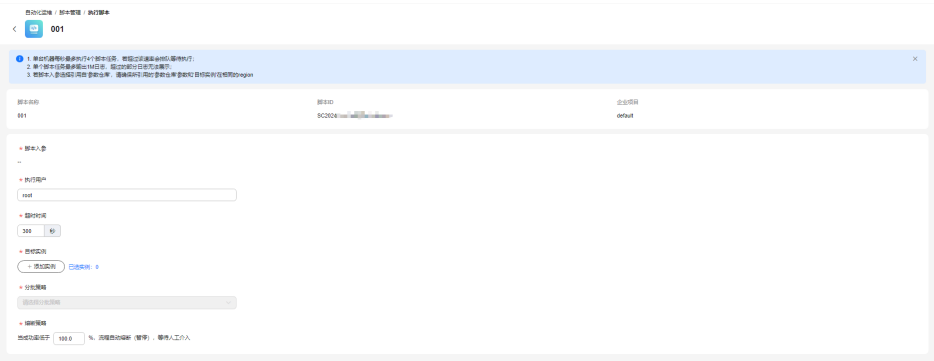
已上传一键式重置密码插件至OBS桶的区域包括：华北-北京一、华北-北京四、华东-上海二、华南-广州、中国-香港。

- 7. 单击“提交”。

执行脚本

- 1. 脚本创建完成后，在脚本列表“操作”列单击“执行”，创建执行脚本任务。

图 10-16 创建执行脚本任务



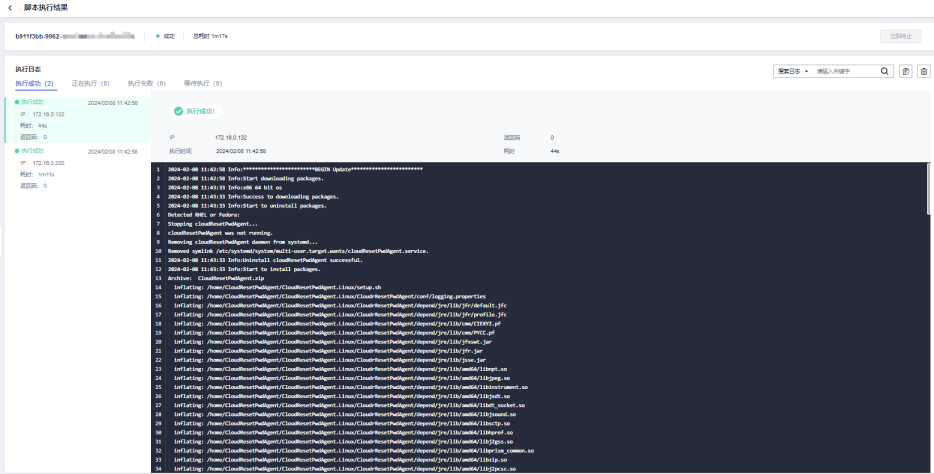
设置执行账号为root，目标实例选择已经安装好UniAgent的机器，更多参数设置，请参见[执行自定义脚本](#)。

📖 说明

执行脚本时目标实例数量建议不要超过100台，否则会影响性能。

- 2. 单击“提交”，执行脚本。
- 3. 查看脚本是否执行成功，有如下显示说明执行成功。

图 10-17 执行成功



检查插件是否更新成功

1. 参考步骤4~步骤7，创建检查服务状态的脚本，脚本内容为：  
**service cloudResetPwdAgent status**  
**ls -lh /Cloud\***
2. 单击“提交”，执行脚本。  
如果服务CloudResetPwdAgent的状态不是“unrecognized service”，表示插件安装成功，否则安装失败。

Windows 弹性云服务器插件更新方法

安装UniAgent

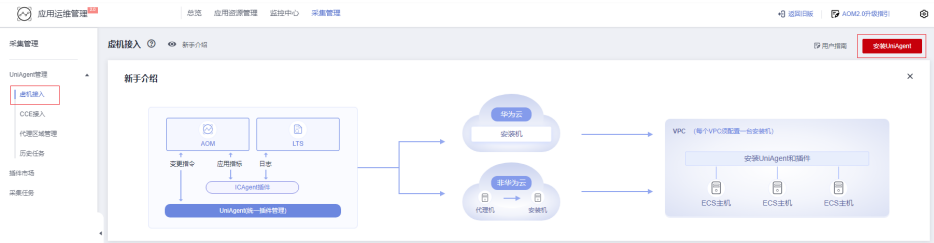
1. 登录AOM华为云官网。
2. 在AOM产品简介下方单击“AOM2.0控制台”，进入应用运维管理控制台。

图 10-18 AOM 2.0 入口



3. 在应用运维管理控制台左侧导航栏，单击“采集管理”，进入采集管理控制台。

图 10-19 采集管理控制台



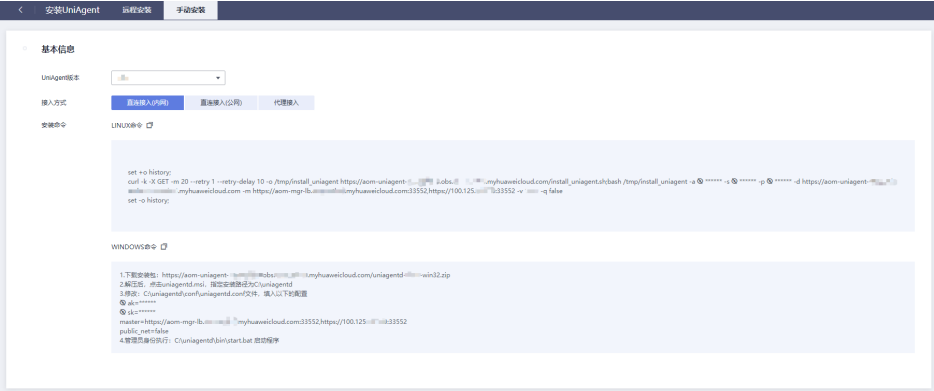
- 4. 在左侧导航栏选择“UniAgent管理 > 虚机接入”。
- 5. 单击“安装UniAgent”。

说明

Windows操作系统的弹性云服务器只能选择手动安装的方式，暂不支持Windows操作系统的远程安装。

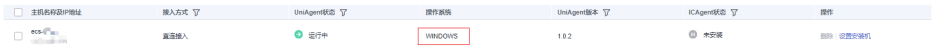
- 6. 在安装UniAgent页面中，复制Windows操作系统的安装包下载地址。

图 10-20 安装 UniAgent（手动安装）



- 7. 登录待安装UniAgent的弹性云服务器，打开PowerShell、命令行工具或者在浏览器中复制链接下载UniAgent安装包。  
命令示例：  
**wget https://aom-uniagent-cn-north-4.obs.cn-north-4.myhuaweicloud.com/uniagentd-1.0.2-win32.zip -o c:\uniagent.zip**
- 8. 下载完成后继续按照步骤6中的指导进行安装。  
安装完成后，在虚机接入界面可以看到已经安装成功的虚拟机。

图 10-21 安装成功的虚拟机



- 9. 重复步骤5~步骤8，为其余虚拟机安装UniAgent。

创建脚本

- 1. 在本地浏览器通过以下链接获取脚本，并复制内容。  
请根据云服务器所在区域选择脚本的下载地址：
  - 华北-北京一：[https://cn-north-1-cloud-reset-pwd.obs.cn-north-1.myhuaweicloud.com/windows/uniagent/update\\_log4j\\_version\\_for\\_resetpwdagent\\_windows\\_for\\_uniagent.bat](https://cn-north-1-cloud-reset-pwd.obs.cn-north-1.myhuaweicloud.com/windows/uniagent/update_log4j_version_for_resetpwdagent_windows_for_uniagent.bat)

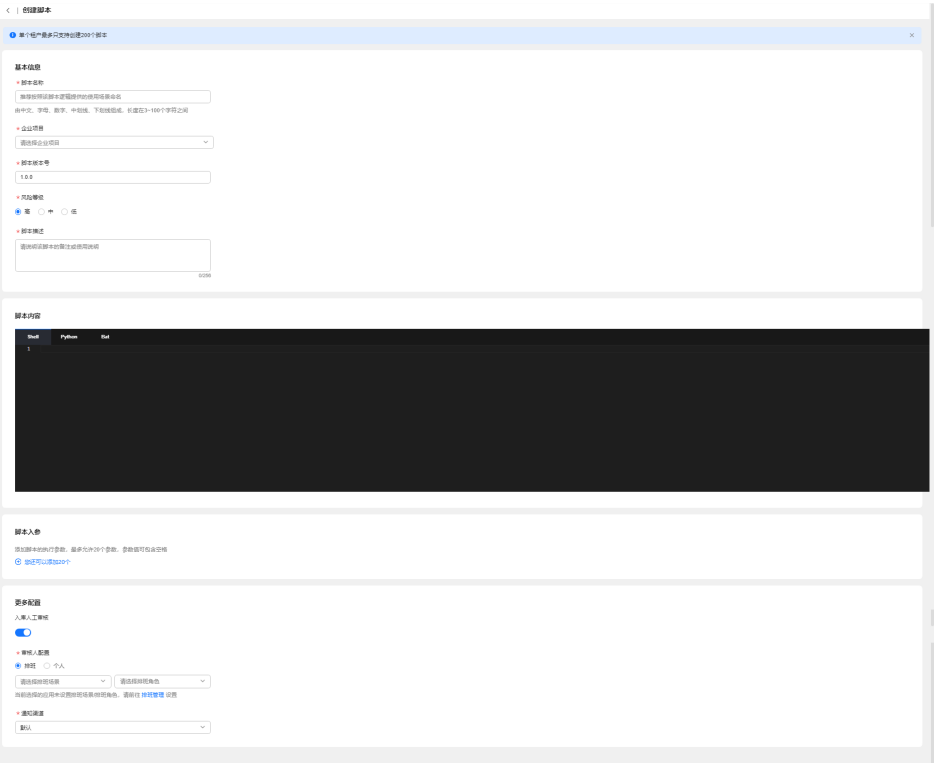
- 华北-北京四: [https://cn-north-4-cloud-reset-pwd.obs.cn-north-4.myhuaweicloud.com/windows/uniagent/update\\_log4j\\_version\\_for\\_resetpwdagent\\_windows\\_for\\_uniagent.bat](https://cn-north-4-cloud-reset-pwd.obs.cn-north-4.myhuaweicloud.com/windows/uniagent/update_log4j_version_for_resetpwdagent_windows_for_uniagent.bat)
  - 华东-上海二: [https://cn-east-2-cloud-reset-pwd.obs.cn-east-2.myhuaweicloud.com/windows/uniagent/update\\_log4j\\_version\\_for\\_resetpwdagent\\_windows\\_for\\_uniagent.bat](https://cn-east-2-cloud-reset-pwd.obs.cn-east-2.myhuaweicloud.com/windows/uniagent/update_log4j_version_for_resetpwdagent_windows_for_uniagent.bat)
  - 华南-广州: [https://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/windows/uniagent/update\\_log4j\\_version\\_for\\_resetpwdagent\\_windows\\_for\\_uniagent.bat](https://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/windows/uniagent/update_log4j_version_for_resetpwdagent_windows_for_uniagent.bat)
  - 中国-香港: [https://ap-southeast-1-cloud-reset-pwd.obs.ap-southeast-1.myhuaweicloud.com/windows/uniagent/update\\_log4j\\_version\\_for\\_resetpwdagent\\_windows\\_for\\_uniagent.bat](https://ap-southeast-1-cloud-reset-pwd.obs.ap-southeast-1.myhuaweicloud.com/windows/uniagent/update_log4j_version_for_resetpwdagent_windows_for_uniagent.bat)
2. 进入[云运维中心控制台](#)，在左侧导航栏单击“资源运维 > 自动化运维”。

 说明

云运维中心处于公测阶段，需[申请公测](#)后才能使用。

3. 在自动化运维控制台，单击“脚本管理”。
4. 在脚本管理页面，单击“创建脚本”。
- 参数设置相关内容，请参见[创建自定义脚本](#)。

图 10-22 创建脚本



5. 输入“脚本名称”，并将步骤1下载的脚本文件复制到“脚本内容”区域。

 说明

对于Windows操作系统的弹性云服务器，需将“脚本内容”的格式切换为“Bat”。

6. 手动替换脚本中下载地址，下载对应操作系统架构的一键式重置密码插件包。



仅未绑定弹性公网IP的弹性云服务器需要执行本步骤。若待更新的弹性云服务器均已绑定弹性公网IP，则跳过本步骤，无需操作。

图 10-23 脚本内容

```
22 goto :eof
23
24 :download_packages
25 call :log_info "Start downloading packages."
26 if not exist %ZIP_FILE% (
27 powershell wget -uri https://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/windows/reset_pwd_agent/CloudResetPwdAgent.zip -Outfile %ZIP_FILE%
28 call :log_info "Success to downloading packages."
29) else (
30 call :log_info "CloudResetPwdAgent already exists."
31)
32 goto :eof
33
34 :download_retry
35 call :log_info "Start retry downloading packages."
36 if not exist %ZIP_FILE% (
```

如**图10-23**所示，图中红框内容为脚本中的插件下载地址，需要参考**获取一键式重置密码插件**进行替换。

以“华南-广州”区域为例：

```
wget -Uri https://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/windows/reset_pwd_agent/CloudResetPwdAgent.zip
```

## 说明

已上传一键式重置密码插件至OBS桶的区域包括：华北-北京一、华北-北京四、华东-上海二、华南-广州、中国-香港。

7. 单击“提交”。

## 执行脚本

- 脚本创建完成后，在脚本列表“操作”列单击“执行”，创建执行脚本任务。

图 10-24 创建执行脚本任务

设置执行账号为Administrator，目标实例选择已经安装好UniAgent的机器，更多参数设置，请参见[执行自定义脚本](#)。

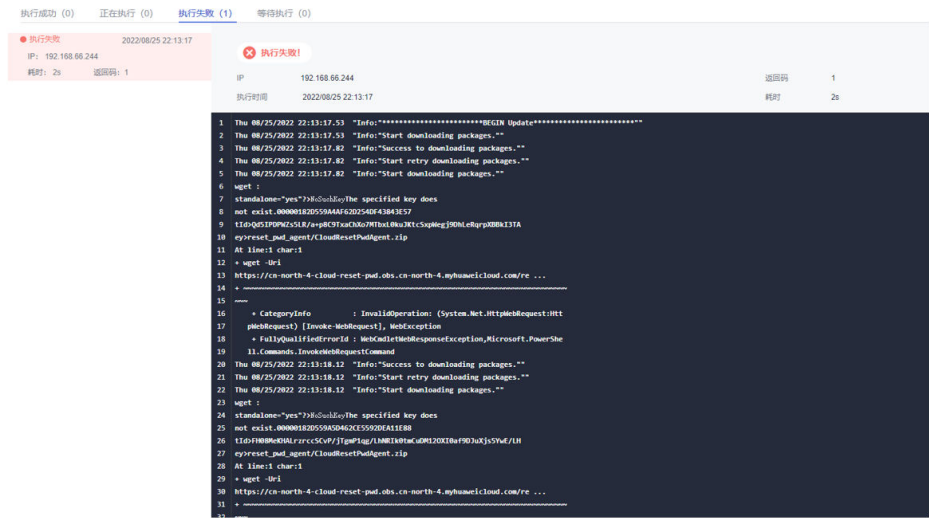
2. 查看脚本是否执行成功，有如下显示说明执行成功。

**图 10-25 执行成功**

```
56 wget |
57 Wed 06/17/2022 5:01:22.08 "Info:Install SecurePayloadAgent success"
58 Wed 06/17/2022 5:01:22.08 "Info:Install SecurePayloadAgent success"
59 Wed 06/17/2022 5:01:22.08 "Info:Install SecurePayloadAgent success"
60 wget |
61 Wed 06/17/2022 5:01:22.08 "Info:Install SecurePayloadAgent success"
62 Wed 06/17/2022 5:01:22.08 "Info:Install SecurePayloadAgent success"
63 wget |
64 Wed 06/17/2022 5:01:22.08 "Info:Install SecurePayloadAgent success"
65 wget |
66 Wed 06/17/2022 5:01:22.08 "Info:Install SecurePayloadAgent success"
67 wget |
68 Wed 06/17/2022 5:01:22.08 "Info:Install SecurePayloadAgent success"
69 wget |
70 Wed 06/17/2022 5:01:22.08 "Info:Install SecurePayloadAgent success"
71 wget |
72 Wed 06/17/2022 5:01:22.08 "Info:Install SecurePayloadAgent success"
73 wget |
74 Wed 06/17/2022 5:01:22.08 "Info:Install SecurePayloadAgent success"
75 wget |
76 Wed 06/17/2022 5:01:22.08 "Info:Install SecurePayloadAgent success"
77 wget |
78 Wed 06/17/2022 5:01:22.08 "Info:Install SecurePayloadAgent success"
79 wget |
80 Wed 06/17/2022 5:01:22.08 "Info:Install SecurePayloadAgent success"
81 wget |
82 Wed 06/17/2022 5:01:22.08 "Info:Install SecurePayloadAgent success"
83 wget |
84 Wed 06/17/2022 5:01:22.08 "Info:Install SecurePayloadAgent success"
85 wget |
86 Wed 06/17/2022 5:01:22.08 "Info:Install SecurePayloadAgent success"
87 wget |
88 Wed 06/17/2022 5:01:22.08 "Info:Install SecurePayloadAgent success"
89 wget |
90 Wed 06/17/2022 5:01:22.08 "Info:Install SecurePayloadAgent success"
91 wget |
92 Wed 06/17/2022 5:01:22.08 "Info:Install SecurePayloadAgent success"
93 wget |
94 Wed 06/17/2022 5:01:22.08 "Info:Install SecurePayloadAgent success"
95 wget |
96 Wed 06/17/2022 5:01:22.08 "Info:Install SecurePayloadAgent success"
97 wget |
98 Wed 06/17/2022 5:01:22.08 "Info:Install SecurePayloadAgent success"
99 wget |
100 Wed 06/17/2022 5:01:22.08 "Info:Install SecurePayloadAgent success"
```

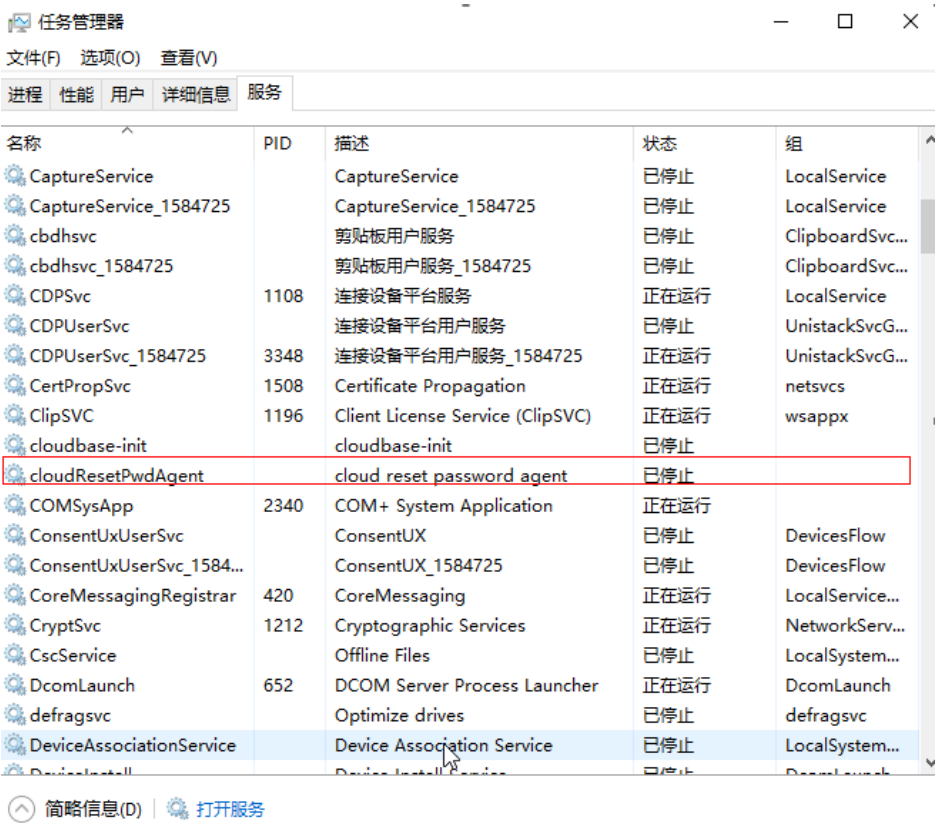
如果脚本执行有如下报错，请检查脚本下载地址是否正确。如果地址正确，请重试或者绑定弹性公网IP后更换其他区域的下载地址。

图 10-26 执行失败



检查插件是否更新成功  
登录windows云服务器，有如下显示说明更新成功。

图 10-27 插件更新成功



## 后续处理

- 更新一键式重置密码插件后，如果无法通过弹性云服务器开机自动启动该插件，可以将其添加至开机启动项。具体方法请参见[一键式密码重置插件启动失败时如何操作？](#)。
- 一键式重置密码插件更新成功后，请勿删除重置密码进程CloudResetPwdAgent，否则，会导致一键式重装密码功能不可用。
- 华为云对一键式重置密码插件进行了升级，对于新创建的弹性云服务器，默认采用PIPE模式，不会占用端口。对于已创建云服务器，仍采用AUTO模式，随机占用31000~32999中的一个端口。占用端口的原则是：在该范围内，系统会按照自小到大的顺序，占用当前空闲的端口。

## 10.2.5 通过脚本批量更新 ECS 一键式重置密码插件（Linux）

### 操作场景

当您需要对多台Linux系统的云服务器批量更新一键式重置密码插件时，可参考本文档操作。

### 前提条件

- 准备好执行机，执行机需满足的条件请参见[约束与限制](#)。
- 需要提前准备待批量安装插件的云服务器的IP地址、root用户的密码信息或者私钥文件。
- 执行机应该与待更新机器在同一VPC下。
- 在执行完步骤6之后可以解绑eip。

### 约束与限制

- 需要选取一台操作系统为CentOS 7（公共镜像）且已绑定弹性公网IP的云服务器作为执行机，且与待批量安装插件的弹性云服务器之间网络需要互通。

#### 说明

- 若已配置yum内部源，可不需要绑定弹性公网IP。
- 仅支持对使用同一密钥对的弹性云服务器执行批量安装插件的操作。

### 操作步骤

1. 以root用户登录执行机。
2. 执行以下命令，安装批量脚本运行所需要的依赖。  
**yum install ansible -y**
3. 请参考[获取并校验一键式重置密码插件完整性（Linux）](#)，下载对应的一键式重置密码插件CloudResetPwdAgent.zip并完成完整性校验。  
安装一键式重置密码插件对插件的具体放置目录无特殊要求，请您自定义。
4. 执行以下命令，将批量操作脚本下载到root目录下。  
**curl URL > ~/batch\_update\_log4j\_version.py**  
其中，URL为批量操作的执行脚本。  
请根据云服务器所在区域选择脚本的下载地址：

- 华北-北京一: [https://cn-north-1-cloud-reset-pwd.obs.cn-north-1.myhuaweicloud.com/linux/batch\\_update\\_resetpwd/batch\\_update\\_log4j\\_version.py](https://cn-north-1-cloud-reset-pwd.obs.cn-north-1.myhuaweicloud.com/linux/batch_update_resetpwd/batch_update_log4j_version.py)
  - 华北-北京四: [https://cn-north-4-cloud-reset-pwd.obs.cn-north-4.myhuaweicloud.com/linux/batch\\_update\\_resetpwd/batch\\_update\\_log4j\\_version.py](https://cn-north-4-cloud-reset-pwd.obs.cn-north-4.myhuaweicloud.com/linux/batch_update_resetpwd/batch_update_log4j_version.py)
  - 华东-上海二: [https://cn-east-2-cloud-reset-pwd.obs.cn-east-2.myhuaweicloud.com/linux/batch\\_update\\_resetpwd/batch\\_update\\_log4j\\_version.py](https://cn-east-2-cloud-reset-pwd.obs.cn-east-2.myhuaweicloud.com/linux/batch_update_resetpwd/batch_update_log4j_version.py)
  - 华南-广州: [https://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/linux/batch\\_update\\_resetpwd/batch\\_update\\_log4j\\_version.py](https://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/linux/batch_update_resetpwd/batch_update_log4j_version.py)
  - 中国-香港: [https://ap-southeast-1-cloud-reset-pwd.obs.ap-southeast-1.myhuaweicloud.com/linux/batch\\_update\\_resetpwd/batch\\_update\\_log4j\\_version.py](https://ap-southeast-1-cloud-reset-pwd.obs.ap-southeast-1.myhuaweicloud.com/linux/batch_update_resetpwd/batch_update_log4j_version.py)
  - 亚太-曼谷: [https://ap-southeast-2-cloud-reset-pwd.obs.ap-southeast-2.myhuaweicloud.com/linux/batch\\_update\\_resetpwd/batch\\_update\\_log4j\\_version.py](https://ap-southeast-2-cloud-reset-pwd.obs.ap-southeast-2.myhuaweicloud.com/linux/batch_update_resetpwd/batch_update_log4j_version.py)
5. 执行以下命令，将更新插件脚本下载到root目录下。
- ```
curl URL > ~/update_log4j_version_for_resetpwdagent.sh
```
- 其中，URL为更新插件脚本的下载地址。
- 请根据云服务器所在区域选择脚本的下载地址：
- 华北-北京一: https://cn-north-1-cloud-reset-pwd.obs.cn-north-1.myhuaweicloud.com/linux/batch_update_resetpwd/update_log4j_version_for_resetpwdagent.sh
 - 华北-北京四: https://cn-north-4-cloud-reset-pwd.obs.cn-north-4.myhuaweicloud.com/linux/batch_update_resetpwd/update_log4j_version_for_resetpwdagent.sh
 - 华东-上海二: https://cn-east-2-cloud-reset-pwd.obs.cn-east-2.myhuaweicloud.com/linux/batch_update_resetpwd/update_log4j_version_for_resetpwdagent.sh
 - 华南-广州: https://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/linux/batch_update_resetpwd/update_log4j_version_for_resetpwdagent.sh
 - 中国-香港: https://ap-southeast-1-cloud-reset-pwd.obs.ap-southeast-1.myhuaweicloud.com/linux/batch_update_resetpwd/update_log4j_version_for_resetpwdagent.sh
 - 亚太-曼谷: https://ap-southeast-2-cloud-reset-pwd.obs.ap-southeast-2.myhuaweicloud.com/linux/batch_update_resetpwd/update_log4j_version_for_resetpwdagent.sh
6. 检查如下脚本是否在root目录下：
- batch_update_log4j_version.py
 - update_log4j_version_for_resetpwdagent.sh
 - CloudResetPwdAgent.zip
7. 执行以下命令，新建并编辑host_list.txt，按i进入编辑模式。
- ```
vi host_list.txt
```
- 将需要自动安装驱动的云服务器的相关信息填写到host\_list.txt文件中。

文件填写格式与登录待切换弹性云服务器的方式需要匹配。

- 使用密钥对方式鉴权的云服务器，填写方式如下：

 **注意**

- 使用密钥对方式鉴权的云服务器，请将创建弹性云服务器时保存的私钥文件，上传至与host\_list.txt同一个文件夹下。
- 使用密钥对方式鉴权的云服务器，请确保私钥文件的权限为400。  
**chmod 400 私钥文件**

每行仅需填写云服务器IP地址。

示例：

```
192.168.1.10
192.168.1.11
```

- 使用密码方式登录的云服务器，填写方式如下：  
请严格按照每行ip,root用户密码，中间以英文逗号隔开的格式填写。

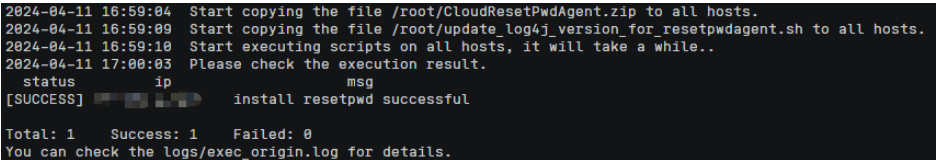
示例：

```
192.168.1.10, '*****'
192.168.1.11, '*****'
```

8. 运行批量执行操作脚本 “batch\_update\_log4j\_version.py” 。
- 密钥对鉴权方式的服务器
- 如果私钥文件与批量操作执行脚本在一个目录下，则直接指定私钥文件名称即可。

**python batch\_update\_log4j\_version.py {私钥文件路径/私钥文件名称}**

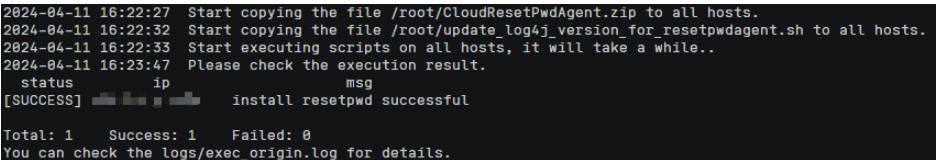
图 10-28 运行成功



若如图10-28所示，则表示脚本运行成功。

- 密码方式鉴权的服务器。
- python batch\_update\_log4j\_version.py**

图 10-29 运行成功



若如图10-29所示，则表示脚本运行成功。

9. 执行如下命令，在 “/root/logs/exec\_origin.log” 的最后一行查看运行结果日志。
- vim /root/logs/exec\_origin.log**

若如图10-30所示，则表示批量更新一键式重置密码插件成功。

图 10-30 运行结果日志

```
begin install CloudResetPwdAgent
=====cp LinuxCloudResetPwdAgent=====
=====v1 /etc/profile=====
=====begin install CloudResetPwdAgent=====
Detected RHEL or Fedora:
Installing the cloudResetPwdAgent daemon using systemd...
creating default service file...
Reading file /etc/systemd/system/cloudResetPwdAgent.service

/home/CloudResetPwdAgent/CloudResetPwdAgent.Linux
cloudResetPwdAgent install successfully.
2024-04-11 17:08:03 Info:sh setup.sh successful
2024-04-11 17:08:03 Info:install resetpwd successful
2024-04-11 17:08:03 Info:update file permission successfulRemoved symlink /etc/systemd/system/multi-user.target.wants/cloudResetPwdAgent.service.
ls: cannot access /CloudResetPwdUpdateAgent: No such file or directory
Created symlink from /etc/systemd/system/multi-user.target.wants/cloudResetPwdAgent.service to /etc/systemd/system/cloudResetPwdAgent.service.
Redirecting to /bin/systemctl status cloudResetPwdAgent.service
```

后续处理

- 更新一键式重置密码插件后，如果无法通过弹性云服务器开机自动启动该插件，可以将其添加至开机启动项。具体方法请参见[一键式密码重置插件启动失败时如何操作？](#)。
- 一键式重置密码插件更新成功后，请勿删除重置密码进程CloudResetPwdAgent，否则，会导致一键式重装密码功能不可用。
- 华为云对一键式重置密码插件进行了升级，对于新创建的弹性云服务器，默认采用PIPE模式，不会占用端口。对于已创建云服务器，仍采用AUTO模式，随机占用31000~32999中的一个端口。占用端口的原则是：在该范围内，系统会按照自小到大的顺序，占用当前空闲的端口。

10.2.6 通过脚本批量更新 ECS 一键式重置密码插件（Windows）

操作场景

当您需要对多台Windows系统的云服务器批量更新一键式重置密码插件时，可参考本文档操作。

前提条件

- 准备好执行机，执行机需满足的条件请参见[约束与限制](#)。
- 需要提前准备待批量安装插件的云服务器的IP地址、Administrator用户的密码信息。
- 执行机应该与待更新机器在同一VPC下。
- 在执行完步骤7之后可以解绑eip。

约束与限制

需要选取一台操作系统为CentOS 8.2（公共镜像）且已绑定弹性公网IP的云服务器作为执行机，且与待批量安装插件的弹性云服务器之间网络需要互通。

说明

若已配置yum内部源，可不需要绑定弹性公网IP。

操作步骤

- 以root用户登录执行机。
- 执行以下命令，安装批量脚本运行所需要的依赖。



- a. 执行以下命令，安装epel。  
**yum install epel-release -y**
- b. 执行以下命令，安装ansible。  
**yum install ansible -y --skip-broken**  
执行**ansible --version**命令检查ansible是否安装成功。

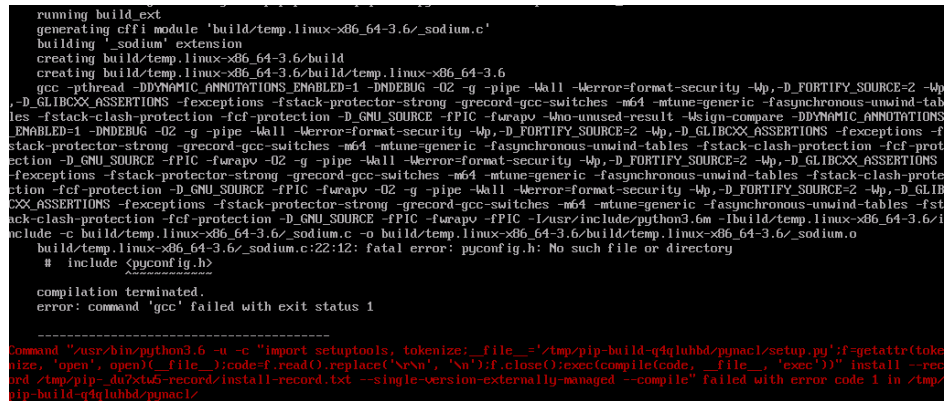
#### 说明

如果因为yum源配置问题导致无法安装ansible，可以使用如下命令安装ansible：

```
yum install python3 python3-pip
pip3 install --upgrade pip
pip3 install ansible
```

- c. 执行以下命令，安装pip。  
**python3.6 -m pip install bcrypt==3.2.0 paramiko==3.3.1 cryptography==3.3.0 pywinrm PyYAML Jinja2 httpplib2 six**  
若出现如图10-31所示报错信息，请执行以下操作。
  - i. 执行以下命令，安装依赖：  
**dnf install python3-devel**
  - ii. 然后再次执行以下命令：  
**python3.6 -m pip install bcrypt==3.2.0 paramiko==3.3.1 cryptography==3.3.0 pywinrm PyYAML Jinja2 httpplib2 six**

图 10-31 报错信息



```
running build_ext
generating cffi module 'build/temp.linux-x86_64-3.6/_sodium.c'
building '_sodium' extension
creating build/temp.linux-x86_64-3.6/build
creating build/temp.linux-x86_64-3.6/build/temp.linux-x86_64-3.6
gcc -pthread -DDYNAMIC_ANNOTATIONS_ENABLED=1 -DNDEBUG -O2 -g -pipe -Wall -Werror=format-security -Wp,-D_FORTIFY_SOURCE=2 -Wp,-D_GLIBCXX_ASSERTIONS -fexceptions -fstack-protector-strong -grecord-gcc-switches -m64 -mtune=generic -fasynchronous-unwind-tables -fstack-clash-protection -fcf-protection -D_GNU_SOURCE -fPIC -fwrapv -Wno-unused-result -Wsign-compare -DDYNAMIC_ANNOTATIONS_ENABLED=1 -DNDEBUG -O2 -g -pipe -Wall -Werror=format-security -Wp,-D_FORTIFY_SOURCE=2 -Wp,-D_GLIBCXX_ASSERTIONS -fexceptions -fstack-protector-strong -grecord-gcc-switches -m64 -mtune=generic -fasynchronous-unwind-tables -fstack-clash-protection -fcf-protection -D_GNU_SOURCE -fPIC -fwrapv -O2 -g -pipe -Wall -Werror=format-security -Wp,-D_FORTIFY_SOURCE=2 -Wp,-D_GLIBCXX_ASSERTIONS -fexceptions -fstack-protector-strong -grecord-gcc-switches -m64 -mtune=generic -fasynchronous-unwind-tables -fstack-clash-protection -fcf-protection -D_GNU_SOURCE -fPIC -fwrapv -fPIC -I/usr/include/python3.6m -Ibuild/temp.linux-x86_64-3.6 -Ibuild/temp.linux-x86_64-3.6/_sodium.o -c build/temp.linux-x86_64-3.6/_sodium.c -o build/temp.linux-x86_64-3.6/build/temp.linux-x86_64-3.6/_sodium.o
In file included from build/temp.linux-x86_64-3.6/_sodium.c:22:12: fatal error: pyconfig.h: No such file or directory
include <pyconfig.h>
^
compilation terminated.
error: command 'gcc' failed with exit status 1

Command "/usr/bin/python3.6 -u -c "import setuptools, tokenize; _file_ = '/tmp/pip-build-qdqlubhd/pynacl/setup.py'; if getattr(tokenize, 'open', open)(__file__).code.read().replace('\r\n', '\n') if __close__: exec(compile(code, _file_, 'exec'))" install --record /tmp/pip-4u7xtu65-record/install-record.txt --single-version-externally-managed --compile" failed with error code 1 in /tmp/pip-build-qdqlubhd/pynacl/
```

3. 执行以下命令，参考表10-6，下载对应区域的Windows操作系统的一键式重置密码插件CloudResetPwdAgent.zip并完成完整性校验。

以“华北-北京四”区域的Windows操作系统为例：

```
wget https://cn-north-4-cloud-reset-pwd.obs.cn-north-4.myhuaweicloud.com/windows/reset_pwd_agent/CloudResetPwdAgent.zip
```

```
wget https://cn-north-4-cloud-reset-pwd.obs.cn-north-4.myhuaweicloud.com/windows/reset_pwd_agent/CloudResetPwdAgent.zip.sha256
```

完整性校验步骤，请参见[获取并校验一键式重置密码插件完整性（Linux）](#)的步骤4。

安装一键式重置密码插件对插件的具体放置目录无特殊要求，请您自定义。

4. 执行以下命令，将对应OS架构的Windows版本的安装包下载到root目录下：  
执行命令pwd确认当前路径是否为/root，若不是请切换至/root路径下。
  - 32位操作系统，x86架构：  
**wget https://www.7-zip.org/a/7z2107.exe '--no-check-certificate'**
  - 64位操作系统，x86架构：  
**wget https://www.7-zip.org/a/7z2107-x64.exe '--no-check-certificate'**
  - 64位操作系统，鲲鹏架构：  
**wget https://www.7-zip.org/a/7z2107-x64.exe '--no-check-certificate'**
5. 执行以下命令，将批量操作脚本下载到root目录下。  
**curl URL > ~/batch\_update\_log4j\_version\_for\_windows.py**  
其中，URL为批量操作的执行脚本。  
请根据云服务器所在区域选择脚本的下载地址：
  - 华北-北京一：[https://cn-north-1-cloud-reset-pwd.obs.cn-north-1.myhuaweicloud.com/windows/batch\\_update\\_resetpwd/batch\\_update\\_log4j\\_version\\_for\\_windows.py](https://cn-north-1-cloud-reset-pwd.obs.cn-north-1.myhuaweicloud.com/windows/batch_update_resetpwd/batch_update_log4j_version_for_windows.py)
  - 华北-北京四：[https://cn-north-4-cloud-reset-pwd.obs.cn-north-4.myhuaweicloud.com/windows/batch\\_update\\_resetpwd/batch\\_update\\_log4j\\_version\\_for\\_windows.py](https://cn-north-4-cloud-reset-pwd.obs.cn-north-4.myhuaweicloud.com/windows/batch_update_resetpwd/batch_update_log4j_version_for_windows.py)
  - 华东-上海二：[https://cn-east-2-cloud-reset-pwd.obs.cn-east-2.myhuaweicloud.com/windows/batch\\_update\\_resetpwd/batch\\_update\\_log4j\\_version\\_for\\_windows.py](https://cn-east-2-cloud-reset-pwd.obs.cn-east-2.myhuaweicloud.com/windows/batch_update_resetpwd/batch_update_log4j_version_for_windows.py)
  - 华南-广州：[https://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/windows/batch\\_update\\_resetpwd/batch\\_update\\_log4j\\_version\\_for\\_windows.py](https://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/windows/batch_update_resetpwd/batch_update_log4j_version_for_windows.py)
  - 中国-香港：[https://ap-southeast-1-cloud-reset-pwd.obs.ap-southeast-1.myhuaweicloud.com/windows/batch\\_update\\_resetpwd/batch\\_update\\_log4j\\_version\\_for\\_windows.py](https://ap-southeast-1-cloud-reset-pwd.obs.ap-southeast-1.myhuaweicloud.com/windows/batch_update_resetpwd/batch_update_log4j_version_for_windows.py)
  - 亚太-曼谷：[https://ap-southeast-2-cloud-reset-pwd.obs.ap-southeast-2.myhuaweicloud.com/windows/batch\\_update\\_resetpwd/batch\\_update\\_log4j\\_version\\_for\\_windows.py](https://ap-southeast-2-cloud-reset-pwd.obs.ap-southeast-2.myhuaweicloud.com/windows/batch_update_resetpwd/batch_update_log4j_version_for_windows.py)
6. 执行以下命令，将更新插件脚本下载到root目录下。  
**curl URL > ~/update\_log4j\_version\_for\_resetpwdagent\_windows.bat**  
其中，URL为更新插件脚本的下载地址。  
请根据云服务器所在区域选择脚本的下载地址：
  - 华北-北京一：[https://cn-north-1-cloud-reset-pwd.obs.cn-north-1.myhuaweicloud.com/windows/batch\\_update\\_resetpwd/update\\_log4j\\_version\\_for\\_resetpwdagent\\_windows.bat](https://cn-north-1-cloud-reset-pwd.obs.cn-north-1.myhuaweicloud.com/windows/batch_update_resetpwd/update_log4j_version_for_resetpwdagent_windows.bat)
  - 华北-北京四：[https://cn-north-4-cloud-reset-pwd.obs.cn-north-4.myhuaweicloud.com/windows/batch\\_update\\_resetpwd/update\\_log4j\\_version\\_for\\_resetpwdagent\\_windows.bat](https://cn-north-4-cloud-reset-pwd.obs.cn-north-4.myhuaweicloud.com/windows/batch_update_resetpwd/update_log4j_version_for_resetpwdagent_windows.bat)
  - 华东-上海二：[https://cn-east-2-cloud-reset-pwd.obs.cn-east-2.myhuaweicloud.com/windows/batch\\_update\\_resetpwd/update\\_log4j\\_version\\_for\\_resetpwdagent\\_windows.bat](https://cn-east-2-cloud-reset-pwd.obs.cn-east-2.myhuaweicloud.com/windows/batch_update_resetpwd/update_log4j_version_for_resetpwdagent_windows.bat)
  - 华南-广州：[https://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/windows/batch\\_update\\_resetpwd/update\\_log4j\\_version\\_for\\_resetpwdagent\\_windows.bat](https://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/windows/batch_update_resetpwd/update_log4j_version_for_resetpwdagent_windows.bat)



- 中国-香港: [https://ap-southeast-1-cloud-reset-pwd.obs.ap-southeast-1.myhuaweicloud.com/windows/batch\\_update\\_resetpwd/update\\_log4j\\_version\\_for\\_resetpwdagent\\_windows.bat](https://ap-southeast-1-cloud-reset-pwd.obs.ap-southeast-1.myhuaweicloud.com/windows/batch_update_resetpwd/update_log4j_version_for_resetpwdagent_windows.bat)
  - 亚太-曼谷: [https://ap-southeast-2-cloud-reset-pwd.obs.ap-southeast-2.myhuaweicloud.com/windows/batch\\_update\\_resetpwd/update\\_log4j\\_version\\_for\\_resetpwdagent\\_windows.bat](https://ap-southeast-2-cloud-reset-pwd.obs.ap-southeast-2.myhuaweicloud.com/windows/batch_update_resetpwd/update_log4j_version_for_resetpwdagent_windows.bat)
7. 检查如下文件是否在root目录下。
- batch\_update\_log4j\_version\_for\_windows.py
  - update\_log4j\_version\_for\_resetpwdagent\_windows.bat
  - CloudResetPwdAgent.zip
  - 7z\*.exe
8. 执行以下命令，新建并编辑host\_list.txt，按i进入编辑模式。
- vi host\_list.txt**
- 将需要自动安装驱动的云服务器器的相关信息填写到host\_list.txt文件中。
- 填写Administrator用户的IP和密码，请严格按照每行“IP,用户密码”的格式填写，中间以英文逗号隔开。
- 示例：
- ```
192.168.1.10,*****!
192.168.1.11,*****!
```
9. 执行以下命令，添加ansible配置文件。
- mkdir -p /etc/ansible**
- touch /etc/ansible/ansible.cfg**
10. 运行批量执行操作脚本“batch_update_log4j_version_for_windows.py”。
- python3.6 batch_update_log4j_version_for_windows.py**

图 10-32 运行脚本

```
2022-01-08 17:00:36 Start copying the file /root/CloudResetPwdAgent.zip to all hosts.
2022-01-08 17:00:43 Start copying the file /root/update_log4j_version_for_resetpwdagent_windows.bat to all hosts.
2022-01-08 17:00:45 Start copying the file /root/7z.exe to all hosts.
2022-01-08 17:00:46 Start executing scripts on all hosts, it will take a while..
2022-01-08 17:00:57 Please check the execution result.
      status      ip      msg
[SUCCESS] 192.168.96.118 started successfully
Total: 1      Success: 1      Failed: 0
You can check the logs/exec_origin.log for details.
```

11. 执行如下命令，在“/root/logs/exec_origin.log”的最后一行查看运行结果日志。
- vim /root/logs/exec_origin.log**
- 若如下图所示，则表示运行成功。

图 10-33 运行成功

```
"C:\\temp\\CloudResetPwdAgent\\CloudResetPwdUpdateAgent.Windows\\CloudResetPwdUpdateAgent\\lib\\json-20160810.jar",
"C:\\temp\\CloudResetPwdAgent\\CloudResetPwdUpdateAgent.Windows\\CloudResetPwdUpdateAgent\\lib\\log4j-api-2.17.0.jar",
"C:\\temp\\CloudResetPwdAgent\\CloudResetPwdUpdateAgent.Windows\\CloudResetPwdUpdateAgent\\lib\\log4j-core-2.17.0.jar",
"C:\\temp\\CloudResetPwdAgent\\CloudResetPwdUpdateAgent.Windows\\CloudResetPwdUpdateAgent\\lib\\resetpwdupdateagent.jar",
"C:\\temp\\CloudResetPwdAgent\\CloudResetPwdUpdateAgent.Windows\\CloudResetPwdUpdateAgent\\lib\\wrapper.dll",
"C:\\temp\\CloudResetPwdAgent\\CloudResetPwdUpdateAgent.Windows\\CloudResetPwdUpdateAgent\\lib\\wrapper.jar",
"205 File(s) copied",
"The cloud reset password update agent service is starting.",
"The cloud reset password update agent service was started successfully.",
"
2022/01/08 17:00:56.63 \\Info: \\install ResetPwdUpdateAgent success\\",
2022/01/08 17:00:56.83 \\Info: \\*****Update Success*****\\",
"Press any key to continue . . ."
```

后续处理

- 更新一键式重置密码插件后，如果无法通过弹性云服务器开机自动启动该插件，可以将其添加至开机启动项。具体方法请参见[一键式密码重置插件启动失败时如何操作？](#)。
- 一键式重置密码插件更新成功后，请勿删除重置密码进程CloudResetPwdAgent，否则，会导致一键式重装密码功能不可用。
- 华为云对一键式重置密码插件进行了升级，对于新创建的弹性云服务器，默认采用PIPE模式，不会占用端口。对于已创建云服务器，仍采用AUTO模式，随机占用31000~32999中的一个端口。占用端口的原则是：在该范围内，系统会按照自小到大的顺序，占用当前空闲的端口。

10.3 管理 ECS 密钥对

10.3.1 密钥对使用场景介绍

密钥对

密钥对，即SSH密钥对，是为用户提供远程登录云服务器的安全凭证，是一种区别于传统的用户名和密码登录的认证方式。

密钥对包含一个公钥和一个私钥，公钥自动保存在KPS（Key Pair Service）中，私钥由用户保存在本地。若用户将公钥配置在Linux云服务器中，则可以使用私钥安全地登录Linux云服务器，而不需要输入密码。由于密钥对可以让用户无需输入密码登录到Linux云服务器，因此，可以防止由于密码被拦截、破解造成的账户密码泄露，从而提高Linux云服务器的安全性。

您可以通过[数据加密服务](#)（Data Encryption Workshop）管理密钥对，包括创建、导入、绑定、查看、重置、替换、解绑、删除密钥对等。

本章节主要介绍如何创建和导入密钥对，其余操作，请参见“[管理密钥对](#)”。

使用场景

用户在购买弹性云服务器时，建议选择密钥对进行用户身份认证，或者通过提供的密钥对获取Windows操作系统弹性云服务器的登录密码。

- 登录Linux操作系统的弹性云服务器
若用户购买的是Linux操作系统的弹性云服务器，可以直接使用密钥对远程登录云服务器。
 - 创建弹性云服务器时，选择“密钥对方式”登录，详细操作，请参见[自定义购买ECS](#)的“设置‘登录凭证’”。
 - 创建弹性云服务器完成后，通过“[重置密钥对](#)”的方式为云服务器绑定密钥对。
- 获取Windows操作系统弹性云服务器的登录密码
若用户购买的是Windows操作系统的弹性云服务器，可以通过密钥对的私钥获取登录密码，该密码为随机密码，安全性高。
详细内容，请参见[获取Windows弹性云服务器的密码](#)

创建密钥对操作指引

您可以使用已有密钥对或新建一个密钥对，用于远程登录身份验证。

- 新建密钥对

如果没有可用的密钥对，需新建一个密钥对，生成公钥和私钥，并在登录弹性云服务器时提供私钥进行鉴权。创建密钥对的方法如下：

- **（推荐）通过管理控制台创建密钥对**：公钥自动保存在系统中，私钥由用户保存在本地。
- **通过PuTTY Key Generator工具创建密钥对**：公钥和私钥均保存在用户本地。

创建成功的密钥对，还需要执行[导入密钥对](#)，导入系统才能正常使用密钥对。

- 使用已有密钥对

如果本地已有密钥对（例如，使用PuTTYgen工具生成的密钥对），可以在管理控制台导入密钥对公钥，由系统维护您的公钥文件。具体操作请参见[导入密钥对](#)。

说明

如果已有密钥对的公钥文件是通过puttygen.exe工具的“Save public key”按钮保存的，该公钥文件不能直接导入管理控制台。

如需继续使用该密钥对作远程身份验证，请参见[通过puttygen.exe工具创建的密钥对，导入管理控制台失败怎么办？](#)

约束与限制

- 仅支持远程登录Linux云服务器。
- 通过管理控制台创建的SSH-2密钥对仅支持“RSA-2048”加解密算法。
- 密钥对仅适用于本区域的云服务器。
- 通过外部导入的密钥对支持的加解密算法为：
 - RSA-1024
 - RSA-2048
 - RSA-4096
- 私钥是保证您的弹性云服务器安全的重要手段之一，用于远程登录身份认证，为保证弹性云服务器安全，只能下载一次，请妥善保管。

10.3.2 （推荐）通过管理控制台创建密钥对

操作场景

您可以通过管理控制台创建密钥对，创建完成后，公钥自动保存在系统中，私钥由用户保存在本地。通过管理控制台绑定密钥对后，如果没有私钥，您将无法登录该ECS实例，请您妥善保管私钥文件。

操作步骤

1. 登录管理控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。

3. 单击“”，选择“计算 > 弹性云服务器”。
4. 在左侧导航树中，选择“密钥对”。
5. 在“密钥对管理”页面，单击“创建密钥对”。

说明

密钥对包括私有密钥对和账户密钥对。私有密钥对仅限本用户使用，账户密钥对账户下其他用户也可使用。

您可以根据业务需要选择创建合适的密钥对。

6. 根据界面提示输入参数。
 - a. 输入密钥对“名称”。
 - b. 输入“密钥对类型”。
 - c. 选择“KMS加密”。

如果同意托管私钥并勾选“我同意将密钥对私钥托管。”则显示该参数，用于对私钥进行加密。

说明

- 若未托管私钥，为保证安全，私钥只能下载一次，请妥善保管。
若不慎遗失，您可以通过[重置密钥对](#)的方式，重新为弹性云服务器绑定密钥对。
 - 若已授权托管私钥，可根据需要将托管的私钥导出使用，详细内容请参见[导出私钥](#)。
- d. 勾选“我已经阅读并同意《密钥对管理服务免责声明》”
7. 单击“确定”

相关操作

- 如果私钥文件丢失，您可以通过“[重置密钥对](#)”功能重新配置弹性云服务器的密钥对。
- 如果私钥文件泄露，您可以通过“[替换密钥对](#)”功能使用新的密钥对替换弹性云服务器内的公钥。

10.3.3 通过 PuTTY Key Generator 工具创建密钥对

操作场景

您可以通过第三方工具puttygen.exe工具创建密钥对，创建完成后，公钥和私钥均保存在用户本地。

说明

通过puttygen.exe工具创建成功的密钥对，还需要执行[导入密钥对](#)，导入系统才能正常使用密钥对。

操作步骤

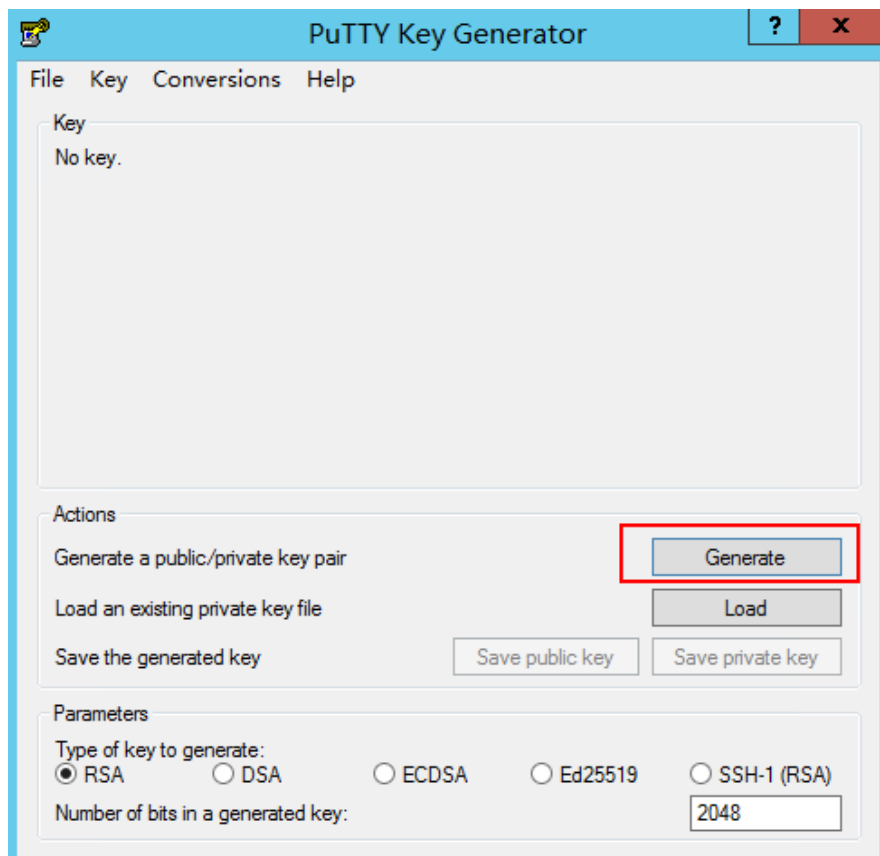
1. 在以下路径中下载并安装PuTTY和PuTTYgen。
<https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>

说明

PuTTYgen是密钥生成器，用于创建密钥对，生成一对公钥和私钥供PuTTY使用。

2. 生成公钥和私钥文件。
 - a. 双击“puttygen.exe”，打开“PuTTY Key Generator”。

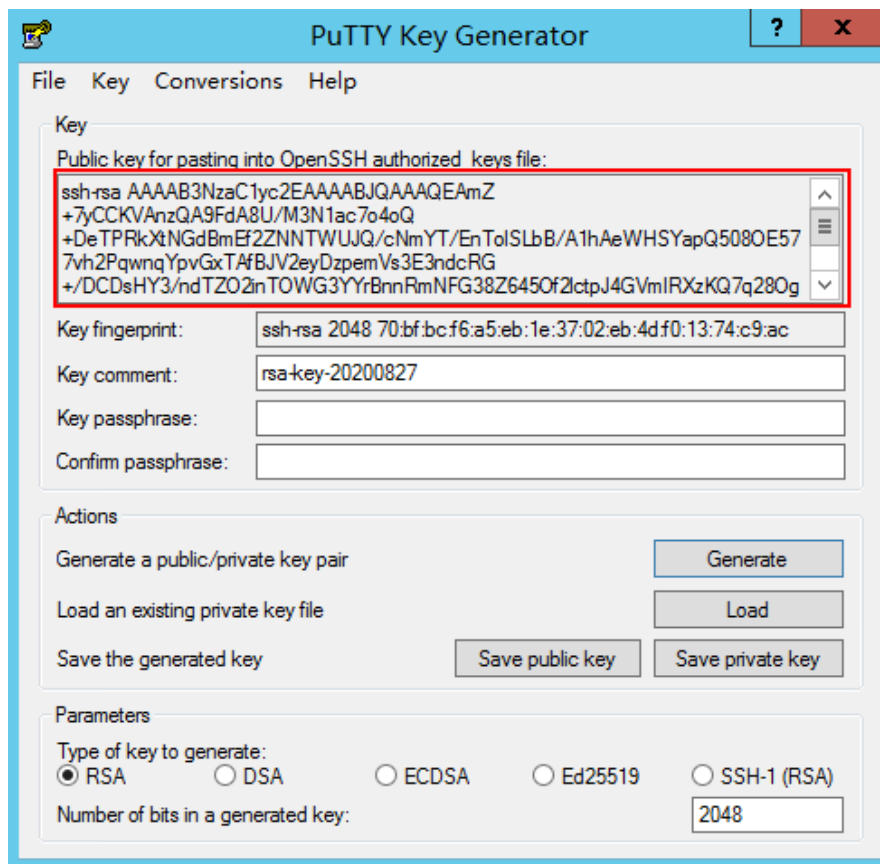
图 10-34 PuTTY Key Generator



- b. 单击“Generate”。

密钥生成器将自动生成一对公钥和私钥，其中，图10-35的红框内容为生成的公钥文件。

图 10-35 生成公钥和私钥文件



3. 复制红框中的公钥内容，并将其粘贴在文本文档中，以.txt格式保存在本地，保存公钥文件。

说明

请勿直接单击“Save public key”保存公钥文件。因为通过puttygen.exe工具的“Save public key”按钮保存在本地的公钥文件，公钥内容的格式会发生变化，不能直接导入管理控制台使用。

4. 保存私钥文件。

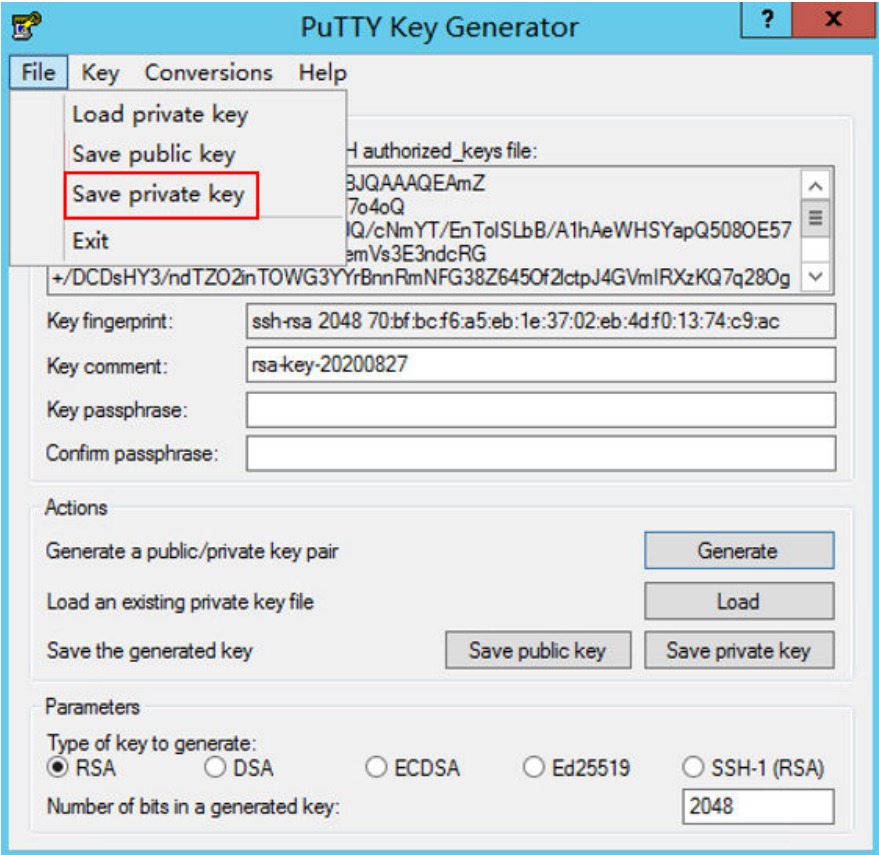
根据不同用途，需将私钥文件保存为不同格式。为保证安全，私钥只能下载一次，请妥善保管。

- 保存私钥文件为“.ppk”格式。

当用户使用PuTTY工具登录Linux弹性云服务器时，需使用“.ppk”格式的私钥文件。保存方法如下：

- i. 在“PuTTY Key Generator”界面，选择“File > Save private key”。

图 10-36 保存私钥文件

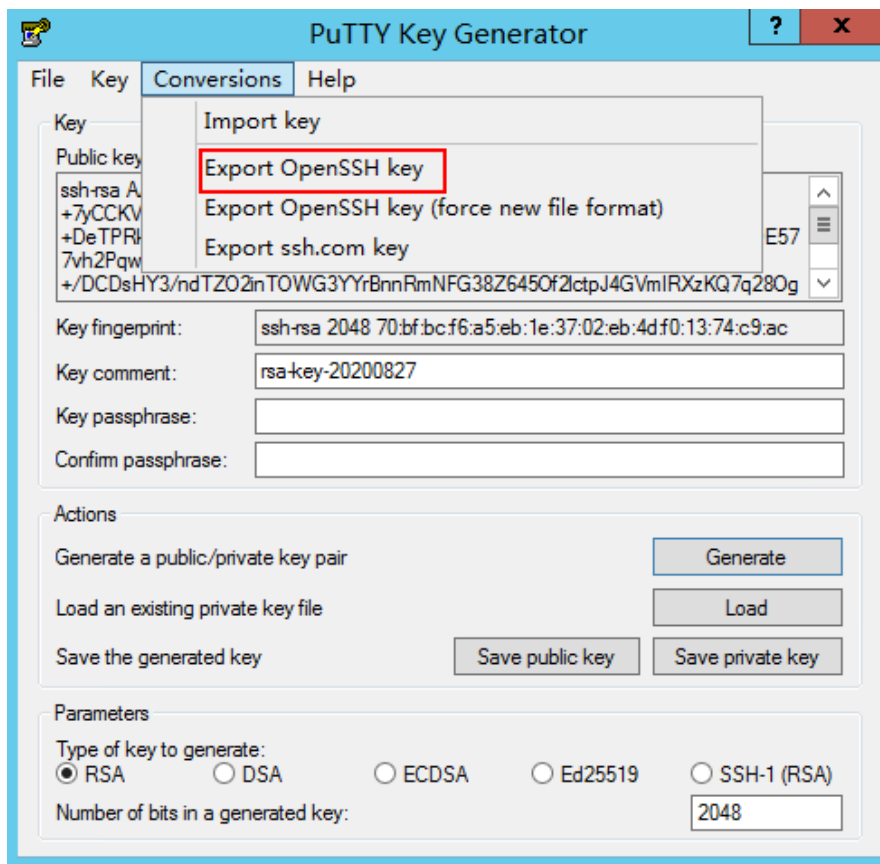


- ii. 保存转化后的私钥到本地。例如：kp-123.ppk
- 保存私钥文件为“.pem”格式。
当用户使用Xshell工具登录Linux弹性云服务器，或者获取Windows弹性云服务器的密码时，需使用“.pem”格式的私钥文件。保存方法如下：
 - i. 选择“Conversions > Export OpenSSH key”。

说明

如果该私钥文件用于Windows弹性云服务器的获取密码操作，在选择“Export OpenSSH key”时，请勿填写“Key passphrase”信息，否则会导致获取密码失败。

图 10-37 保存私钥文件



ii. 保存私钥到本地。例如：kp-123.pem

5. 公钥和私钥文件按照需要正确保存后，请参见[导入密钥对](#)的“复制公钥文件内容方式”，将公钥导入系统中。

相关操作

- 如果私钥文件丢失，您可以通过“[重置密钥对](#)”功能重新配置弹性云服务器的密钥对。
- 如果私钥文件泄露，您可以通过“[替换密钥对](#)”功能使用新的密钥对替换弹性云服务器内的公钥。

10.3.4 导入密钥对

操作场景

以下两种场景，需要执行导入密钥对的操作：

- 通过puttygen.exe工具新建密钥对，需要将密钥对导入系统才能正常使用。
- 如果本地已有密钥对（例如，使用PuTTYgen工具生成的密钥对），可以在管理控制台导入密钥对公钥，由系统维护您的公钥文件。

说明

如果已有密钥对的公钥文件是通过puttygen.exe工具的“Save public key”按钮保存的，该公钥文件不能直接导入管理控制台。

如需继续使用该密钥对作远程身份验证，请参见[通过puttygen.exe工具创建的密钥对，导入管理控制台失败怎么办？](#)

操作步骤

1. 登录管理控制台。
2. 单击“≡”，选择“计算 > 弹性云服务器”。
3. 在左侧导航树中，选择“密钥对”。
4. 在“密钥对管理”页面，单击“导入密钥对”。

图 10-38 导入密钥对



5. 在“导入密钥对”页面，导入公钥内容、私钥内容。
通过单击“选择文件”，可以导入本地保存的公钥文件（例如，[通过PuTTY Key Generator工具创建密钥对](#)的步骤3中保存的“.txt”格式文件）。
更多参数设置，请参见[导入密钥对](#)。

图 10-39 参数设置

×

导入密钥对

密钥对当前免费使用，但有配额限制。首次创建账号密钥对时，需要具有Tenant Administrator系统角色的用户完成一次账号密钥对创建。

导入公钥有两种方式：
1、选择文件导入，导入成功后，可以修改公钥名称。
2、复制内容到“公钥内容”文本框，手工输入公钥名称。
说明：仅支持导入使用RSA算法的密钥，且密钥长度为1024、2048、4096（bit）。

名称

KeyPair-

公钥

选择文件

未选择任何文件

公钥内容

私钥内容

KMS加密

kps/default

查看密钥列表 手工输入

密钥ID a0ff3eb-4804-

☒ 我同意将密钥对私钥托管。[了解详情](#)

 建议开启加密，核心数据更安全，如果您使用KMS加密，超过免费配额会收取相应费用。[价格详情](#)

☒ 我已经阅读并同意《[密钥对管理服务免责声明](#)》

取消

确定

6. 单击“确定”，完成密钥对的导入。

相关链接

- [无法导入密钥对，怎么办？](#)
- [通过puttygen.exe工具创建的密钥对，导入管理控制台失败怎么办？](#)

10.3.5 获取和清除云服务器密码（Windows）

10.3.5.1 获取 Windows 弹性云服务器的密码

操作场景

登录Windows操作系统的弹性云服务器时，需使用密码方式登录。因此，用户需先根据创建弹性云服务器时使用的私钥文件，获取该弹性云服务器初始安装时系统生成的管理员密码（Administrator账户或Cloudbase-init设置的账户）。该密码为随机密码，安全性高，请放心使用。

请根据您的个人需求，通过管理控制台或API方式获取Windows弹性云服务器的初始密码，获取方法请参见本节内容。

前提条件

已获取创建弹性云服务器时使用的私钥文件（.pem文件）。

私钥文件（.pem文件）与创建弹性云服务器时选择的密钥对有关，在创建密钥对时生成。密钥对的创建和使用方法，请参见[密钥对使用场景介绍](#)。

若私钥文件不慎遗失，可以通过[重置密钥对](#)的方式，重新为弹性云服务器绑定密钥对。若已授权托管私钥，可根据需要将托管的私钥导出使用，详细内容请参见[导出私钥](#)。

通过管理控制台获取密码

1. 获取创建弹性云服务器时使用的私钥文件（.pem文件）。
2. 登录管理控制台。
3. 单击管理控制台左上角的 ，选择区域和项目。
4. 单击 ，选择“计算 > 弹性云服务器”。
5. 在弹性云服务器列表，选择待获取密码的弹性云服务器。
6. 在“操作”列，单击“更多 > 密码管理 > 获取密码”。

图 10-40 获取密码



 说明

如果不显示“获取密码”，可能是由于弹性云服务器未安装一键式重置密码插件。

您可以参考[重置Windows云服务器密码（未安装重置密码插件）](#)为弹性云服务器重置密码。

7. 通过私钥文件获取密码，获取方法有如下两种：
 - 单击“选择文件”，从本地上传私钥文件。
 - 将私钥文件内容复制粘贴在空白框中。
8. 单击“获取密码”，获取随机密码。

通过 API 方式获取密码

1. 获取创建弹性云服务器时使用的私钥文件（.pem文件）。
2. 设置调用接口的环境。
3. 具体方法请参见《弹性云服务器接口参考》的“接口调用方法”。
4. 获取密文密码。

调用获取密码的接口，获取密钥的公钥加密后的密文密码。该密文密码是通过RSA算法加密的。其中，URI格式为“GET /v2/{project_id}/servers/{server_id}/os-server-password”。

 说明

调用接口的具体方法请参见《弹性云服务器接口参考》的“[Windows云服务器获取密码](#)”章节。

5. 解密密文密码。

通过创建云服务器时使用的密钥的私钥文件对4中获取的密文密码进行解密。

 - a. 使用OpenSSL工具，执行以下命令，将密文密码转换为.key -nocrypt格式。
openssl pkcs8 -topk8 -inform PEM -outform DER -in rsa_pem.key -out pkcs8_der.key -nocrypt
 - b. 调用Java类库org.bouncycastle.jce.provider.BouncyCastleProvider，使用密钥文件，编写代码解密密文。

10.3.5.2 清除 Windows 弹性云服务器的密码

操作场景

为安全起见，建议用户获取初始密码后，执行清除密码操作，清除系统中记录的初始密码信息。

该操作不会影响弹性云服务器的正常登录与运行。清除密码后，系统不能恢复获取密码功能，因此，请在执行清除密码操作前，记录弹性云服务器密码信息。

操作步骤

1. 登录管理控制台。
2. 单击管理控制台左上角的，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”。

4. 在弹性云服务器列表，选择待获取密码的弹性云服务器。
5. 选择“操作 > 更多”，单击“清除密码”。
系统弹窗提示用户是否确认清除密码。
6. 单击“确定”，执行清除密码操作。

11 启动模板管理

11.1 启动模板概述

什么是启动模板？

启动模板是可用于快速创建实例的模板。模板中包含了创建实例所需的配置信息，包括实例类型、网络配置、密钥对（不包含密码）等信息。

创建后的启动模板无法进行修改，您可以根据实际需要创建多个启动模板，每个模板均可配置不同的参数。

创建启动模板的方法

在控制台创建启动模板

具体操作请参考[创建启动模板](#)。

11.2 创建启动模板

操作场景

本节操作介绍在管理控制台创建启动模板的操作步骤。

约束限制

- 每个账号在每个区域最多可创建30个启动模板。
- 创建启动模板时，所有配置项均为可选。
但如果缺失了创建实例的必要参数，例如规格、镜像类型，那么在使用该模板创建实例时需重新设置这些缺失的配置项。
- 如果包含以下任一配置项，则不支持保存为启动模板：计费模式为包年/包月、竞价类型为竞价模式、配置了主机安全、登录凭证为密码。
- 启动模板创建成功后，不支持修改。
- 支持的区域包括：华北-乌兰察布一、华东-上海一、华东-上海二、华南-广州、西南-贵阳一。

通过控制台创建启动模板

1. 登录管理控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”。
4. 在左侧导航树中，选择“启动模板”。
5. 在“启动模板”页面，单击“创建模板”。
6. 在创建启动模板页面，完成相关参数配置。
各参数含义可以参考[自定义购买ECS](#)。
7. 在页面右侧的“配置概要”中，查看配置详情。
未设置的必选字段会通过红色字体进行提示，需在参数配置区域进行设置。
8. 勾选协议并单击“立即创建”。
返回启动模板列表，可查看到已创建的启动模板。

通过 ECS 的自定义购买页面创建启动模板

您还可以选择在创建云服务器时将实例的配置保存为启动模板。

1. 登录管理控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”。
4. 单击“购买弹性云服务器”，系统进入购买页面。
5. 在自定义购买页面完成云服务器的相关参数配置。
各参数含义可以参考[自定义购买ECS](#)。
6. 在页面右侧的“配置概要”中，查看配置详情。
未设置的必选字段会通过红色字体进行提示，需在参数配置区域进行设置。
7. 在“配置概要”右上角单击 ，再单击“保存为启动模板”。
8. 阅读协议并单击“同意并立即购买”。
9. 输入“模板名称”和“模板描述”后，单击“确定”。
在启动模板列表页即可查看已创建的模板。

11.3 管理启动模板

操作场景

启动模板支持以下操作：

- [查看启动模板详情](#)
- [删除启动模板](#)

查看启动模板详情

1. 登录管理控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。
3. 单击 “”，选择“计算 > 弹性云服务器”。
4. 在左侧导航树中，选择“启动模板”。
5. 在“启动模板”页面，单击模板名称，查看启动模板的详情。

表 11-1 启动模板详情

参数	说明
模板名称	启动模板名称。
模板ID	启动模板ID。
创建时间	启动模板的创建时间。
描述	自定义的启动模板的描述信息。
版本信息	版本信息中包含了当前版本模板的配置信息，例如区域、规格、镜像类型等配置信息。

删除启动模板

1. 登录管理控制台。
2. 单击 “”，选择“计算 > 弹性云服务器”。
3. 在左侧导航树中，选择“启动模板”。
4. 找到要删除的启动模板，在操作列下单击“删除”。
5. 单击“确定”。

12 智能购买组管理

12.1 智能购买组概述

什么是智能购买组？

智能购买组是一种新的算力获取方式，通过自定义配置，可以自动化获得不同可用区、不同实例类型以及不同计费模式的算力。极大程度降低投入成本，同时简化算力获取方式。

应用场景

智能购买组适用于图像渲染、无状态Web服务、基因测序、离线分析、函数计算、批量计算、样本分析、CI/CD与测试等场景。

使用须知

- 智能购买组可以跨可用区部署实例，但是不可以跨区域部署实例。
- 每个智能购买组的目标容量限制：
 - 如果以实例个数为目标容量最多创建500台实例。
 - 如果以vCPUs为目标容量最大创建40000vCPUs。
- 每个智能购买组最多指定一个启动模板。

智能购买组的优势

- 支持使用跨计费模式的实例部署集群
华为云提供了多种计费模式：其中竞价计费型实例成本低，但存在中断回收机制，当市场价格高于报价或库存资源不足就会被中断回收。按需实例可以随时创建和删除，库存充足稳定，但价格高于竞价实例。
智能购买组实现了同时搭配使用竞价计费型实例和按需实例，既可保证最低算力，同时又兼具性价比和实例灵活性。
- 支持使用跨可用区的实例部署集群
智能购买组支持跨可用区部署实例集群，提高了集群的容灾能力。
- 支持使用多种类型实例部署集群

智能购买组支持选择多种类型的实例规格，可满足不同的使用场景。

- 灵活的实例分配策略

智能购买组设置多种实例分配策略以满足更多形态的业务需求。

支持设置集群目标容量、竞价计费型实例目标容量和按需实例目标容量。支持设置智能购买组的目标容量保持策略，即支持在与目标容量有差异时自动补齐对应容量的实例或释放超过容量的实例。

- 高性价比

智能购买组支持设置实例的分配策略为“最低价格策略”，确保智能购买组购买的所有实例的价格总和最低。

计费说明

智能购买组免费，但由智能购买组创建的实例正常计费。

具体请参考[弹性云服务器产品价格详情](#)。

12.2 创建智能购买组

操作场景

本节操作介绍在管理控制台创建智能购买组的操作步骤。

约束与限制

支持的区域包括：华北-乌兰察布一、华东-上海一、华东-上海二、华南-广州、西南-贵阳一。

操作步骤

1. 登录管理控制台。
2. 单击管理控制台左上角的，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”。
4. 在左侧导航树中，选择“智能购买组”。
5. 在“智能购买组”页面，单击“创建智能购买组”。
6. 设置智能购买组名称。
智能购买组的名称，长度为2~64个字符，只能包含中文、字母、数字、下划线（_）和中划线（-）。
7. 设置目标容量。
计划使用智能购买组交付的算力，您可以指定实例个数或vCPU数量。
勾选“使用按需实例提供部分算力”后，需设置按需实例容量，按需实例可以保证智能购买组的最低算力需求。
目标容量决定智能购买组交付的算力总和，以及竞价实例和按需实例的算力占比。
每个智能购买组的目标容量限制：
 - 如果以实例个数为目标容量最多创建500台实例。

- 如果以vCPUs为目标容量最大创建40000vCPUs。
 - 8. 选择启动模板。
智能购买组需要选择一个实例启动模板和对应的版本作为配置来源，您还可以基于该启动模板自定义多个可选的实例配置。
 - 9. 设置实例分配策略。
 - 最低价格策略：智能购买组购买的所有实例的价格总和最低。
 - 多可用区均衡策略：智能购买组购买的实例在多个可用区之间均匀分配算力。
 - 容量优化策略：智能购买组购买的实例按照大规格优先进行购买。
即目标容量为实例个数时智能购买组的vCPU容量最大；目标容量为vCPU太小时智能购买组的实例个数最小。
 - 10. 选择智能购买组类型。
 - 一次性交付：智能购买组仅在启动时尝试一次性创建目标容量的实例，即使未达到目标容量也不再重试。
 - 持续保持：智能购买组实时监控当前集群的容量与目标容量，如未达到目标容量继续创建实例，直至满足目标容量。如果超出目标容量则自动缩容至目标容量。
 - 11. 选择启动时间。
智能购买组开始创建实例的时间，与结束时间结合使用，确定智能购买组的有效时段。
 - 立即启动：智能购买组创建成功后立即启动。
 - 指定启动时间：自定义智能购买组的启动时间。
 - 12. 选择结束时间。
与启动时间结合使用，确定智能购买组的有效时段。
 - 无限期：智能购买组长期有效。
 - 指定结束时间：自定义智能购买组的过期时间。
 - 13. 设置全局竞价实例价格上限。
智能购买组内竞价实例的价格上限。当智能购买组内某一竞价实例的市场价格高于该价格上限时，该竞价实例将被中断回收。
如果同时设置了单个竞价实例的价格上限和全局竞价实例的价格上限，则以单个竞价实例的价格上限为准。
设置的竞价实例的价格上限不得小于0，如果高于按需实例价格，代表对竞价实例价格上限无约束限制。
 - 14. 智能购买组内实例释放设置。
 - 智能购买组过期时释放实例：当设置了智能购买组的结束时间时，如果智能购买组超过有效时间，即删除组内实例。
 - 超过容量时释放实例：当智能购买组的实例个数/vCPU之和超过目标容量时，即删除超出容量的实例。
-  **说明**
- 如果不勾选超过容量时释放实例，那么当智能购买组超过目标容量时，超过容量的实例将被移出智能购买组，但并不释放。在ECS列表页面可以查询到被移出的实例，如需停止计费，请手动删除。
15. 单击“立即创建”。

执行结果

智能购买组创建成功后，会在您指定的时间启动并交付集群。如果您选择了持续保持模式，智能购买组会实时监控当前集群的容量与目标容量，在竞价实例被回收时自动创建新的实例。

12.3 管理智能购买组

操作场景

智能购买组支持以下操作：

- [查看智能购买组详情](#)
- [修改智能购买组](#)
- [删除智能购买组](#)

查看智能购买组详情

1. 登录管理控制台。
2. 单击“”，选择“计算 > 弹性云服务器”。
3. 在左侧导航树中，选择“智能购买组”。
4. 在智能购买组列表页面，单击智能购买组名称，查看智能购买组的详情。

在详情页面可以查看智能购买组的基本信息和容量配置信息。

基本信息包括智能购买组名称、使用的启动模板、智能购买组类型、实例分配策略等信息。

在容量配置信息中可以查看当前容量与目标容量，竞价实例/按需实例的当前容量和目标容量等信息。

修改智能购买组

1. 登录管理控制台。
 2. 单击“”，选择“计算 > 弹性云服务器”。
 3. 在左侧导航树中，选择“智能购买组”。
 4. 找到智能购买组，在操作列下单击“修改”。
- 支持修改智能购买组名称、目标容量、按需实例容量、全局竞价实例的价格上限、智能购买组过期时释放实例、超过容量时释放实例。
5. 修改完后单击“是”。

删除智能购买组

1. 登录管理控制台。
2. 单击“”，选择“计算 > 弹性云服务器”。
3. 在左侧导航树中，选择“智能购买组”。
4. 找到智能购买组，在操作列下单击“删除”。

5. 选择是否删除智能购买组内实例。
如果选择不删除实例，您可以在ECS列表页查看保留的实例，如需停止实例计费请手动删除实例。
6. 单击“是”。

13 事件管理

13.1 事件概述

在日常运维中，华为云会对ECS实例所在底层宿主机的软硬件故障进行预测和主动规避。

当宿主机上的故障风险无法规避时，为避免因ECS实例的资源可用性或性能受损对您的业务造成的更大影响，系统会对受影响的实例生成事件并进行上报，例如实例重部署、本地盘换盘等，事件详细内容请参见[事件类型](#)。系统上报事件不会频繁发生。

您可通过云服务器控制台查看事件详情，包括事件类型，实例ID、事件状态等信息。也可以通过云监控服务的“事件监控”查看ECS实例的事件，详细内容请参见[查看事件监控数据](#)。

事件类型

系统支持上报的事件如[表13-1](#)所示。

表 13-1 支持系统上报的事件

事件类型	事件说明	事件影响	用户侧处理建议
实例重部署	当系统检测到ECS实例的底层宿主机异常，计划将ECS实例部署到新主机时，会自动上报实例重部署事件。	实例重部署过程中，云服务器将会有短暂时间不可用。 系统会在计划事件执行时间前24~72小时发送该系统事件通知。 须知 对于包含本地盘的实例，会丢失所有本地盘上的数据。	您可以根据业务需要选择如下处理方式，并在事件处理完成后，及时验证业务受损情况，如遇问题，请联系技术支持。 响应实例重部署事件 建议您在授权时选择业务低谷期为开始时间，如不指定将会以当前时间为开始时间。

事件类型	事件说明	事件影响	用户侧处理建议
本地盘换盘	系统检测到磁盘增强型（D系列）ECS实例或裸金属类型ECS实例的底层宿主机存在磁盘故障风险，会对受影响的ECS实例自动生成本地盘换盘事件。	本地盘换盘会丢失本地盘上的数据。	您可以根据业务需要选择如下处理方式，并在事件处理完成后，及时验证业务受损情况，如遇问题，请联系技术支持。 须知 本地盘换盘操作会丢失本地盘上的数据，如果无需保留本地盘数据，可根据业务需要选择如下处理方式。 ● 重部署：会丢失所有本地盘数据 ● 授权换盘：会丢失故障本地盘数据 建议您在授权时选择业务低谷期为开始时间，如不指定将会以当前时间为开始时间。 通常会在开始时间后5个工作日内完成本地盘换盘，请耐心等待。
实例迁移	当系统检测到ECS实例的底层宿主机异常，需要进行重启、关机、下线等系统维护时，计划对ECS实例进行迁移，会自动上报实例迁移事件。	系统会先尝试对云服务器进行热迁移，如遇异常，则会触发HA机制（云服务器将会有短暂时间不可用）。	建议您在事件处理完成后，及时验证业务受损情况，如遇问题，请联系技术支持。

事件类型	事件说明	事件影响	用户侧处理建议
系统维护	系统检测到ECS实例（含裸金属类型实例）的宿主机存在软硬件故障风险，计划对受影响的实例进行维护操作，会自动生成系统维护事件。	系统维护过程中，宿主机可能会进入下电状态，云服务器不可用。	您可以根据业务需要选择如下处理方式，并在事件处理完成后，及时验证业务受损情况，如遇问题，请联系技术支持。 响应系统维护事件 建议您在授权时确保实例的业务已离线并选择业务低谷期为开始时间，如不指定将会以当前时间为开始时间。 不同故障系统维护的耗时不同。通常会在授权开始时间后5个工作日内完成系统维护，请耐心等待。

事件状态

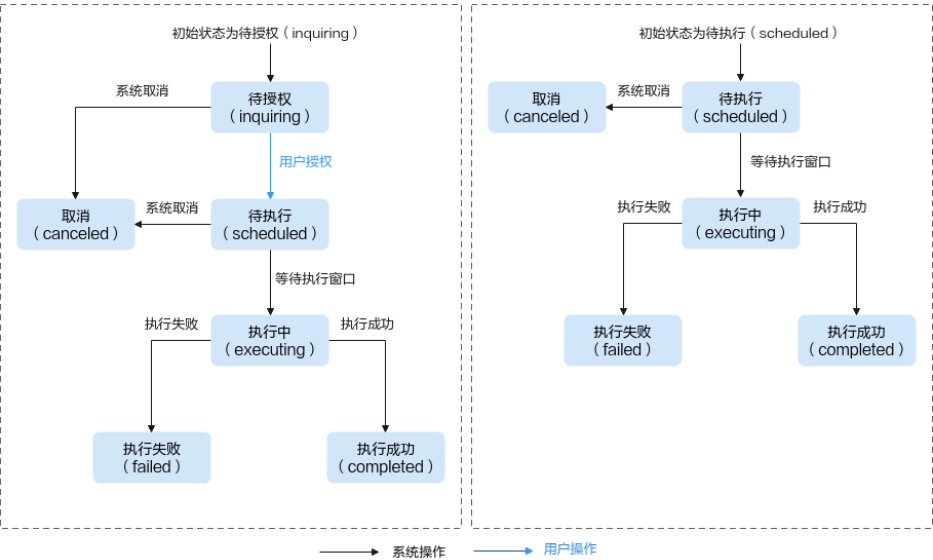
系统上报的事件状态如表13-2所示，您可以根据状态判断系统上报事件的进展，也可以通过状态进行事件筛选。

表 13-2 事件状态

类型	描述
待授权	需要用户对事件操作进行授权，授权时支持指定开始时间，系统会在一定时间内完成操作，详细内容请参见响应事件。
待执行	等待系统资源调度中。
执行中	系统已完成资源调度，正在修复中。
执行成功	系统已完成事件执行。请验证业务受损情况，如遇异常，请联系技术支持。
执行失败	系统自动修复失败。
取消	该事件已被系统取消。

事件状态会随着用户和系统的操作进行变化。

图 13-1 事件状态示意图



13.2 查询事件

操作场景

本文介绍如何通过弹性云服务器的控制台查询系统上报的事件。

您还可以通过云监控服务的“事件监控”查看ECS实例的事件，详细内容请参见[查看事件监控数据](#)。

前提条件

如果您通过IAM用户进行本操作，则需要在操作前对IAM用户进行授权。

查询及响应事件操作依赖以下策略：

- 查询事件：ecs:instanceScheduledEvents:list
- 接受并授权执行事件：ecs:instanceScheduledEvents:accept
- 修改预约时间：ecs:instanceScheduledEvents:update

为IAM用户授权的操作，请参见[ECS自定义策略](#)。

操作步骤

1. 登录管理控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”。
4. 在左侧导航树中，选择“事件”。
在“事件”页面的列表中，可以查看系统上报的事件ID、实例名称、事件类型等信息。
在列表的“操作”列，您可以进行事件的响应操作，详细内容请参见[响应事件](#)。

13.3 响应事件

13.3.1 响应实例重部署事件

操作场景

当系统上报“实例重部署”事件时，您需要对ECS实例进行“授权重部署”操作。

本文介绍如何响应“待授权”状态的“实例重部署”事件，指导您完成实例重部署的授权操作。

授权重部署包括两种模式：

- 立即部署：即系统收到请求后，会立即进行实例重部署。
- 预约部署：即系统收到请求后，会在设置的重部署时间进行实例重部署。
设置重部署时间后，您还可以修改预约时间，详细内容，请参见[修改预约时间](#)。

须知

- 实例重部署大约耗时10分钟，并且会重启实例，请选择合适的时间授权并提前进行业务切流。
- 实例重部署后，实例的系统盘和云硬盘类型的数据盘不受影响。
- 对于包含本地盘的实例，实例重部署后，实例的本地盘数据会被清空。为了保障数据安全，请在授权重部署前进行本地盘数据备份。
详细内容，请参见[本地盘数据备份](#)。
- 对于包含本地盘的实例，授权重部署前需要对本地盘进行[预处理操作](#)，防止重部署后启动云服务器进入Emergency Mode（紧急模式）。

请根据ECS的实例类型，选择授权重部署操作指导：

- [授权重部署（仅包含云硬盘的实例）](#)
- [授权重部署（包含本地盘的实例）](#)

前提条件

如果您通过IAM用户进行本操作，则需要在操作前对IAM用户进行授权。

查询及响应事件操作依赖以下策略：

- 查询事件：ecs:instanceScheduledEvents:list
- 接受并授权执行事件：ecs:instanceScheduledEvents:accept
- 修改预约时间：ecs:instanceScheduledEvents:update

为IAM用户授权的操作，请参见[ECS自定义策略](#)。

授权重部署（仅包含云硬盘的实例）

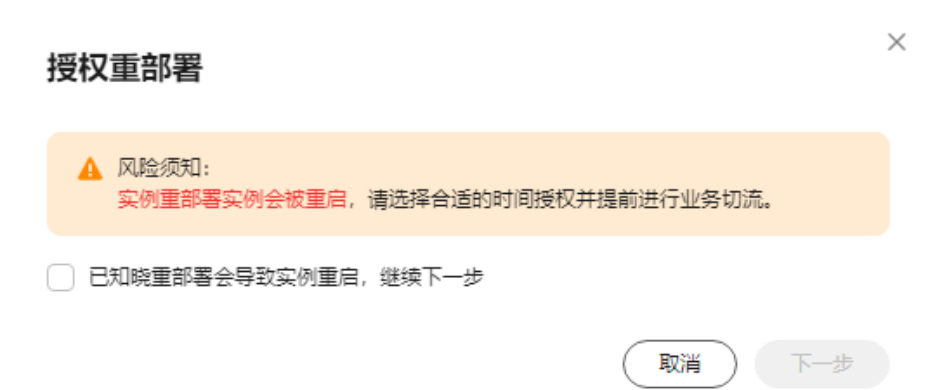
- 1. 登录管理控制台。
- 2. 单击管理控制台左上角的 ，选择区域和项目。
- 3. 单击“”，选择“计算 > 弹性云服务器”。
- 4. 在左侧导航树中，选择“事件”。

图 13-2 事件列表



- 5. 在“事件”页面，单击“”，通过以下条件过滤出待授权的“实例重部署”事件。
 - a. 选择“事件类型 > 实例重部署”。
 - b. 选择“事件状态 > 待授权”。
- 6. 在待授权的事件“操作”列，单击“授权重部署”。

图 13-3 授权重部署



说明

- 在进行“实例重部署”操作之前，请先了解风险须知。
- 7. 了解风险须知后，勾选已知晓风险的提示，并单击“下一步”。
 - 8. 进行“重部署设置”。
 - 选择“立即部署”。即系统收到请求后，会立即进行实例重部署。

图 13-4 立即部署



授权重部署

确定并授权对云服务器ecs-进行实例重部署操作吗？

重部署设置 ☒ 立即部署 ☐ 预约部署

同意授权重部署，请输入 AGREE

AGREE

取消 确定

- 选择“预约部署”，并设置重部署时间。
即系统在收到请求后，会在设置的预约部署时间进行实例重部署。

图 13-5 预约部署



授权重部署

确定并授权对云服务器ecs-进行实例重部署操作吗？

重部署设置 ☐ 立即部署 ☒ 预约部署

设置重部署时间 请选择日期时间

同意授权重部署，请输入 AGREE

AGREE

取消 确定

设置重部署时间后，您还可以修改预约时间，详细内容，请参见[修改预约时间](#)。

9. 输入“AGREE”确定授权实例重部署。
10. 单击“确定”，完成授权重部署。

授权重部署后，“实例重部署”事件更新为“待执行”状态。系统收到授权请求后，会根据授权设置将事件更新为执行中，开始进行实例重部署。

待“实例重部署”事件更新为“执行成功”状态，实例重部署完成，请检查云服务器业务运行情况。

授权重部署（包含本地盘的实例）

1. 登录管理控制台。

2. 单击管理控制台左上角的，选择区域和项目。

3. 单击“”，选择“计算 > 弹性云服务器”。

4. 在左侧导航树中，选择“事件”。

图 13-6 事件列表



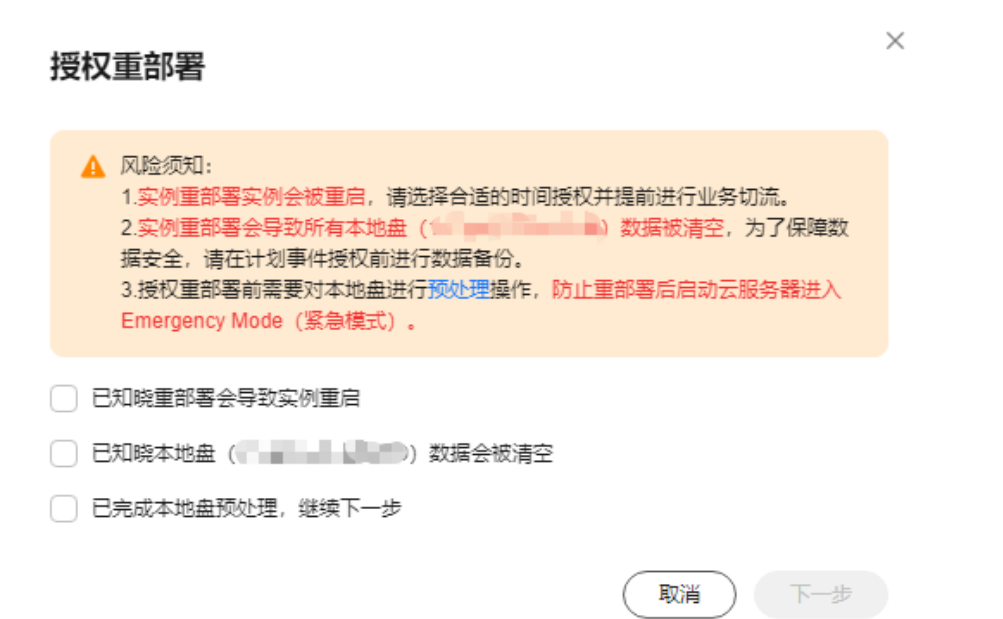
5. 在“事件”页面，单击“”，通过以下条件过滤出待授权的“实例重部署”事件。

a. 选择“事件类型 > 实例重部署”。

b. 选择“事件状态 > 待授权”。

6. 在待授权的事件“操作”列，单击“授权重部署”。

图 13-7 授权重部署



说明

- 在进行“实例重部署”操作之前，请先了解风险须知，并完成本地盘预处理操作，为所有数据盘增加nofail参数。

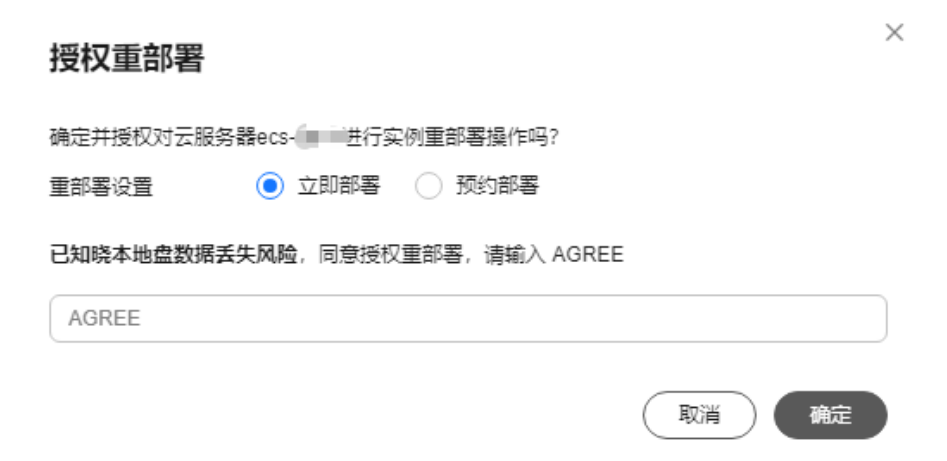
详细内容，请参见[实例重部署预处理](#)。

7. 了解风险须知后，勾选已知晓风险的提示，并单击“下一步”。

8. 进行“重部署设置”。

- 选择“立即部署”。
即系统收到请求后，会立即进行实例重部署。

图 13-8 立即部署



- 选择“预约部署”，并设置重部署时间。
即系统在收到请求后，会在设置的预约部署时间进行实例重部署。

图 13-9 预约部署



设置重部署时间后，您还可以修改预约时间，详细内容，请参见[修改预约时间](#)。

9. 输入“AGREE”确定授权实例重部署。
10. 单击“确定”，完成授权重部署。
授权重部署后，“实例重部署”事件更新为“待执行”状态。系统收到授权请求后，会根据授权设置将事件更新为执行中，开始进行实例重部署。
待“实例重部署”事件更新为“执行成功”状态，实例重部署完成，请检查云服务器业务运行情况。

修改预约时间

完成“预约部署”方式的授权重部署操作后，“实例重部署”事件状态变为“待执行”，此时，您可以修改预约时间。

1. 登录管理控制台。
2. 单击管理控制台左上角的，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”。
4. 在左侧导航树中，选择“事件”。
5. 在“事件”页面，单击“”，通过以下条件过滤出待执行的“实例重部署”事件。
 - a. 选择“事件类型 > 实例重部署”。
 - b. 选择“事件状态 > 待执行”。
6. 在待执行的事件“操作”列，单击“修改预约时间”。

图 13-10 修改预约时间

×

修改预约时间

当前预约执行时间 2024/05/22 10:18:26 GMT+08:00

修改预约执行时间 

可预约最晚时间 2024/05/29 10:18:26 GMT+08:00

取消

确定

7. 设置“修改预约执行时间”，并单击“确定”，完成预约时间的修改。

说明

您需要在“可预约最晚时间”前至少30分钟修改预约时间，否则无法设置。

13.3.2 响应本地盘换盘事件

操作场景

当系统检测到ECS实例（含裸金属类型实例）的本地盘出现软硬件故障时，会对受影响的ECS实例自动生成“本地盘换盘”事件。

本文介绍响应“待授权”状态的“本地盘换盘”事件的方案：

- **授权换盘**：您可以选择通过“授权换盘”操作响应“本地盘换盘”事件，授权更换故障的本地盘。

授权换盘包括两种模式：

- 立即换盘：即系统收到换盘请求后，会在5个工作日内完成换盘操作。
 - 预约换盘：即系统收到换盘请求后，会在预约时间后5个工作日内完成换盘操作。
- 设置预约换盘时间后，您还可以修改预约时间，详细内容，请参见[修改预约时间](#)。

须知

- 本地盘换盘期间，实例的系统盘、云硬盘类型的数据盘以及正常的本地盘不受影响。
 - 本地盘换盘期间，故障本地盘会被卸载并清空所有数据，为了保障数据安全，请提前进行本地盘数据备份。
详细内容，请参见[本地盘数据备份](#)。
 - 磁盘增强型（D系列）的ECS，本地盘换盘期间，实例不会关机，仅故障本地盘不可用。
 - 裸金属类型的ECS，本地盘换盘期间，可能伴随宿主机的下电与重启，在授权前，请确保云服务器中部署的业务离线，或云服务器停止对业务无影响。
如果云服务器上的业务不可停止，请勿授权，并联系技术支持进行处理。
 - 授权换盘前需执行[换盘预处理](#)操作，避免因换盘引起的异常风险。
-
- **重部署**：您可以选择通过“重部署”操作响应“本地盘换盘”事件，授权立即对实例进行重部署。

须知

- 实例重部署操作会重启实例，请选择合适的时间触发并提前进行业务切流。
- 实例重部署操作不会影响实例的系统盘和云硬盘类型的数据盘。
- 实例重部署会导致所有本地盘数据被清空，为了保障数据安全，请在重部署前进行数据备份。
- 实例重部署前需要对本地盘进行[预处理](#)操作，防止重部署后启动云服务器进入Emergency Mode（紧急模式）。

前提条件

如果您通过IAM用户进行本操作，则需要在操作前对IAM用户进行授权。

查询及响应事件操作依赖以下策略：

- 查询事件：ecs:instanceScheduledEvents:list
- 接受并授权执行事件：ecs:instanceScheduledEvents:accept
- 修改预约时间：ecs:instanceScheduledEvents:update

为IAM用户授权的操作，请参见[ECS自定义策略](#)。

授权换盘

1. 登录管理控制台。

2. 单击管理控制台左上角的，选择区域和项目。

3. 单击“”，选择“计算 > 弹性云服务器”。

4. 在左侧导航树中，选择“事件”。

图 13-11 事件列表



5. 在“事件”页面，单击“”，通过以下条件过滤出待授权的“本地盘换盘”事件。

a. 选择“事件类型 > 本地盘换盘”。

b. 选择“事件状态 > 待授权”。

6. 在待授权的事件“操作”列，单击“授权换盘”。

图 13-12 授权换盘（磁盘增强型实例）

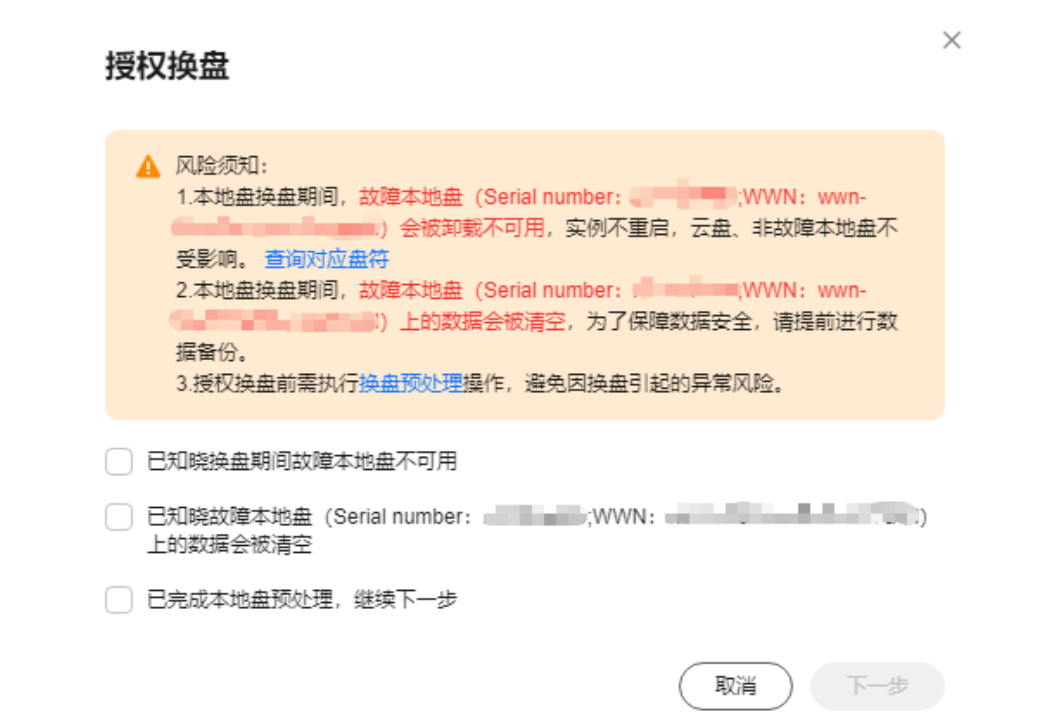


图 13-13 授权换盘（裸金属类型实例）



说明

- 在进行“授权换盘”操作之前，请先了解风险须知，并完成换盘预处理操作：
- 如需保留本地盘上的数据，请先备份故障本地盘的数据。
 - 在云服务器的/etc/fstab中，注释掉故障本地盘对应的挂载点，防止换盘后启动云服务器时进入维护模式。
 - 在云服务器操作系统内部，使用umount命令，卸载故障本地盘对应的设备或者文件系统。
- 请根据实例类型，选择对应的预处理操作指导，详细内容，请参见[换盘预处理](#)。
7. 了解风险须知后，勾选已知晓风险的提示，并单击“下一步”。
8. 进行“授权设置”。
- 选择“立即换盘”。
- 即系统收到换盘请求后，会在5个工作日内完成换盘操作。

图 13-14 立即换盘



- 选择“预约换盘”，并设置换盘时间。
即系统收到换盘请求后，会在预约时间后5个工作日内完成换盘操作。

图 13-15 预约换盘



设置预约换盘时间后，您还可以修改预约时间，详细内容，请参见[修改预约时间](#)。

- 9. 输入“AGREE”确定授权本地盘换盘。
- 10. 单击“确定”，完成授权换盘。
授权换盘后，“本地盘换盘”事件更新为“待执行”状态。系统收到换盘请求后，会根据授权设置将事件更新为执行中，开始进行换盘。
待“本地盘换盘”事件更新为“执行成功”状态，本地盘换盘完成，请检查云服务器业务运行情况。

重部署

- 1. 登录管理控制台。
- 2. 单击管理控制台左上角的 ，选择区域和项目。
- 3. 单击 ，选择“计算 > 弹性云服务器”。
- 4. 在左侧导航树中，选择“事件”。

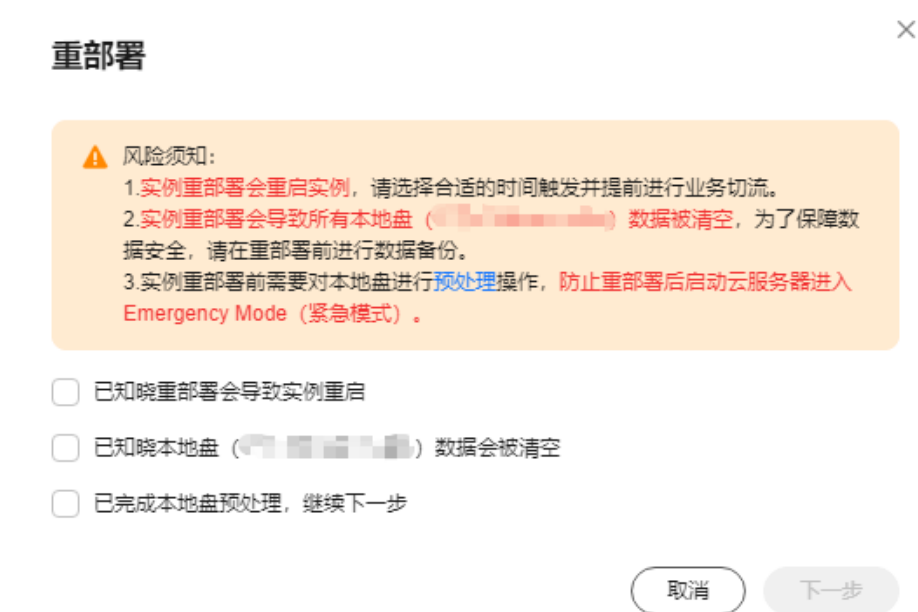
图 13-16 事件列表



- 5. 在“事件”页面，单击 ，通过以下条件过滤出待授权的“本地盘换盘”事件。

- a. 选择“事件类型 > 本地盘换盘”。
- b. 选择“事件状态 > 待授权”。
6. 在事件“操作”列，单击“重部署”。

图 13-17 重部署



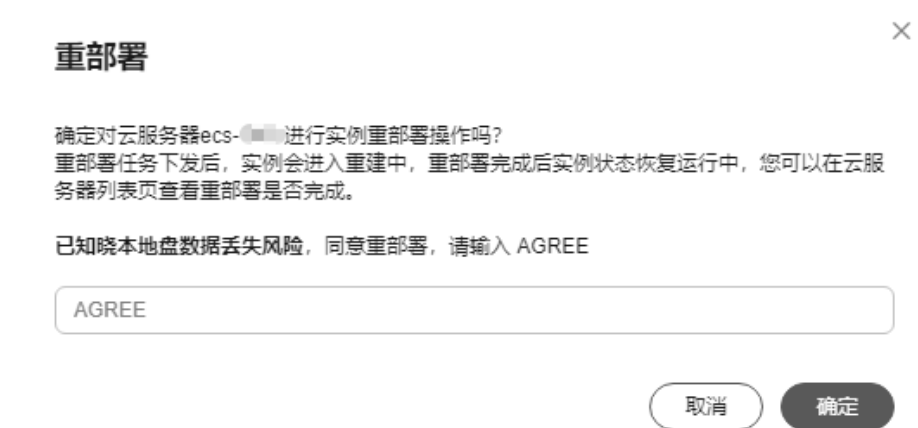
说明

在进行“重部署”操作之前，请先了解本地盘数据丢失风险，完成实例重部署预处理操作，为所有数据盘增加nofail参数。

详细内容，请参见[实例重部署预处理](#)。

7. 了解风险须知后，勾选已知晓风险提示，并单击“下一步”。
8. 输入“AGREE”确定进行实例重部署操作。

图 13-18 确定实例重部署



9. 单击“确定”。

确定实例重部署后，“本地盘换盘”事件更新为“待执行”状态。系统收到重部署请求后，会将事件更新为执行中，开始进行实例重部署。

待“本地盘换盘”事件更新为“执行成功”状态，实例重部署完成，请检查云服务器业务运行情况。

修改预约时间

完成“预约换盘”方式的授权换盘操作后，“本地盘换盘”事件状态变为“待执行”，此时，您可以修改预约换盘时间。

1. 登录管理控制台。
2. 单击管理控制台左上角的，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”。
4. 在左侧导航树中，选择“事件”。
5. 在“事件”页面，单击“”，通过以下条件过滤出待执行的“本地盘换盘”事件。
 - a. 选择“事件类型 > 本地盘换盘”。
 - b. 选择“事件状态 > 待执行”。
6. 在待执行的事件“操作”列，单击“修改预约时间”。

图 13-19 修改预约时间

修改预约时间

当前预约执行时间 2024/05/22 10:18:26 GMT+08:00

修改预约执行时间 

可预约最晚时间 2024/05/29 10:18:26 GMT+08:00

取消

确定

7. 设置“修改预约执行时间”，并单击“确定”，完成预约换盘时间的修改。

说明

您需要在“可预约最晚时间”前至少30分钟修改预约时间，否则无法设置。

13.3.3 响应系统维护事件

操作场景

当系统上报“系统维护”事件时，您需要对ECS实例（含裸金属类型实例）进行“授权维护”操作。

本文介绍如何响应“待授权”状态的“系统维护”事件，指导您完成系统维护的授权操作。

授权维护包括两种模式：

- 立即授权维护：即系统收到请求后，会在5个工作日内完成实例宿主机的系统维护。
- 预约授权维护：即系统收到请求后，会在设置的预约维护时间后5个工作日内完成实例宿主机的系统维护。

设置预约维护时间后，您还可以修改预约时间，详细内容，请参见[修改预约时间](#)。

须知

系统维护操作需要对主机进行下电，在此期间云服务器将停止无法工作。在授权维护前，请确保云服务器中部署的业务离线或云服务器停止对业务无影响。
如果云服务器上的业务不可停止，请勿授权，并联系技术支持进行处理。

前提条件

如果您通过IAM用户进行本操作，则需要在操作前对IAM用户进行授权。

查询及响应事件操作依赖以下策略：

- 查询事件：ecs:instanceScheduledEvents:list
- 接受并授权执行事件：ecs:instanceScheduledEvents:accept
- 修改预约时间：ecs:instanceScheduledEvents:update

为IAM用户授权的操作，请参见[ECS自定义策略](#)。

授权维护

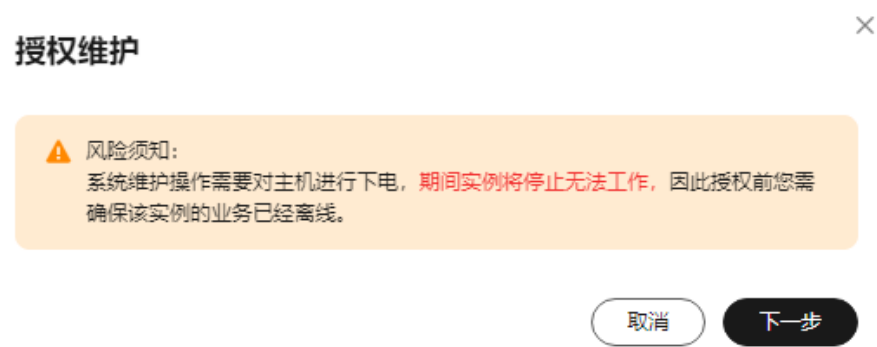
- 登录管理控制台。
- 单击管理控制台左上角的，选择区域和项目。
- 单击“”，选择“计算 > 弹性云服务器”。
- 在左侧导航树中，选择“事件”。

图 13-20 事件列表



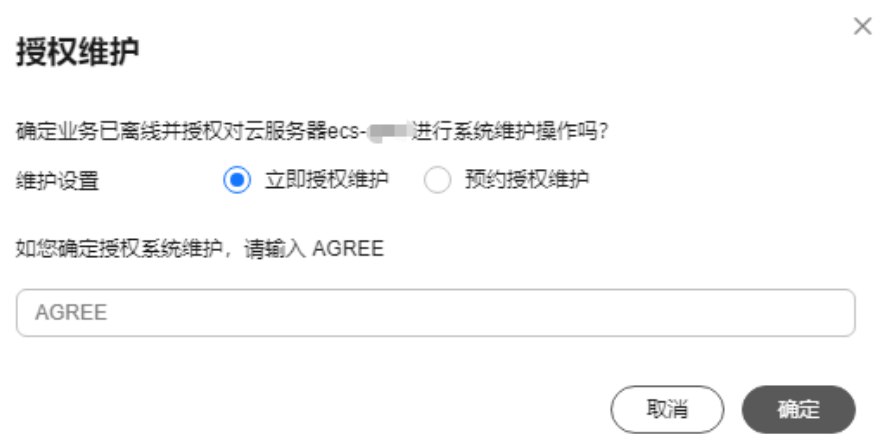
5. 在“事件”页面，单击“”，通过以下条件过滤出待授权的“系统维护”事件。
- a. 选择“事件类型 > 系统维护”。
- b. 选择“事件状态 > 待授权”。
6. 在待授权的事件“操作”列，单击“授权维护”。

图 13-21 授权维护



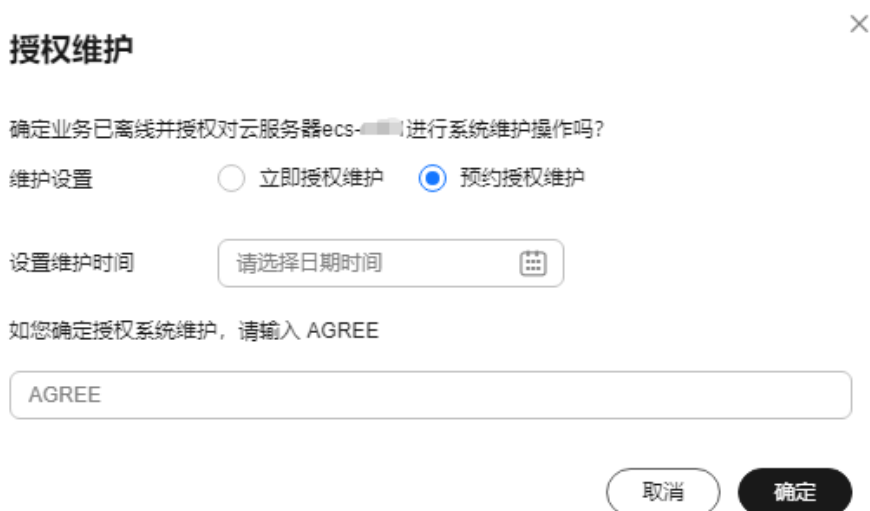
7. 了解风险须知后，单击“下一步”。
8. 进行“维护设置”。
- 选择“立即授权维护”。
- 即系统收到请求后，会在5个工作日内完成实例宿主机的系统维护。

图 13-22 立即授权维护



- 选择“预约授权维护”，并设置维护时间。
- 即系统在收到请求后，会在设置的预约维护时间后5个工作日内完成系统维护操作。

图 13-23 预约授权维护



授权维护

确定业务已离线并授权对云服务器ecs-进行系统维护操作吗?

维护设置 ☐ 立即授权维护 ☒ 预约授权维护

设置维护时间

如您确定授权系统维护, 请输入 AGREE

设置预约维护时间后, 您还可以修改预约时间, 详细内容, 请参见[修改预约时间](#)。

9. 输入“AGREE”确定授权系统维护。
10. 单击“确定”, 完成授权维护。

授权维护后, “系统维护”事件更新为“待执行”状态。系统收到授权请求后, 会根据授权设置将事件更新为执行中, 开始进行系统维护。

待“系统维护”事件更新为“执行成功”状态, 系统维护完成, 请检查云服务器业务运行情况。

修改预约时间

完成“预约授权维护”方式的授权维护操作后, “系统维护”事件状态变为“待执行”, 此时, 您可以修改预约时间。

1. 登录管理控制台。
2. 单击管理控制台左上角的 , 选择区域和项目。
3. 单击“”, 选择“计算 > 弹性云服务器”。
4. 在左侧导航树中, 选择“事件”。
5. 在“事件”页面, 单击“”, 通过以下条件过滤出待执行的“系统维护”事件。
 - a. 选择“事件类型 > 系统维护”。
 - b. 选择“事件状态 > 待执行”。
6. 在待执行的事件“操作”列, 单击“修改预约时间”。

图 13-24 修改预约时间

×

修改预约时间

当前预约执行时间2024/05/22 10:18:26 GMT+08:00

修改预约执行时间

2024/05/22 10:18:26

可预约最晚时间2024/05/29 10:18:26 GMT+08:00

取消

确定

7. 设置“修改预约执行时间”，并单击“确定”，完成预约时间的修改。

说明

您需要在“可预约最晚时间”前至少30分钟修改预约时间，否则无法设置。

13.4 换盘预处理

13.4.1 本地盘换盘预处理（磁盘增强型实例）

操作场景

当进行“本地盘换盘”事件的“授权换盘”操作时，需要先对本地盘进行换盘预处理。

本文介绍如何对磁盘增强型（D系列）的ECS实例进行本地盘的换盘预处理操作。

须知

本地盘换盘操作会丢失故障本地盘上的数据，如果无需保留本地盘上的数据，可通过本操作换盘预处理。
如果需要保留本地盘上的数据，请结束操作并联系技术支持进行处理。

操作步骤（Linux 实例）

获取故障本地盘信息

- 1. 登录管理控制台。
- 2. 单击管理控制台左上角的，选择区域和项目。
- 3. 单击“”，选择“计算 > 弹性云服务器”。
- 4. 在左侧导航树中，选择“事件”。

5. 在事件列表中，查看“本地盘换盘”事件的“事件描述”列。
通过“事件描述”信息获取故障本地盘的WWN号，本文以“wwn-0x5000c500e01a4930”为例进行介绍。

获取故障盘挂载点

1. [远程登录](#)待换盘预处理的弹性云服务器。
2. 执行以下命令，查看故障本地盘的WWN号对应的盘符信息。

ll /dev/disk/by-id/ | grep WWN号

以WWN号“wwn-0x5000c500e01a4930”为例，命令如下：

ll /dev/disk/by-id/ | grep wwn-0x5000c500e01a4930

回显信息如下：

```
lrwxrwxrwx 1 root root 9 May 13 14:05 wwn-0x5000c500e01a4930 -> ../../sdb
```

3. 执行以下命令，查询故障本地盘的挂载点。

df -Th | grep 盘符信息

以盘符信息“/dev/sdb”为例，命令如下：

df -Th | grep /dev/sdb

回显信息如下：

```
/dev/sdb ext4 3.6T 28K 3.4T 1% /data
```

须知

本地盘的换盘预处理会导致本地盘数据丢失。如需保留本地盘数据，请结束操作并联系技术支持进行处理。

卸载故障的本地磁盘

1. 执行以下命令，卸载故障本地盘。

umount 挂载点

以挂载点“/data”为例，命令如下：

umount /data

检查报障云服务器的/etc/fstab中是否配置了故障盘对应的自动挂载信息

说明

如果报障云服务器的/etc/fstab中配置了故障盘对应的自动挂载信息，则需要删除或注释掉，防止本地盘换盘后启动云服务器进入Emergency Mode（紧急模式）。

1. 执行以下命令，查询磁盘分区的UUID。

blkid 磁盘分区

以查询磁盘分区“/dev/sdb”的UUID为例，命令如下：

blkid /dev/sdb

回显信息如下：

```
/dev/sdb: UUID="626c4774-e60e-4d86-bbe6-031bac126e4c" TYPE="ext4"
```

2. 执行以下命令，查询/etc/fstab中是否存在磁盘分区的自动挂载信息。

cat /etc/fstab | grep 磁盘分区的UUID

以查询磁盘分区的UUID “626c4774-e60e-4d86-bbe6-031bac126e4c” 为例，命令如下：

```
cat /etc/fstab | grep 626c4774-e60e-4d86-bbe6-031bac126e4c
```

回显信息如下，表示/etc/fstab中存在磁盘分区的自动挂载信息：

```
UUID=626c4774-e60e-4d86-bbe6-031bac126e4c /mnt ext4 defaults 0 0
```

3. 如果存在自动挂载信息，执行以下命令，删除磁盘分区的自动挂载信息，避免在更换本地盘后，云服务器开机时进入Emergency Mode（紧急模式）。

- a. 执行以下命令，编辑/etc/fstab文件。

```
vi /etc/fstab
```

- b. 单击“i”进入编辑模式。
- c. 删除或注释掉步骤2中查询的磁盘分区的自动挂载信息。

在自动挂载信息前面添加#，表示注释掉自动挂载信息，示例如下：

```
# UUID=626c4774-e60e-4d86-bbe6-031bac126e4c /mnt ext4 defaults 0 0
```

- d. 单击Esc键并输入:wq后回车，保存并退出编辑模式。

操作步骤（Windows 实例）

获取故障盘标识符

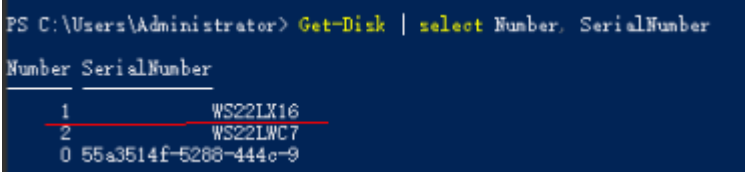
1. 登录管理控制台。
2. 单击管理控制台左上角的，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”。
4. 在左侧导航树中，选择“事件”。
5. 在事件列表中，查看“本地盘换盘”事件的“事件描述”列。
通过“事件描述”信息获取故障本地盘的SN号，本文以“WS22LX16”为例进行介绍。

获取磁盘编号，确认影响范围

1. [远程登录](#)待换盘预处理的弹性云服务器。
2. 以管理员身份打开“Windows PowerShell”，查询磁盘编号和SN号的对应关系，获取磁盘编号。

```
Get-Disk | select Number, SerialNumber
```

图 13-25 查询磁盘编号和 SN 号的对应关系



Number	SerialNumber
1	WS22LX16
2	WS22LWC7
0	55a3514f-5288-444e-9

须知

本地盘换盘操作会导致本地盘数据丢失。如需保留本地盘数据，请结束操作并联系技术支持进行处理。

13.4.2 本地盘换盘预处理（裸金属类型实例）

操作场景

当进行“本地盘换盘”事件的“授权换盘”操作时，需要先对本地盘进行换盘预处理。

本文介绍如何对裸金属类型的ECS实例进行本地盘的换盘预处理操作。

须知

本地盘换盘操作会丢失故障本地盘上的数据，如果无需保留本地盘上的数据，可通过本操作换盘预处理。

本地盘换盘操作可能伴随宿主机的下电与重启，在预处理前，请确保云服务器中部署的业务离线，或云服务器停止对业务无影响。

如果需要保留本地盘上的数据或如果云服务器上的业务不可停止，请结束操作并联系技术支持进行处理。

操作步骤（Linux 实例）

获取故障本地盘标识符

1. 登录管理控制台。
2. 单击管理控制台左上角的，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”。
4. 在左侧导航树中，选择“事件”。
5. 在事件列表中，查看“本地盘换盘”事件的“事件描述”列。
通过“事件描述”信息获取故障本地盘的SN号，本文以“99K0A046FL3G”为例进行介绍。

获取故障本地盘挂载点

1. [远程登录](#)待换盘预处理的裸金属类型实例。
2. 执行以下命令，查看故障盘的SN号对应的盘符信息。

```
ll /dev/disk/by-id/ | grep SN号
```

以SN号“99K0A046FL3G”为例，命令如下：

```
ll /dev/disk/by-id/ | grep 99K0A046FL3G
```

回显信息如下：

```
/lrxxxrxxx 1 root root 9 Sep 18 19: 20 ata-MG06ACA10TE_99K0A046FL3G ->././sda  
lrwxrwxrwx 1 root root 10 Sep 18 19: 20 ata-MG06ACA10TE_99K0A046FL3G-part1->././sda1
```

3. 执行以下命令，查询故障盘的挂载点。

```
df -Th | grep 盘符信息
```

以盘符信息“/dev/sda1”为例，命令如下：

```
df -Th | grep /dev/sda1
```

回显信息如下：

```
/dev/sda1 ext4 9.1T 7.5T 1.6T 83% /srv/data
```

须知

本地盘的换盘预处理会导致本地盘数据丢失。如需保留本地盘数据，请结束操作并联系技术支持进行处理。

卸载故障的本地磁盘

1. 执行以下命令，卸载故障的本地磁盘。

umount 挂载点

以挂载点“/data”为例，命令如下：

umount /data

检查报障云服务器的/etc/fstab中是否配置了故障盘对应的自动挂载信息**说明**

如果报障云服务器的/etc/fstab中配置了故障盘对应的自动挂载信息，则需要删除或注释掉，防止本地盘换盘后启动云服务器进入Emergency Mode（紧急模式）。

1. 执行以下命令，查询磁盘分区的UUID。

blkid 磁盘分区

以查询磁盘分区“/dev/sda1”的UUID为例：

blkid /dev/sda1

回显信息如下：

```
/dev/sda1: UUID="e7100f3e-af65-49da-a013-c4ace8e5aba7" TYPE
="ext4" RTLABEL="logical" PARTUUID="cd358d32-e02b-4b23-bbd9-8a8bdae0e070"
```

2. 执行以下命令，查询/etc/fstab中是否存在磁盘分区的自动挂载信息。

cat /etc/fstab | grep 磁盘分区的UUID

以查询磁盘分区的UUID“e7100f3e-af65-49da-a013-c4ace8e5aba7”为例，命令如下：

cat /etc/fstab | grep e7100f3e-af65-49da-a013-c4ace8e5aba7

回显信息如下，表示/etc/fstab中存在磁盘分区的自动挂载信息：

```
UUID=e7100f3e-af65-49da-a01 3-c4ace8e5aba7 /srv/data ext4 defaults,noatime, nodiratime 1 0
```

3. 如果存在挂载信息，执行以下命令，删除磁盘分区的自动挂载信息，避免在更换本地盘后，云服务器开机时进入Emergency Mode（紧急模式）。

- a. 执行以下命令，编辑/etc/fstab文件。

vi /etc/fstab

- b. 单击“i”进入编辑模式。

- c. 删除或注释掉步骤2中查询的磁盘分区的自动挂载信息。

在自动挂载信息前面添加#，表示注释掉自动挂载信息，示例如下：

```
# UUID=e7100f3e-af65-49da-a01 3-c4ace8e5aba7 /srv/data ext4 defaults,noatime, nodiratime 1 0
```

- d. 单击Esc键并输入:wq后回车，保存并退出编辑模式。

云服务器关机

1. 在事件列表中，查看“本地盘换盘”事件对应的实例ID。
2. 在左侧导航选择“弹性云服务器”，在报障的云服务器“操作”列，单击“更多 > 关机”。

说明

本地盘的换盘预处理需要通过将云服务器关机再开机的过程，将本地盘信息同步至虚拟化层。

操作步骤（Windows 实例）

获取故障本地盘标识符

1. 登录管理控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”。
4. 在左侧导航树中，选择“事件”。
5. 在事件列表中，查看“本地盘换盘”事件的“事件描述”列。

通过“事件描述”信息获取故障本地盘的SN号，本文以“WS22LX16”为例进行介绍。

获取磁盘编号，确认影响范围

1. [远程登录](#)待换盘预处理的裸金属类型实例。
2. 以管理员身份打开“Windows PowerShell”，查询磁盘编号和SN号的对应关系，获取磁盘编号。

```
Get-Disk | select Number, SerialNumber
```

图 13-26 查询磁盘编号和 SN 号的对应关系

```
PS C:\Users\Administrator> Get-Disk | select Number, SerialNumber
Number SerialNumber
-----
1       WS22LX16
2       WS22LWC7
0 55a3514f-5288-444c-9
```

须知

本地盘换盘操作会导致本地盘数据丢失。如需保留本地盘数据，请结束操作并联系技术支持进行处理。

云服务器关机

1. 在事件列表中，查看“本地盘换盘”事件对应的实例ID。
2. 在左侧导航选择“弹性云服务器”，在报障的云服务器“操作”列，单击“更多 > 关机”。

说明

本地盘的换盘预处理需要通过将云服务器关机再开机的过程，将本地盘信息同步至虚拟化层。

13.5 实例重部署预处理

操作场景

对于包含本地盘的云服务器，当进行“本地盘换盘”和“实例重部署”事件的“授权重部署”操作时，需要先对本地盘进行实例重部署预处理，避免云服务器异常风险。

本文介绍如何对Linux操作系统的磁盘增强型（D系列）和超高I/O型（I系列）的ECS实例进行实例重部署的预处理操作。

须知

对于包含本地盘的实例，实例重部署操作会丢失所有本地盘上的数据，如果无需保留本地盘上的数据，可通过本操作实例重部署预处理。

如果需要保留本地盘上的数据，请勿授权，结束操作并联系技术支持进行处理。

操作步骤

实例重部署预处理，即在实例的/etc/fstab配置文件中为所有数据盘增加nofail参数。

1. [远程登录](#)待预处理的弹性云服务器。
2. 执行以下命令，打开并编辑/etc/fstab配置文件。
vim /etc/fstab
3. 单击“i”进入编辑模式，在/etc/fstab配置文件中为所有数据盘加入nofail参数。

示例如下：

```
UUID-8232fee7-f20a-416c-a2e0-cbc8c85a01a2 /mnt/nvme0n1 ext4 defaults,nofail 0 2
```

- UUID-8232fee7-f20a-416c-a2e0-cbc8c85a01a2：数据盘的UUID。
 - /mnt/nvme0n1：数据盘挂载点，可通过**mount | grep "盘符信息"**命令进行查询。
 - ext4：数据盘的文件系统类型，可通过**blkid 盘符信息**命令进行查询。
 - nofail：用于设置当文件系统中包含本地盘但实际缺失时，不中断云服务器的启动流程，避免云服务器异常风险。
4. 单击:wq退出编辑模式。
 5. 执行以下命令，使配置生效。
systemctl daemon-reload

14 操作系统 dump 管理

14.1 配置操作系统 dump

操作场景

云服务器的操作系统在运行过程中如果出现故障，可能导致系统崩溃，例如操作系统蓝屏或死机。在这种情况下，如果使用操作系统dump，系统会将内存中的数据以存储文件的形式进行保存，以便于进行云服务器的故障定位和问题分析。

本文介绍如何配置操作系统dump的方法。

- [配置操作系统dump（Windows）](#)
- [配置操作系统dump（Linux）](#)

背景知识

操作系统dump，即内核转储或崩溃转储，是当云服务器系统运行出现异常时，对操作系统内存数据的实时完整备份。

操作系统dump功能主要利用操作系统内核对硬件异常的处理能力。操作系统内核可以监测到硬件异常，并根据异常的类型来决定处理方式。当系统遇到无法处理的异常或错误时，系统的部分或全部运行状态信息将会转储到磁盘上，这些状态信息包括：CPU的寄存器、物理内存、进程状态、文件系统状态、硬件设备状态等。

操作系统dump可以由以下几种方式触发：

- 系统崩溃：当操作系统遇到无法处理的异常或错误时，例如非法的内存访问、内核panic等，系统会自动触发dump。
- 手动触发：系统管理员也可以通过一些命令或者操作手动触发系统dump，例如在Linux系统中可以通过向/proc/sysrq-trigger写入c字符来触发系统dump。
- 计划触发：某些情况下，系统管理员为了获取系统的某一时刻的运行状态信息，或者模拟系统崩溃的情况，也可以设置在某一特定的时间触发系统dump。

在多数情况下，为了准确获得系统dump，需要对系统进行相关的配置，例如在Linux系统中，需要配置kdump服务等。本文主要介绍手动触发dump的操作指导。

约束与限制

- 执行操作系统dump会重启云服务器，请提前做好业务备份，避免数据丢失。
- 鲲鹏架构的云服务器不支持操作系统dump。
- 支持运行中、关机和故障状态的云服务器进行操作系统dump。
- 仅支持对4vCPUs，8GiB内存以上规格的ECS使用操作系统dump功能。
- 预留内存需大于ECS规格的内存。

配置操作系统 dump（Windows）

本文以Windows Server 2016版本操作系统为例进行介绍，更多版本的操作，请参考对应操作系统官网帮助文档。

1. [远程登录云服务器](#)。
2. 在“控制面板中，打开“系统 > 高级系统配置”。

图 14-1 高级系统配置



3. 在“系统属性”的“性能”区域，单击“设置”。
4. 在“高级”页签的“虚拟内存”区域，单击“更改”。

图 14-2 性能选项设置



5. 在“虚拟内存”页面，勾选“自动管理所有驱动器的分页文件大小”。

图 14-3 虚拟内存设置



- 6. 单击“确定”，完成虚拟内存设置。
- 7. 在“系统属性”的“启动和故障恢复”区域，单击“设置”。
- 8. 设置参数。
 - 写入调试信息：设置为“完全内存转储”。
 - 转储文件：可以将路径从“%SystemRoot%\Memory.dmp”更改为指向具有足够磁盘空间的本地驱动器，例如“E: |Memory.dmp”。

图 14-4 启动和故障恢复设置

启动和故障恢复

系统启动

默认操作系统(S):
Windows Server 2016

☒ 显示操作系统列表的时间(T): 30 秒

☐ 在需要时显示恢复选项的时间(D): 30 秒

系统失败

☒ 将事件写入系统日志(W)

☒ 自动重新启动(R)

写入调试信息

完全内存转储

转储文件:
%SystemRoot%\MEMORY.DMP

☒ 覆盖任何现有文件(O)

☐ 禁止在磁盘空间不足时自动删除内存转储(A)

确定 取消

9. 单击“确定”。
10. 重启云服务器，完成配置。

配置操作系统 dump (Linux)

本文以CentOS 7.5版本操作系统为例进行介绍，更多版本的操作，请参考对应操作系统官网帮助文档。

1. [远程登录云服务器](#)。
2. 执行以下命令，安装kexec-tools。
yum install kexec-tools
3. 执行以下命令，查看crashkernel预留内存大小。
cat /etc/default/grub

```
GRUB_TIMEOUT=5
GRUB_DISTRIBUTOR="$(sed 's, release .*$,g' /etc/system-release)"
GRUB_DEFAULT=saved
GRUB_DISABLE_SUBMENU=true
GRUB_TERMINAL_OUTPUT="console"
GRUB_CMDLINE_LINUX="net.ifnames=0 consoleblank=600 console=tty0 console=ttyS0,115200n8
spectre_v2=off nopti crashkernel=auto "
GRUB_DISABLE_RECOVERY="true"
```

4. 执行以下命令，设置crashkernel的大小。

vim /etc/default/grub

当前crashkernel预留内存大小为“auto”，您可以在“GRUB_CMDLINE_LINUX”字段，修改“**crashkernel**”的值，设置crashkernel的大小。

```
GRUB_TIMEOUT=5
GRUB_DISTRIBUTOR="$(sed 's, release .*$,g' /etc/system-release)"
GRUB_DEFAULT=saved
GRUB_DISABLE_SUBMENU=true
GRUB_TERMINAL_OUTPUT="console"
GRUB_CMDLINE_LINUX="net.ifnames=0 consoleblank=600 console=tty0 console=ttyS0,115200n8
spectre_v2=off nopti crashkernel=256M"
GRUB_DISABLE_RECOVERY="true"
```

说明

您可以根据系统架构决定crashkernel预留内存大小，过小会导致生成coredump文件失败。

当前示例的系统内存是1GiB，预留内存设置为256M。

5. 执行以下命令，重新生成grub配置文件。

grub2-mkconfig -o /boot/grub2/grub.cfg

6. 执行以下命令，编辑内核参数文件/etc/sysctl.conf。

vim /etc/sysctl.conf

在/etc/sysctl.conf配置文件中增加以下参数，以便于在收到NMI时将操作系统切换到应急模式，并生成内存转储。

```
kernel.panic_on_unrecovered_nmi=1
kernel.unknown_nmi_panic=1
```

7. 重启系统。

reboot

8. 执行以下命令，修改kdump默认配置/etc/kdump.conf。

vim /etc/kdump.conf

```
#指定coredump文件存储位置
path /var/crash
#增加-c参数，代表压缩coredump文件
core_collector makedumpfile -c -l --message-level 1 -d 31
#生成coredump后，重启系统
default reboot
```

9. 执行以下命令，开启kdump服务并设置开机自启动。

systemctl start kdump.service

systemctl enable kdump.service

10. 执行以下命令，检查kdump是否开启成功。

service kdump status

```
Redirecting to /bin/systemctl status kdump.service
● kdump.service - Crash recovery kernel arming
   Loaded: loaded (/usr/lib/systemd/system/kdump.service; enabled; vendor preset: enabled)
   Active: active (exited) since Wed 2024-05-22 21:19:47 CST; 11min ago
```

```
Main PID: 591 (code=exited, status=0/SUCCESS)
CGroup: /system.slice/kdump.service
```

systemctl is-active kdump.service

active

触发操作系统 dump

1. 登录管理控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”。
4. 在弹性云服务器列表的“操作”列，单击“更多 > 故障排查 > 触发操作系统 dump”。
5. 了解风险须知后，勾选已知晓风险的提示。
6. 单击“确定”，完成触发操作系统dump。

14.2 查看操作系统 dump

操作场景

触发操作系统dump后，您可以在云服务器上查看对应的内存dump文件。

本文介绍如何触发和查看操作系统dump的内核转储文件的方法。

- [触发操作系统dump](#)
- [查看操作系统dump（Windows）](#)
- [查看操作系统dump（Linux）](#)

前提条件

已经完成[配置操作系统dump](#)。

触发操作系统 dump

1. 登录管理控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”。
4. 在弹性云服务器列表的“操作”列，单击“更多 > 故障排查 > 触发操作系统 dump”。
5. 了解风险须知后，勾选已知晓风险的提示。
6. 单击“确定”，完成触发操作系统dump。

查看操作系统 dump（Windows）

本文以Windows Server 2016版本操作系统为例进行介绍，更多版本的操作，请参考对应操作系统官网帮助文档。

1. [远程登录云服务器](#)。
2. 根据[配置操作系统dump（Windows）](#)中设置的转储文件路径，可以查看到操作系统dump的内核转储文件。
例如，在“C:\Windows”路径下，获取到文件“memory.dmp”。
您可以通过工具检查和分析内核转储文件，详细操作，请参见[分析内核模式转储文件](#)。

查看操作系统 dump（Linux）

本文以CentOS 7.5版本操作系统为例进行介绍，更多版本的操作，请参考对应操作系统官网帮助文档。

1. [远程登录云服务器](#)。
2. 执行以下命令，查看是否生成操作系统dump的内核转储文件。

```
ls /var/crash/
```

```
127.0.0.1-2024-05-22-21:35:26
```

您可以通过Linux平台的crash工具来分析操作系统内核的转储文件，详细操作，请参见[crash](#)。

15 自助运维管理

15.1 配置 ECS 自助运维自定义策略

操作场景

ECS自助运维功能依赖云运维中心（Cloud Operations Center，简称COC），需开通并授权COC服务。开通并授权后，系统自动创建名为ServiceLinkedAgencyForCOC和ServiceAgencyForCOC的委托，并授予必要的权限，用于通过COC代理操作对应的云服务器资源。详细内容，请参见[查看委托](#)。

当您想要使用IAM用户进行ECS自助运维操作时，需联系IAM用户所属华为账号为该IAM用户授予COC的资源操作类权限。

本文为您介绍为IAM用户授权的方法。

前提条件

本文默认IAM用户已具备ECS相关操作权限。

说明

若操作过程中出现ECS权限相关问题，请为IAM用户授权，详细操作，请参见[创建用户并授权使用ECS](#)。

操作步骤

1. 使用IAM用户所属华为账号登录[IAM权限管理](#)页面。
2. 在页面右上角，单击“创建自定义策略”，并增加COC自定义权限策略。
详细操作步骤，请参见[创建自定义策略](#)。

以添加开通COC以及操作COC的自定义策略为例，进行介绍

- a. （可选）创建名为“开通COC”的自定义策略，并增加如下权限。

说明

如果IAM用户所属华为账号已开通COC，则无需为IAM用户添加“开通COC”的权限。

```
{  
  "Version": "1.1",
```

```
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "iam:agencies:list*",
      "iam:agencies:createAgency",
      "iam:agencies:createServiceLinkedAgencyV5",
      "coc:agency:get",
      "coc:agency:create",
      "iam:permissions:grantRoleToAgency",
      "iam:permissions:grantRoleToAgencyOnDomain",
      "iam:roles:listRoles"
    ]
  }
]
```

- b. 创建名为“COC操作权限”的自定义策略，并增加如下权限。

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "coc:instance:listResources",
        "coc:application:listResources",
        "coc:schedule:list",
        "coc:schedule:enable",
        "coc:schedule:update",
        "coc:schedule:disable",
        "coc:schedule:approve",
        "coc:schedule:create",
        "coc:schedule:delete",
        "coc:schedule:count",
        "coc:schedule:get",
        "coc:schedule:getHistories",
        "coc:application:GetDiagnosisTaskDetails",
        "coc:application>CreateDiagnosisTask",
        "coc:document:create",
        "coc:document:listRunbookAtomics",
        "coc:document:getRunbookAtomicDetails",
        "coc:document:list",
        "coc:document:delete",
        "coc:document:update",
        "coc:document:get",
        "coc:document:analyzeRisk",
        "coc:instance:autoBatchInstances",
        "coc:instance:executeDocument",
        "coc:instance:start",
        "coc:instance:reboot",
        "coc:instance:stop",
        "coc:job:action",
        "coc:instance:reinstallOS",
        "coc:instance:changeOS",
        "coc:hostAccount:describe",
        "coc:instance:syncResources"
      ]
    }
  ]
}
```

3. 创建用户组并授予COC的资源操作类权限。

详细操作步骤，请参见[创建用户组并授权](#)。

需要为用户组授予如下权限：

- COC ReadOnlyAccess
- 步骤2中创建的“开通COC”以及“COC操作权限”自定义策略。

图 15-1 为用户组授权



4. 在IAM控制台的“用户”页面，单击待授权的IAM用户“操作”列的“授权”，为IAM用户授予COC权限。
详细操作步骤，请参见[给IAM用户授权](#)。
在“授权”页面，将待授权的IAM用户加入到步骤3创建的用户组，完成IAM用户的授权。

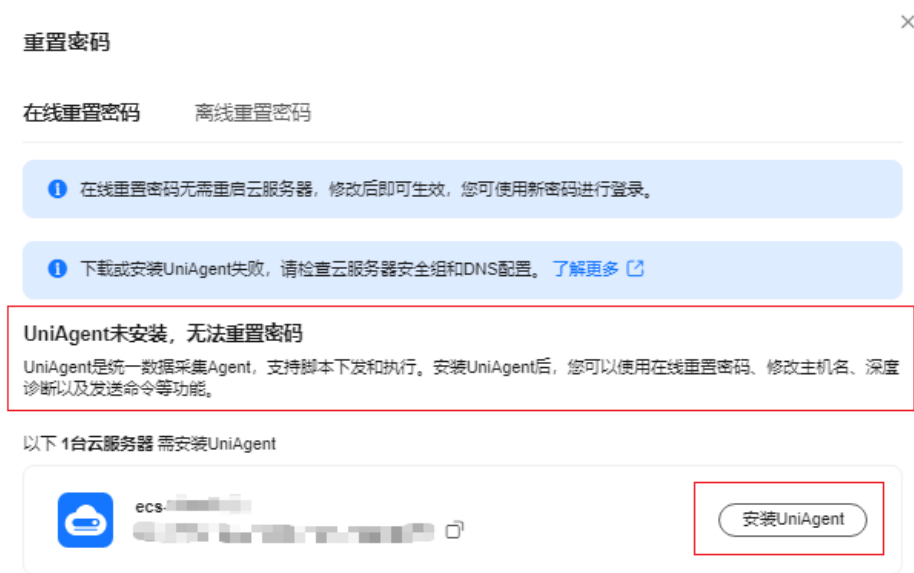
15.2 为 ECS 安装 UniAgent

操作场景

ECS的修改主机名、在线重置密码等自助运维操作依赖应用运维管理（Application Operations Management，简称AOM）的统一数据采集Agent（简称UniAgent）功能。

在进行上述操作时，如果提示未安装UniAgent或者安装失败，需登录ECS安装UniAgent后才可进行后续操作。

图 15-2 提示信息（图示以单台 ECS 在线重置密码时的提示信息为例）



本文为您介绍安装UniAgent的方法。

- **安装UniAgent（ECS控制台）**：单台ECS进行自助运维相关操作时，触发未安装UniAgent提示信息，在ECS控制台进行UniAgent的安装。
- **安装UniAgent（采集管理控制台）**：多台ECS批量进行自助运维操作时，触发未安装UniAgent提示信息，跳转至采集管理控制台进行UniAgent的安装。

前提条件

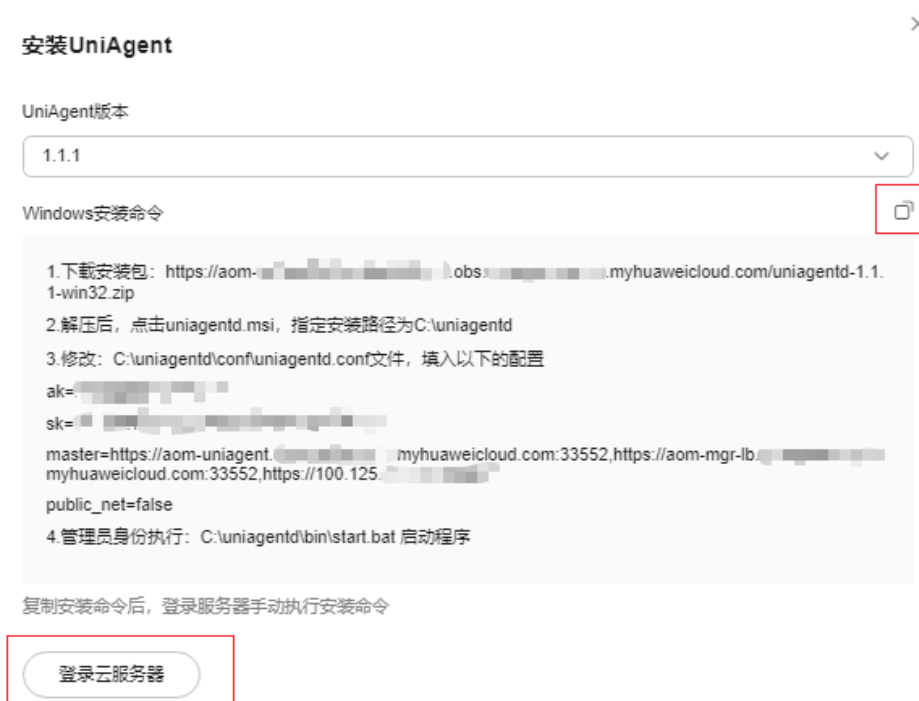
已**开通AOM 2.0**。

安装 UniAgent（ECS 控制台）

当单台ECS进行自助运维相关操作时，若提示未安装UniAgent或者安装失败，可参考本步骤安装UniAgent。

1. 在自助运维操作页面，单击提示信息中的“安装UniAgent”，进入“安装UniAgent”页面。

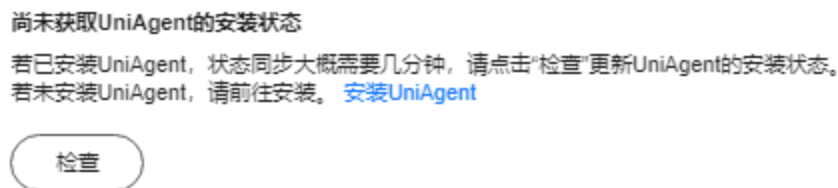
图 15-3 安装 UniAgent（图示以 Windows 操作系统 ECS 为例）



2. 选择“UniAgent版本”，建议选择最新版本。
3. 单击安装命令区域右上角的复制按钮，复制安装命令。
4. 单击“登录云服务器”，登录ECS。
5. 在ECS上执行UniAgent的安装命令。
 - 对于Windows系统ECS：参考安装指导下载安装包并完成UniAgent的安装。
 - 对于Linux系统ECS：粘贴并执行步骤3中复制的安装命令，完成UniAgent的安装。
6. 返回操作页面，单击“检查”查看UniAgent的安装状态。

UniAgent的安装及状态同步大约需要几分钟，您可以单击“检查”查看并更新UniAgent的安装状态。安装完成即可进行后续操作。

图 15-4 检查 UniAgent 安装状态



安装 UniAgent（采集管理控制台）

当多台ECS批量进行自助运维相关操作时，若提示未安装UniAgent或者安装失败，可参考本步骤安装UniAgent。

1. 在自助运维操作页面，单击提示信息中的“安装UniAgent”，进入采集管理控制台的[安装UniAgent](#)页面。

图 15-5 安装 UniAgent（采集管理控制台）



2. 根据页面提示进行参数设置，完成UniAgent的安装。
详细内容，请参见[安装UniAgent](#)。
3. 返回自助运维对应操作页面，单击“检查UniAgent安装状态”，查看并更新UniAgent的安装状态。

UniAgent的安装及状态同步大约需要几分钟，您可以单击“检查UniAgent安装状态”查看并更新UniAgent的安装状态。安装完成即可进行后续操作。

15.3 为 ECS 配置定时运维任务

操作场景

ECS支持定时运维，您可以通过配置定时运维任务，对ECS进行定时开机、定时关机等操作。该功能适用于需要在特定时间对多台ECS进行开机、关机等运维操作的场景。

例如，若您的业务有比较规律的波峰和波谷，可以选择在业务波峰时开机、波谷时关机，以便于降低使用成本。如果采用手动方式对多台ECS进行开机、关机操作，耗时长且容易出错，此时，可以通过设置定时运维任务，自动化的进行多台ECS的定时运维操作，节省人力和时间成本。

本文介绍如何设置ECS的定时运维任务。

约束与限制

- ECS的定时运维依赖云运维中心（ Cloud Operations Center，简称COC ），需开通并授权COC服务。
对于IAM用户，需额外配置COC资源操作类权限，详细内容，请参见[配置ECS自助运维自定义策略](#)。
- 单个租户最多支持创建200个定时任务。
- 定时运维任务仅支持应用于同一区域的目标ECS实例。

操作步骤

您可以为单台或多台ECS创建定时开机、定时关机等运维任务。

为单台 ECS 创建定时任务

- 登录管理控制台，进入[弹性云服务器](#)列表页面。
- 在待创建定时任务ECS的“操作”列，单击“更多 > 定时任务 > 定时开机”或“更多 > 定时任务 > 定时关机”。
- （可选）在“开通云运维中心并添加权限”页面，阅读服务声明并勾选后，单击“开通并授权”。
若当前账号未开通并授权COC服务，则会显示该页面。
- 在“创建定时任务”页面，根据界面提示信息，完成相关参数配置。

表 15-1 定时任务参数配置

参数	说明
任务名称	定时任务的名称。 由中文、字母、数字、中划线、下划线组成，长度在3~100之间。
企业项目	定时任务所属的企业项目，用于提供项目内的资源管理、成员管理。 默认项目为default。
时区	执行定时任务的时间所属时区。
定时类型	定时任务的执行类型，包括： - 单次执行：在指定时间执行一次定时任务。 - 周期执行：在指定的周期和时间循环执行定时任务。

参数	说明
执行时间	定时任务的执行时间。 - 当“定时类型”选择“单次执行”时，设置定时任务的开始执行时间。 - 当“定时类型”选择“周期执行”时，设置定时任务的执行周期和执行时间。 - 简单周期：设置每周自动执行定时任务的具体日期和时间。 - Cron表达式：通过设置秒、分、时、日、月、周的Cron表达式，设置定时任务的执行周期和时间。 详细内容，请参见Cron表达式使用。
规则结束时间	周期执行的定时任务的结束时间。 仅当“定时类型”选择“周期执行”时，会显示该参数。
任务类型	定时任务的类型，包括： - 当步骤2选择“定时开机”时，此参数默认为“ECS开机”，用于设置ECS定时开机任务。 - 当步骤2选择“定时关机”时，此参数默认为“ECS关机”，用于设置ECS定时关机任务。
IAM权限委托	执行定时任务所需的IAM委托权限，以便于通过COC代理操作对应的ECS资源。
目标实例	待执行定时任务的目标实例。默认已选择一台目标实例。
分批策略	目标实例执行定时任务时的分批策略，包括： - 自动分批：系统自动设置目标实例的分批批次，按不同批次执行定时任务。 - 手动分批：手动设置目标实例的分批批次，按不同批次执行定时任务。 - 不分批：目标实例不分批，同时执行定时任务。 每批次中目标实例数的上限为100。

5. 单击“提交”，完成定时任务的创建。

为多台 ECS 创建定时任务

1. 登录管理控制台，进入[弹性云服务器](#)页面。
2. 在ECS列表中，勾选待创建定时任务的多台ECS。
3. 在列表上方，单击“更多 > 定时任务 > 定时开机”或“更多 > 定时任务 > 定时关机”。
4. （可选）在“开通云运维中心并添加权限”页面，阅读服务声明并勾选后，单击“开通并授权”。

若当前账号未开通并授权COC服务，则会显示该页面。

5. 在“创建定时任务”页面，根据界面提示信息，完成相关参数配置。

表 15-2 定时任务参数配置

参数	说明
任务名称	定时任务的名称。 由中文、字母、数字、中划线、下划线组成，长度在3~100之间。
企业项目	定时任务所属的企业项目，用于提供项目内的资源管理、成员管理。 默认项目为default。
时区	执行定时任务的时间所属时区。
定时类型	定时任务的执行类型，包括： ● 单次执行：在指定时间执行一次定时任务。 ● 周期执行：在指定的周期和时间循环执行定时任务。
执行时间	定时任务的执行时间。 ● 当“定时类型”选择“单次执行”时，设置定时任务的开始执行时间。 ● 当“定时类型”选择“周期执行”时，设置定时任务的执行周期和执行时间。 – 简单周期：设置每周自动执行定时任务的具体日期和时间。 – Cron表达式：通过设置秒、分、时、日、月、周的Cron表达式，设置定时任务的执行周期和时间。 详细内容，请参见Cron表达式使用。

参数	说明
规则结束时间	周期执行的定时任务的结束时间。 仅当“定时类型”选择“周期执行”时，会显示该参数。
任务类型	定时任务的类型，包括： - 当步骤3选择“定时开机”时，此参数默认为“ECS开机”，用于设置ECS定时开机任务。 - 当步骤3选择“定时关机”时，此参数默认为“ECS关机”，用于设置ECS定时关机任务。
IAM权限委托	执行定时任务所需的IAM委托权限，以便于通过COC代理操作对应的ECS资源。
目标实例	待执行定时任务的目标实例。默认已选择步骤2的目标实例。
分批策略	目标实例执行定时任务时的分批策略，包括： - 自动分批：系统自动设置目标实例的分批批次，按不同批次执行定时任务。 - 手动分批：手动设置目标实例的分批批次，按不同批次执行定时任务。 - 不分批：目标实例不分批，同时执行定时任务。 每批次中目标实例数的上限为100。

6. 单击“提交”，完成定时任务的创建。

后续操作

定时任务创建成功后，您可以通过[定时运维](#)页面启用、禁用、编辑、删除定时任务，还可以设置定时任务的审批配置和消息通知。

详细内容，请参见[定时任务管理](#)。

15.4 免登录 ECS 发送远程命令

操作场景

ECS支持免登录发送命令功能。通过该功能您可以在不登录ECS的情况下，发送脚本命令至单台或多台ECS，快速完成对ECS的日常维护。

例如，如果您想批量在ECS上安装或卸载软件、重置密码或执行自动化运维脚本，即可通过免登录发送命令功能进行操作。

本文介绍如何通过管理控制台向单台或多台ECS发送命令。

约束与限制

- 该功能依赖云运维中心（Cloud Operations Center，简称COC），需开通并授权COC服务。
对于IAM用户，需额外配置COC资源操作类权限，详细内容，请参见[配置ECS自助运维自定义策略](#)。
- 该功能依赖UniAgent。UniAgent是统一数据采集Agent，支持脚本下发和执行。若ECS未安装UniAgent，则无法免登录发送命令，详细内容，请参见[ECS安装UniAgent](#)。
- 该功能仅支持“运行中”状态的ECS。

操作步骤

您可以向单台或多台ECS发送脚本命令。

向单台 ECS 发送命令

- 登录管理控制台，进入[弹性云服务器](#)列表页面。
- 在待发送命令的ECS的“操作”列，单击“更多 > 发送命令”。
- （可选）在“开通云运维中心并添加权限”页面，阅读服务声明并勾选后，单击“开通并授权”。
若当前账号未开通并授权COC服务，则会显示该页面。
- 在“发送命令”页面，根据界面提示信息，完成相关参数配置。

须知

发送命令功能依赖UniAgent，如果提示未安装UniAgent或者安装失败，请参考[ECS安装UniAgent](#)进行安装，否则无法发送命令。

图 15-6 发送命令

发送命令

目标实例

已选实例: 1

操作系统

Linux

Windows

执行用户

root

执行计划

立即执行

超时时间

60秒

命令类型

Shell

Python

命令输入

一键输入上次的命令

1 #!/bin/bash

表 15-3 发送命令参数配置

参数	说明
目标实例	选择待发送命令的目标实例。默认已选择一台目标实例。
操作系统	目标实例的操作系统类型，当前支持Linux和Windows。 请根据目标实例的操作系统类型进行选择。
执行用户	命令的执行用户。 - Windows系统ECS：默认为system，不支持修改。 - Linux系统ECS：默认为root，支持手动输入其他用户作为执行用户。
执行计划	命令的执行计划，默认为“立即执行”。
超时时间	单次命令执行的超时时间，超时后会强制终止发送进程。 范围：6～1800秒（24小时）。 单位：秒。

参数	说明
命令类型	支持发送的脚本命令类型。 - Windows系统ECS：支持Bat。 - Linux系统ECS：支持Shell（默认）、Python。
命令输入	待发送命令的输入框。 输入内容必须为单次执行可返回结果的命令，即不支持与命令返回信息进行二次交互。 说明 一条命令执行完成后，可在命令输入框中继续输入命令，再次进行执行。
命令输出	命令的输出框，可查看命令执行结果。

向多台 ECS 发送命令

1. 登录管理控制台，进入[弹性云服务器](#)列表页面。
 2. 在ECS列表中，勾选待发送命令的多台ECS。
 3. 在列表上方，单击“更多 > 发送命令”。
 4. （可选）在“开通云运维中心并添加权限”页面，阅读服务声明并勾选后，单击“开通并授权”。
- 若当前账号未开通并授权COC服务，则会显示该页面。
5. 在“批量发送命令”页面，根据界面提示信息，完成相关参数配置。

须知

发送命令功能依赖UniAgent，如果提示未安装UniAgent或者安装失败，请参考[为ECS安装UniAgent](#)进行安装，否则无法发送命令。

批量操作时，如果勾选的多个ECS不属于同一操作系统，既包含Linux系统ECS，又包含Windows系统ECS，则需要分别进行配置。

图 15-7 批量发送命令

批量发送命令

目标实例

已选实例: 2

操作系统

Linux

Windows

执行用户

root

执行计划

立即执行

超时时间

60

秒

命令类型

Shell

Python

命令输入

1

#!/bin/bash

一键输入上次的命令

命令输出

fac67167

82d00911

全部实例 2

1

表 15-4 批量发送命令参数配置

参数	说明
目标实例	选择待发送命令的目标实例。默认已选择步骤2中勾选的目标实例。
操作系统	目标实例的操作系统类型，当前支持Linux和Windows。 请根据目标实例的操作系统类型进行选择。若批量操作选择的目标实例包含Linux和Windows两种操作系统类型，则需要分别进行设置。
执行用户	命令的执行用户。 - Windows系统ECS：默认为system，不支持修改。 - Linux系统ECS：默认为root，支持手动输入其他用户作为执行用户。

参数	说明
执行计划	命令的执行计划，默认为“立即执行”。
超时时间	单次命令执行的超时时间，超时后会强制终止发送进程。 范围：6～1800秒（24小时）。 单位：秒。
命令类型	支持发送的脚本命令类型。 - Windows系统ECS：支持Bat。 - Linux系统ECS：支持Shell（默认）、Python。
命令输入	待发送命令的输入框。 输入内容必须为单次执行可返回结果的命令，即不支持与命令返回信息进行二次交互。 说明 一条命令执行完成后，可在命令输入框中继续输入命令，再次进行执行。
命令输出	命令的输出框，可查看命令执行结果。 批量向多台ECS发送命令时，可在命令输出框切换不同页签查看执行结果。

15.5 深度诊断 ECS

操作场景

ECS支持操作系统的深度诊断服务，提供GuestOS内常见问题的自诊断能力，您可以通过方便快捷的自诊断服务解决操作系统内的常见问题。

本文介绍支持深度诊断的操作系统版本以及诊断结论说明。

约束与限制

- 该功能依赖云运维中心（Cloud Operations Center，简称COC），需开通并授权COC服务。
对于IAM用户，需额外配置COC资源操作类权限，详细内容，请参见[配置ECS自助运维自定义策略](#)。
- 该功能依赖UniAgent。UniAgent是统一数据采集Agent，支持脚本下发和执行。若ECS未安装UniAgent，则无法免登录发送命令，详细内容，请参见[为ECS安装UniAgent](#)。
- 仅Linux操作系统的ECS支持深度诊断。
- 支持深度诊断的操作系统类型及版本。

操作系统类型	版本	CPU架构
Huawei Cloud EulerOS	Huawei Cloud EulerOS 2.0 Huawei Cloud EulerOS 1.1	x86/鲲鹏
CentOS	CentOS 8.2 64bit CentOS 8.0 64bit CentOS 7.9 64bit CentOS 7.8 64bit CentOS 7.7 64bit CentOS 7.6 64bit CentOS 7.5 64bit CentOS 7.4 64bit CentOS 7.3 64bit CentOS 7.2 64bit	x86
Ubuntu	Ubuntu 22.04 server 64bit Ubuntu 20.04 server 64bit	x86
Debian	Debian 11.1.0 64bit Debian 10.0.0 64bit	x86

操作步骤

1.

登录管理控制台，进入[弹性云服务器](#)列表页面。
2.

在待深度诊断的ECS的“操作”列，单击“更多 > 运维与监控 > 深度诊断”。
3.

（可选）在“开通云运维中心并添加权限”页面，阅读服务声明并勾选后，单击“开通并授权”。

若当前账号未开通并授权COC服务，则会显示该页面。
4.

在“深度诊断”页面，选择“深度诊断场景”为“全面诊断”。

须知

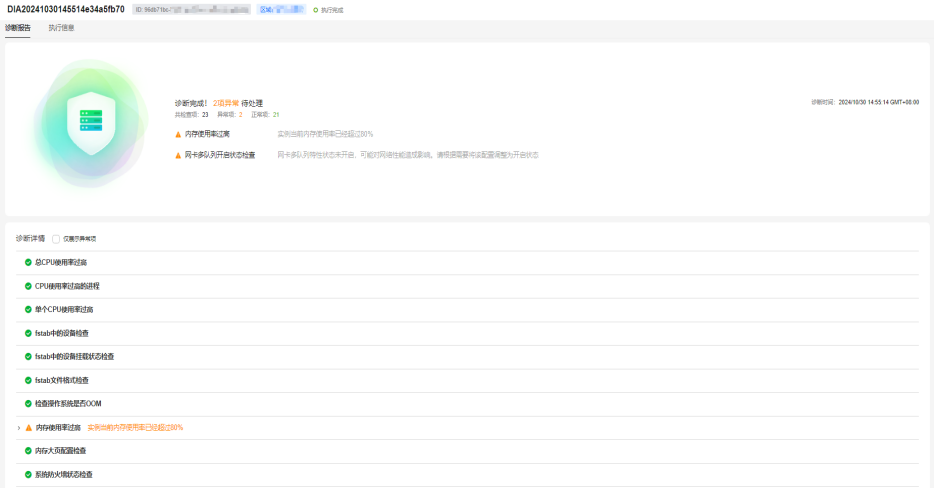
深度诊断功能依赖UniAgent，如果提示未安装UniAgent或者安装失败，请参考[为ECS安装UniAgent](#)进行安装，否则无法发送命令。

图 15-8 深度诊断



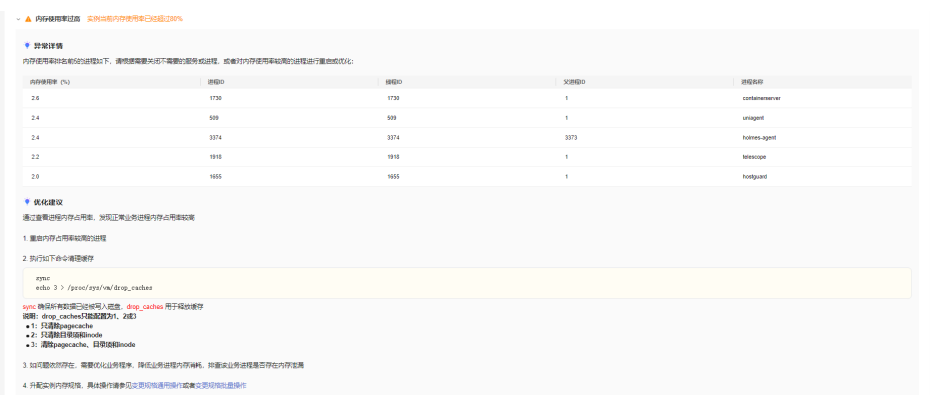
- 5. 勾选“同意安装插件并采集数据”后，单击“确定”。
诊断结果及说明，请参见[深度诊断结论](#)。
- 6. 在诊断结果的“诊断报告”页签查看诊断详情。

图 15-9 诊断报告



- 7. 在“诊断详情”区域，单击异常项左侧的“>”查看异常详情，并根据“优化建议”进行处理。

图 15-10 诊断异常项（示例）



深度诊断结论

诊断项ID	诊断项名称	诊断结论
guestos.cpu.high_total_usage	总CPU占用率过高	实例整体CPU占用率已超过80%。
guestos.cpu.high_process_usage	CPU使用率过高的进程	单进程CPU占用率超过整机的50%。
guestos.cpu.high_core_usage	单核CPU占用率过高	单核CPU占用率超过85%。
guestos.disk.high_inode_usage	磁盘使用率检查	该实例当前部分云盘对应文件系统的使用率或inode使用率已经超过了80%，可能导致在这些分区上无法创建新的文件
guestos.filesystem.invalid_device	fstab中的设备检查	当前实例的/etc/fstab文件中配置的某个设备不存在，可能会导致实例无法启动。
guestos.filesystem.device_mount_failure	fstab中的设备挂载状态检查	该实例存在未在/etc/fstab中配置自动挂载的云盘，可能会导致实例无法启动。
guestos.filesystem.invalid_format	fstab文件格式检查	fstab文件存在配置格式错误，可能会导致实例无法启动。
guestos.network.firewall_status_check	系统防火墙状态检查	当前实例的防火墙（即iptables设置）目前处于开启状态，如果服务器开启了防火墙，并设置了屏蔽外界访问的规则，可能会导致远程访问实例失败。
guestos.memory.oom_events	检查操作系统是否OOM	当前实例Guest OS内部曾经发生了OOM（out-of-memory）问题。
guestos.ssh.incorrect_file_permission	SSH公钥或私钥访问权限检查	当前实例SSH依赖的公钥或私钥文件权限不正确，会导致实例无法通过SSH访问。

诊断项ID	诊断项名称	诊断结论
gustos.ssh.missing_critical_file	SSH关键文件检查	当前实例SSH服务对应的关键文件或目录缺失，会导致实例无法通过SSH访问。
gustos.memory.high_total_usage	内存使用率过高	实例当前内存使用率已经超过80%。
gustos.ssh.forbidden_root_login	SSH是否允许root用户登录	当前实例SSH服务禁止root账号登录，会导致实例无法通过root用户SSH访问。
gustos.system.port_listenning	常见业务端口监听状态检查	端口22不存在进程监听，请您登录实例，检查端口业务服务是否存在异常，并根据需要进行修复。
gustos.system.unreasonable_file_limits	limits设置检查	当前实例系统文件/etc/security/limits.conf 中部分配置大于系统默认值，可能导致实例无法远程登录。
gustos.memory.unreasonable_hugepage_config	内存大页配置检查	当前实例内核参数vm.nr_hugepages配置的大页内存数量过大，可能导致实例无法远程登录。
gustos.network.wrong_nat_config	NAT环境内核参数检查	当前实例NAT相关的内核参数配置存在异常，导致用户无法通过ssh连接实例，还会导致当前实例上的HTTP服务访问出现异常。
gustos.network.wrong_tcp_sack	TCP SACK配置检查	当前实例未开启tcp_sack，可能会影响Linux实例的网络性能。
gustos.system.wrong_selinux_status	selinux状态检查	该实例开启了SELinux服务，会导致SSH远程连接实例时报错，请您视情况选择临时或永久关闭SELinux服务。
gustos.system.missing_critical_user	系统关键用户状态和密码设置检查	当前实例的系统账号不存在，可能会导致实例无法登录。
gustos.network.disabled_multi_queue	网卡多队列开启状态检查	网卡多队列特性状态未开启，可能对网络性能造成影响。请根据需要将该配置调整为开启状态。
gustos.filesystem.critical_file_exists	系统文件状态检查	该实例系统目录中的部分关键系统文件缺失，可能导致实例无法登录。
gustos.system.critical_service_exists	系统关键进程启动状态检查	该实例系统关键进程(比如SSH进程)处于未运行状态，可能会导致实例无法访问。
gustos.filesystem.critical_file_format_invalid	系统关键文件格式检查	当前实例系统账号对应文件的文件格式错误（不是unix格式），可能会导致实例无法登录。

16 资源与标签

16.1 标签管理

16.1.1 标签概述

操作场景

标签是弹性云服务器的标识。为弹性云服务器添加标签，可以方便用户识别和管理拥有的弹性云服务器资源。

您可以在创建弹性云服务器时添加标签，也可以在弹性云服务器创建完成后，在云服务器的详情页添加标签，您最多可以给弹性云服务器添加10个标签。

说明

创建弹性云服务器时添加的标签，将同步添加至一同创建的EIP和云硬盘（包括系统盘、数据盘）上。如果云服务器使用的是已有EIP，则该标签不会在EIP上标识。

如果您的组织已经设定弹性云服务器的相关标签策略，则需按照标签策略规则为弹性云服务器添加标签。如果添加的标签不符合标签策略规则，则可能会导致弹性云服务器创建失败，请联系组织管理员了解标签策略详情。

云服务器创建成功后，您可以在弹性云服务器、EIP和云硬盘详情页，查看到对应的标签。

有关标签的基本知识

标签用于标识资源，当您拥有相同类型的许多云资源时，可以使用标签按各种维度（例如用途、所有者或环境）对云资源进行分类。

图 16-1 标签示例

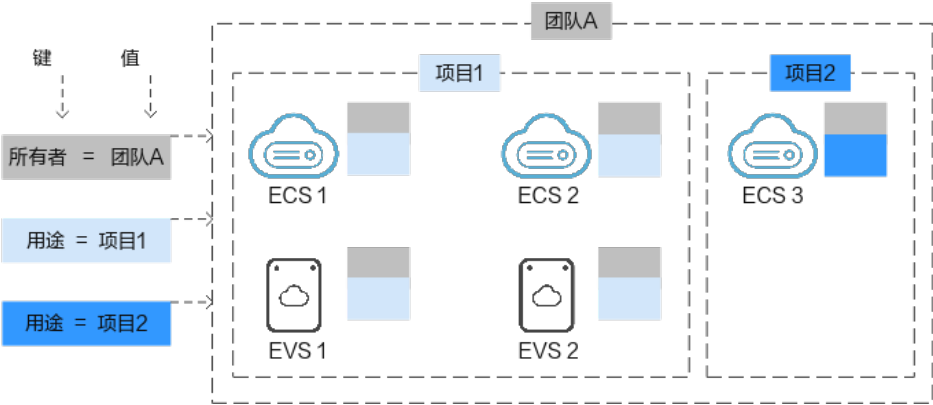


图16-1说明了标签的工作方式。在此示例中，您为每个云资源分配了两个标签，每个标签都包含您定义的一个“键”和一个“值”，一个标签使用键为“所有者”，另一个使用键为“用途”，每个标签都拥有相关的值。

您可以根据为云资源添加的标签快速搜索和筛选特定的云资源。例如，您可以为账户中的资源定义一组标签，以跟踪每个云资源的所有者和用途，使资源管理变得更加轻松。

标签命名规则

- 每个标签由一对键值对（Key-Value）组成。
- 每个弹性云服务器最多可以添加10个标签。
- 对于每个资源，每个标签键（Key）都必须是唯一的，每个标签键（Key）只能有一个值（Value）。
- 标签共由两部分组成：“标签键”和“标签值”，其中，“标签键”和“标签值”的命名规则如表16-1所示。

表 16-1 标签命名规则

参数	规则	样例
标签键	• 不能为空。 • 对于同一台云服务器，Key值唯一。 • 长度不超过36个字符。 • 不能包含“=”、“*”、“<”、“>”、“\”、“,”、“ ”、“/”。 • 首尾字符不能为空格。	Organization
标签值	• 长度不超过43个字符。 • 不能包含“=”、“*”、“<”、“>”、“\”、“,”、“ ”。 • 首尾字符不能为空格。	Apache

16.1.2 添加标签

标签用于标记云资源，如实例、镜像和磁盘等。如果您的账户下有多种云资源，并且不同云资源之间有多种关联，您可以为云资源添加标签，实现云资源的分类和统一管理。更多信息，请参见[标签概述](#)。

有三种途径为弹性云服务器添加标签：

- [在创建弹性云服务器时添加标签](#)
- [在弹性云服务器详情页添加标签](#)
- [在标签管理页面添加标签](#)

预定义标签的使方法请参考[预定义标签的使用方法](#)。

约束与限制

如您的组织已经设定云资源的相关标签策略，则需按照标签策略规则为云资源添加标签。如果添加的标签不符合标签策略规则，则可能会导致云资源创建失败，请联系组织管理员了解标签策略详情。

在创建弹性云服务器时添加标签

1. 登录管理控制台。
2. 单击管理控制台左上角的，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”，进入弹性云服务器页面。
4. 单击“购买弹性云服务器”。
5. 配置弹性云服务器的规格参数。
在“高级配置 > 标签”中，添加标签键和标签值。标签命名规则如[表16-1](#)所示。

说明

其他参数说明请参考[自定义购买ECS](#)。

图 16-2 添加标签



在弹性云服务器详情页添加标签

1. 登录管理控制台。
2. 单击管理控制台左上角的，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”，进入弹性云服务器页面。
4. 在弹性云服务器列表中，单击待管理标签的弹性云服务器名称。
系统跳转至该弹性云服务器详情页面。

5. 选择“标签”页签，单击“添加标签”，在弹出的“添加标签”窗口，输入标签的键和值。标签命名规则如表16-1所示。

图 16-3 在云服务器详情页添加标签



6. 单击“确定”，完成标签的添加。
 标签添加成功后，您可以单击标签“操作”列的“编辑”修改标签值。

在标签管理页面添加标签

说明

此方法适用于为多个资源统一添加拥有同样标签键的标签。

1. 登录管理控制台。
2. 在右上角的用户名下选择“标签管理”，进入标签管理服务页面。

图 16-4 标签管理



3. 在“资源标签”页面，勾选资源所在的区域，“资源类型”请选择“ECS-ECS”，单击“搜索”。
 系统列出所选区域下的所有云服务器资源。
4. 在“搜索结果”区域，单击“创建标签键”，输入键（例如：项目），单击“确定”。
 创建完成后，该标签键会添加至资源标签列表。如果列表中没有显示该标签，单击，在下拉列表中勾选创建的标签键。

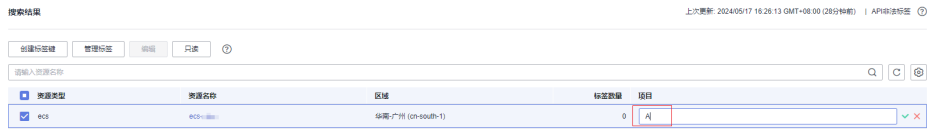
默认该标签键的值为“无标签”，您还需要为每一个资源对应的标签值赋值，完成标签与资源的关联，继续下一步。

图 16-5 资源列表



5. 单击“编辑”，切换资源标签列表为可编辑状态。
6. 在云服务器资源所在行，单击，输入标签“值”（例如：A）。
为标签键赋值后，“标签数量”将加1。按照同样方法依次为其他云服务器添加标签值。

图 16-6 输入标签值



预定义标签的使用方法

如果有多台云服务器或其他云资源需要添加同一标签，为了避免重复输入标签键和值，您可以在标签管理服务中预定义标签，然后在添加标签时直接选择键和值。具体步骤如下：

1. 登录管理控制台。
2. 在右上角的用户名下选择“标签管理”，进入标签管理服务页面。
3. 在左侧导航中选择“预定义标签”，单击“创建标签”，输入标签键和值（例如，项目-A）。
4. 选择“服务列表 > 计算 > 弹性云服务器”，按照上述添加标签的方法，在标签键和标签值输入框中下拉选择预定义的标签。

16.1.3 使用标签检索资源

为云资源添加标签后，您可以通过本文所述的两种方法使用标签检索资源。

使用标签搜索云服务器

在弹性云服务器列表页，按标签键或键值对搜索目标云服务器。

1. 登录管理控制台。
2. 单击管理控制台左上角的，选择区域和项目。
3. 单击“”，选择“计算 > 弹性云服务器”。
4. 在云服务器列表页搜索的输入框中选择“资源标签”，选择标签键值对后自动搜索。

支持多个标签搜索，按“与”的关系搜索目标云服务器。

图 16-7 按标签搜索云服务器



图 16-8 按标签搜索云服务器



通过标签管理筛选资源

- 1. 登录管理控制台。
 - 2. 在右上角的用户名下选择“标签管理”，进入标签管理服务页面。
 - 3. 在“资源标签”页面，设置搜索条件（包括区域、资源类型、资源标签）。
 - 4. 单击“搜索”。
- 搜索结果区域将列出所有符合搜索条件的资源。

16.1.4 删除标签

如果某个标签已经不再适用于您的资源管理，您可以删除资源标签。有三种途径删除资源标签：

- [在弹性云服务器详情页删除](#)
- [在标签管理页面单个删除](#)
- [在标签管理页面批量删除](#)

在弹性云服务器详情页删除

- 1. 登录管理控制台。
- 2. 单击管理控制台左上角的 ，选择区域和项目。
- 3. 单击“≡”，选择“计算 > 弹性云服务器”，进入弹性云服务器页面。
- 4. 在弹性云服务器列表中，单击待删除标签的弹性云服务器名称。
系统跳转至该弹性云服务器详情页面。
- 5. 选择“标签”页签，单击标签所在行“操作”列下的“删除”。
- 6. 单击“确定”，完成标签的删除。

在标签管理页面单个删除

- 1. 登录管理控制台。

2. 在右上角的用户名下选择“标签管理”，进入标签管理服务页面。

图 16-9 标签管理



3. 在“资源标签”页面，设置弹性云服务器资源搜索条件，单击“搜索”。
4. 页面下方展示的搜索结果包含“编辑”与“只读”两种状态，单击“编辑”，切换资源标签列表为可编辑状态。

若需要删除的标签的“键”没有展示在列表中，单击，在下拉列表中勾选需要删除的标签的“键”。勾选需要展示的标签键建议不超过10个。

5. 单击待删除标签的弹性云服务器资源所在行的，资源标签删除完成。
6. （可选）单击搜索结果区域右侧的按钮。
资源标签列表刷新为最新状态，并更新列表刷新时间。

在标签管理页面批量删除

须知

在批量删除标签时，请谨慎操作。执行删除操作后，其所标识的所有弹性云服务器资源对应的该标签均会被删除，且不可恢复。

1. 登录管理控制台。
2. 在右上角的用户名下选择“标签管理”，进入标签管理服务页面。
3. 在“资源标签”页面，设置弹性云服务器资源搜索条件，单击“搜索”。
4. 勾选待删除标签的弹性云服务器资源。
5. 单击列表上方的“管理标签”，进入管理标签页面。
6. 单击待删除标签所在行的“删除”。单击“确认”，资源标签删除完成。

7. （可选）单击搜索结果区域右侧的  按钮。
资源标签列表刷新为最新状态，并更新列表刷新时间。

16.2 配额调整

什么是配额？

为防止资源滥用，平台限定了各服务资源的配额，对用户的资源数量和容量做了限制。如您最多可以创建多少台弹性云服务器、多少块云硬盘。

如果当前资源配额限制无法满足使用需要，您可以申请扩大配额。

怎样查看我的配额？

1. 登录管理控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。
3. 在页面右上角，选择“资源 > 我的配额”。
系统进入“服务配额”页面。

图 16-10 我的配额



4. 您可以在“服务配额”页面，查看各项资源的总配额及使用情况。
如果当前配额不能满足业务要求，请参考后续操作，申请扩大配额。

如何申请扩大配额？

1. 登录管理控制台。
2. 在页面右上角，选择“资源 > 我的配额”。
系统进入“服务配额”页面。

图 16-11 我的配额



3. 在页面右上角，单击“申请扩大配额”。

图 16-12 申请扩大配额



4. 在“新建工单”页面，根据您的需求，填写相关参数。
其中，“问题描述”项请填写需要调整的内容和申请原因。
5. 填写完毕后，勾选协议并单击“提交”。

17 使用 CES 监控 ECS

17.1 监控弹性云服务器

监控是保持弹性云服务器可靠性、可用性和性能的重要部分，通过监控，用户可以观察弹性云服务器资源。为用户更好地掌握自己的弹性云服务器运行状态，云服务平台提供了云监控。您可以使用该服务监控您的弹性云服务器，执行自动实时监控、告警和通知操作，帮助您更好地了解弹性云服务器的各项性能指标。

主机监控分为基础监控、操作系统监控和进程监控。

- 基础监控：ECS自动上报的监控指标，可以监控CPU使用率等指标。
- 操作系统监控：通过在ECS中安装Agent插件，为用户提供服务器的系统级、主动式、细颗粒度监控服务。除了CPU使用率等指标外，还可以支持内存使用率（Linux）等指标。
- 进程监控：通过在ECS中安装Agent插件，对主机内活跃进程进行监控，默认采集活跃进程消耗的CPU、内存，以及打开的文件数量等信息。

安装配置Agent相关操作请参考云监控服务 [“Agent安装配置方式说明”](#)。Agent安装配置完成后，请勿删除Agent进程，否则，会导致监控数据无法上报。

说明

GPU加速型实例若要进行GPU监控，需要安装Agent及对应的GPU监控插件，安装方法，请参见[异构类实例安装支持对应监控的CES Agent（Linux）](#)。

通过后续章节，您可以了解以下内容：

- 弹性云服务器当前支持的基础监控指标
- 弹性云服务器操作系统监控的监控指标（安装Agent）
- 弹性云服务器进程监控的监控指标（安装Agent）
- GPU加速型实例安装GPU监控插件（Linux，公测）
- 如何自定义弹性云服务器告警规则
- 如何查看弹性云服务器运行状态进行日常监控

一键告警

弹性云服务器运行在物理机上，虽然提供了多种机制来保证系统的可靠性、容错能力和高可用性，但是，服务器的硬件、电源等部件仍有较小概率的损坏。云平台默认提

供了自动恢复功能，当弹性云服务器所在的硬件出现故障时，系统会自动将弹性云服务器迁移至正常的物理机，保障您受到的影响最小，该过程会导致云服务器重启。[了解更多](#)

您可以在云监控服务控制台为弹性云服务器开启“一键告警”功能，以便在HA发生（弹性云服务器所在的物理机出现故障，系统自动迁移弹性云服务器至正常的物理机）时，及时获得通知。配置方法请参见[一键告警](#)。

相关链接

- [云监控服务功能总览](#)
- [Windows云服务器带宽和CPU利用率高问题排查方法](#)
- [Linux云服务器带宽和CPU占用率高问题排查方法](#)

17.2 弹性云服务器支持的基础监控指标

功能说明

本节定义了弹性云服务器上报云监控的基础监控指标的命名空间，监控指标列表，各项监控指标的具体含义与使用说明，用户可以通过云监控检索弹性云服务器服务产生的监控指标和告警信息。

命名空间

SYS.ECS

基础监控指标支持列表

对于不同的操作系统、不同的弹性云服务器类型，支持的基础监控指标有所差异，具体如[表17-1](#)所示。其中，√表示支持，×表示不支持。

说明

- 对于部分监控指标，需弹性云服务器使用的镜像安装UVP VMTools，UVP VMTools安装的具体操作，请参见<https://github.com/UVP-Tools/UVP-Tools/>。
- QingTian实例不支持上报“内存使用率”基础监控指标。
- 对于不支持上报的监控指标，需弹性云服务器安装Agent。安装成功后，您可以登录控制台，打开“云监控”服务，在“主机监控 > 弹性云服务器 > 操作系统监控”页面查看各项监控指标，如“AGT.用户空间CPU使用率”，具体请参见[弹性云服务器中操作系统监控的监控指标](#)。
 - Windows云服务器安装Agent的具体操作，请参见“[安装配置Agent（Windows）](#)”。
 - Linux云服务器安装Agent的具体操作，请参见“[安装配置Agent（Linux）](#)”。

表 17-1 弹性云服务器基础监控指标支持列表

指标ID	监控指标	Windows弹性云服务器		Linux弹性云服务器	
		虚拟化类型为XEN的弹性云服务器	虚拟化类型为KVM/QingTian的弹性云服务器	虚拟化类型为XEN的弹性云服务器	虚拟化类型为KVM/QingTian的弹性云服务器
-	-	虚拟化类型为XEN的弹性云服务器	虚拟化类型为KVM/QingTian的弹性云服务器	虚拟化类型为XEN的弹性云服务器	虚拟化类型为KVM/QingTian的弹性云服务器
cpu_util	CPU使用率	√	√	√	√
mem_util	内存使用率	√	√	√（镜像需安装UVP VMTools，否则无法获取该监控指标。）	×（暂不支持）
disk_util_inband	磁盘使用率	√	√	√（镜像需安装UVP VMTools，否则无法获取该监控指标。）	×（暂不支持）
disk_read_bytes_rate	磁盘读带宽	√	√	√	√
disk_write_bytes_rate	磁盘写带宽	√	√	√	√
disk_read_requests_rate	磁盘读IOPS	√	√	√	√
disk_write_requests_rate	磁盘写IOPS	√	√	√	√
network_incoming_bytes_rate_inband	带内网络流入速率	√（镜像需安装UVP VMTools，否则无法获取该监控指标。）	√	√（镜像需安装UVP VMTools，否则无法获取该监控指标。）	×（暂不支持）
network_outgoing_bytes_rate_inband	带内网络流出速率	√（镜像需安装UVP VMTools，否则无法获取该监控指标。）	√	√（镜像需安装UVP VMTools，否则无法获取该监控指标。）	×（暂不支持）

指标ID	监控指标	Windows弹性云服务器		Linux弹性云服务器	
network_incoming_bytes_aggregate_rate	带外网络流入速率	√（镜像如果安装了UVP VMTools，则不提供该指标，请使用带内网络流出速率。）	√	√（镜像如果安装了UVP VMTools，则不提供该指标，请使用带内网络流出速率。）	√
network_outgoing_bytes_aggregate_rate	带外网络流出速率	√（镜像如果安装了UVP VMTools，则不提供该指标，请使用带内网络流出速率。）	√	√（镜像如果安装了UVP VMTools，则不提供该指标，请使用带内网络流出速率。）	√
cpu_credit_usage	CPU积分使用量	×	√（仅T6型支持）	×	√（仅T6型支持）
cpu_credit_balance	CPU积分累积量	×	√（仅T6型支持）	×	√（仅T6型支持）
network_vm_connections	网络连接数	×	√	×	√
network_vm_bandwidth_in	虚拟机入方向带宽	×	√	×	√
network_vm_bandwidth_out	虚拟机出方向带宽	×	√	×	√
network_vm_pps_in	虚拟机入方向PPS	×	√	×	√
network_vm_pps_out	虚拟机出方向PPS	×	√	×	√
network_vm_newconnections	虚拟机整机新建连接数	×	√	×	√

说明

“√”表示支持该监控指标，“×”表示不支持该监控指标。

各项基础监控指标的具体含义与使用说明如表17-2所示。

以下监控指标（原始指标）的监控周期如下：

- 虚拟化类型为XEN的弹性云服务器：4分钟。
- 虚拟化类型为KVM、QingTian的弹性云服务器：5分钟。

表 17-2 弹性云服务器支持的基础监控指标

指标ID	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标，本列监控周期值适用于KVM实例）
cpu_util	CPU使用率	该指标用于统计弹性云服务器的CPU使用率。 该指标为从物理机层面采集的CPU使用率，数据准确性低于从弹性云服务器内部采集的数据，查看详情。 计算公式：单个弹性云服务器CPU使用率 / 单个弹性云服务器的CPU总核数。	0-100	%	不涉及	云服务器	5分钟
mem_util	内存使用率	该指标用于统计弹性云服务器的内存使用率。 如果用户使用的镜像未安装UVP VMTools，则无法获取该监控指标。 计算公式：该弹性云服务器内存使用量 / 该弹性云服务器内存总量。 说明 内存使用率监控指标不支持QingTian实例。	0-100	%	不涉及	云服务器	5分钟

指标ID	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标，本列监控周期值适用于KVM实例）
disk_util_inband	磁盘使用率	该指标用于统计弹性云服务器的磁盘使用情况。 如果用户使用的镜像未安装UVP VMTools，则无法获取该监控指标。 计算公式：该弹性云服务器磁盘使用容量 /该弹性云服务器磁盘总容量。	0-100	%	不涉及	云服务器	5分钟
disk_read_bytes_rate	磁盘读带宽	该指标用于统计每秒从弹性云服务器读出数据量。 计算公式：该弹性云服务器的磁盘读出的字节数之和 / 测量周期。 byte_out = (rd_bytes - last_rd_bytes) /时间差。	≥ 0	byte/s	1024(IEC)	云服务器	5分钟
disk_write_bytes_rate	磁盘写带宽	该指标用于统计每秒写到弹性云服务器的数据量。 计算公式：该弹性云服务器的磁盘写入的字节数之和 / 测量周期。	≥ 0	byte/s	1024(IEC)	云服务器	5分钟
disk_read_requests_rate	磁盘读 IOPS	该指标用于统计每秒从弹性云服务器读取数据的请求次数。 计算公式：请求读取该弹性云服务器磁盘的次数之和 / 测量周期。 req_out = (rd_req - last_rd_req) /时间差。	≥ 0	Requests/s	不涉及	云服务器	5分钟

指标ID	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标，本列监控周期值适用于KVM实例）
disk_write_requests_rate	磁盘写 IOPS	该指标用于统计每秒从弹性云服务器写数据的请求次数。 计算公式：请求写入该弹性云服务器磁盘的次数之和 / 测量周期。 $req\_in = (wr\_req - last\_wr\_req) / 时间差$	≥ 0	Req ues t/s	不 涉 及	云服务器	5分钟
network_incoming_bytes_rate_inband	带内网络流入速率	该指标用于在弹性云服务器内统计每秒流入弹性云服务器的网络流量。 计算公式：该弹性云服务器的带内网络流入字节数之和/测量周期。	≥ 0	byt e/s	10 24(IEC)	云服务器	5分钟
network_outgoing_bytes_rate_inband	带内网络流出速率	该指标用于在弹性云服务器内统计每秒流出弹性云服务器的网络流量。 计算公式：该弹性云服务器的带内网络流出字节数之和 / 测量周期。	≥ 0	byt e/s	10 24(IEC)	云服务器	5分钟
network_incoming_bytes_aggregate_rate	带外网络流入速率	该指标用于在虚拟化层统计每秒流入弹性云服务器的网络流量。 计算公式：该弹性云服务器的带外网络流入字节数之和 / 测量周期。 当使用SRIOV时，无法获取该监控指标。	≥ 0	byt e/s	10 24(IEC)	云服务器	5分钟

指标ID	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标，本列监控周期值适用于KVM实例）
network_outgoing_bytes_aggregate_rate	带外网络流出速率	该指标用于在虚拟化层统计每秒流出弹性云服务器的网络流量。 计算公式：该弹性云服务器的带外网络流出字节数之和 / 测量周期。 当使用SRIOV时，无法获取该监控指标。	≥ 0	byte/s	1024(IEC)	云服务器	5分钟
cpu_credit_usage	CPU积分使用量	该指标表示积分型实例累积花费的CPU积分。 计算公式：一个CPU积分等于一个vCPU按照100%利用率，运行1分钟。 说明 仅T6型支持。	≥ 0	Credit	不涉及	云服务器	5分钟
cpu_credit_balance	CPU积分累积量	该指标表示实例自启动后已累积获得的CPU积分。 计算公式：根据Flavor定义，CPU积分/小时*小时-积分使用量。 说明 当累积积分超过上限以后，不再累积积分，初始积分不计入上限。 仅T6型支持。	≥ 0	Credit	不涉及	云服务器	5分钟
network_vm_connections	网络连接数	该指标表示弹性云服务器已经使用的TCP和UDP的连接数总和。 说明 该指标通过带外采集，因此可能会出现该指标值大于OS中查询到的网络连接数的情况。	≥ 0	Count	不涉及	云服务器	5分钟

指标ID	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标，本列监控周期值适用于KVM实例）
network_vm_bandwidth_in	虚拟机入方向带宽	虚拟机整机每秒接收的比特数，此处为公网和内网流量总和。	≥ 0	Byte/s	1024(IEC)	云服务器	5分钟
network_vm_bandwidth_out	虚拟机出方向带宽	虚拟机整机每秒发送的比特数，此处为公网和内网流量总和。	≥ 0	Byte/s	1024(IEC)	云服务器	5分钟
network_vmpps_in	虚拟机入方向PPS	虚拟机整机每秒接收的数据包数，此处为公网和内网数据包总和。	≥ 0	Packet/s	不涉及	云服务器	5分钟
network_vmpps_out	虚拟机出方向PPS	虚拟机整机每秒发送的数据包数，此处为公网和内网数据包总和。	≥ 0	Packet/s	不涉及	云服务器	5分钟
network_vm_newconnections	虚拟机整机新建连接数	虚拟机整机新建连接数，包括TCP协议、UDP协议以及ICMP协议等。	≥ 0	connections/s	不涉及	云服务器	5分钟

维度

维度	Key	Value
云服务器	instance_id	云服务器ID。

17.3 弹性云服务器支持的操作系统监控指标（安装 Agent）

功能说明

通过在弹性云服务器中安装Agent插件，可以为用户提供服务器的系统级、主动式、细颗粒度监控服务。本节定义了弹性云服务器上报云监控的操作系统监控指标。

操作系统监控目前支持的监控指标有：CPU相关监控项、CPU负载类相关监控项、内存相关监控项、磁盘相关监控项、磁盘I/O相关监控项、文件系统类相关监控项、网卡

类相关监控项、NTP类相关监控项、TCP连接数类相关监控、GPU相关监控项、NPU相关监控项。

安装Agent后，对于不同的操作系统、不同的弹性云服务器类型，您可以查看不同类型的操作系统监控指标。指标采集周期是1分钟。

命名空间

AGT.ECS

操作系统监控指标：CPU

表 17-3 CPU 相关监控指标说明

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
cpu_usage	(Agent) CPU使用率	该指标用于统计测量对象当前CPU使用率。 - 采集方式（Linux）：通过计算采集周期内/proc/stat中的变化得出cpu使用率。用户可以通过top命令查看 %Cpu(s) 值。 - 采集方式（Windows）：通过WindowsAPI GetSystemTimes 获取。	0-100	%	不涉及	云服务器	1分钟
cpu_usage_idle	(Agent) CPU空闲时间占比	该指标用于统计测量对象当前CPU空闲时间占比。 - 采集方式（Linux）：通过计算采集周期内/proc/stat中的变化得出CPU空闲时间占比。 - 采集方式（Windows）：通过WindowsAPI GetSystemTimes 获取。	0-100	%	不涉及	云服务器	1分钟

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
cpu_usage_user	(Agent) 用户空间CPU使用率	该指标用于统计测量对象当前用户空间占用CPU使用率。 - 采集方式（Linux）：通过计算采集周期内/proc/stat中的变化得出cpu使用率。用户可以通过top命令查看 %Cpu(s) us值。 - 采集方式（Windows）：通过WindowsAPI GetSystemTimes 获取。	0-100	%	不涉及	云服务器	1分钟
cpu_usage_system	(Agent) 内核空间CPU使用率	该指标用于统计测量对象当前内核空间占用CPU使用率。 - 采集方式（Linux）：通过计算采集周期内/proc/stat中的变化得出内核空间CPU使用率。用户可以通过top命令查看 %Cpu(s) sy值。 - 采集方式（Windows）：通过WindowsAPI GetSystemTimes 获取。	0-100	%	不涉及	云服务器	1分钟

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
cpu_usage_other	(Agent) 其他CPU使用率	该指标用于统计测量对象其他占用CPU使用率。 - 采集方式（Linux）：其他CPU使用率=1- 空闲CPU使用率（%）- 内核空间CPU使用率- 用户空间CPU使用率。 - 采集方式（Windows）：其他CPU使用率=1- 空闲CPU使用率（%）- 内核空间CPU使用率- 用户空间CPU使用率。	0-100	%	不涉及	云服务器	1分钟
cpu_usage_nice	(Agent) Nice进程CPU使用率	该指标用于统计测量对象当前Nice进程CPU使用率。 - 采集方式（Linux）：通过计算采集周期内/ proc/stat中的变化得出Nice进程CPU使用率。用户可以通过top命令查看%Cpu(s) ni值。 - 采集方式（Windows）：暂不支持。	0-100	%	不涉及	云服务器	1分钟

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
cpu_usage_iowait	(Agent) iowait 状态占比	该指标用于统计测量对象当前iowait状态占用CPU的比率。 - 采集方式（Linux）：通过计算采集周期内/proc/stat中的变化得出iowait状态占比。用户可以通过top命令查看%Cpu(s) wa值。 - 采集方式（Windows）：暂不支持。	0-100	%	不涉及	云服务器	1分钟
cpu_usage_irq	(Agent) CPU中断时间占比	该指标用于统计测量对象当前CPU处理中断用时占用CPU时间的比率。 - 采集方式（Linux）：通过计算采集周期内/proc/stat中的变化得出CPU中断时间占比。用户可以通过top命令查看%Cpu(s) hi值。 - 采集方式（Windows）：暂不支持。	0-100	%	不涉及	云服务器	1分钟
cpu_usage_softirq	(Agent) CPU软中断时间占比	该指标用于统计测量对象当前CPU处理软中断时间占用CPU时间的比率。 - 采集方式（Linux）：通过计算采集周期内/proc/stat中的变化得出CPU软中断时间占比。用户可以通过top命令查看%Cpu(s) si值。 - 采集方式（Windows）：暂不支持。	0-100	%	不涉及	云服务器	1分钟

操作系统监控指标：CPU 负载

表 17-4 CPU 负载指标说明

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
load_average 1	(Agent) 1分钟平均负载	该指标用于统计测量对象过去1分钟的CPU平均负载。 采集方式（Linux）：通过/proc/loadavg中load1/逻辑CPU个数得到。用户可以通过top命令查看load1值。	≥0	不涉及	不涉及	云服务器	1分钟
load_average 5	(Agent) 5分钟平均负载	该指标用于统计测量对象过去5分钟的CPU平均负载。 采集方式（Linux）：通过/proc/loadavg中load5/逻辑CPU个数得到。用户可以通过top命令查看load5值。	≥0	不涉及	不涉及	云服务器	1分钟
load_average 15	(Agent) 15分钟平均负载	该指标用于统计测量对象过去15分钟的CPU平均负载。 采集方式（Linux）：通过/proc/loadavg中load15/逻辑CPU个数得到。用户可以通过top命令查看load15值。	≥0	不涉及	不涉及	云服务器	1分钟

说明

Windows系统暂不支持CPU负载指标。

操作系统监控指标：内存

表 17-5 内存相关监控指标说明

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
mem_available	(Agent) 可用内存	该指标用于统计测量对象的可用内存。 - 采集方式（Linux）：通过/proc/meminfo文件获取， - 若/proc/meminfo中显示MemAvailable，则直接可得 - 若/proc/meminfo中不显示MemAvailable，则MemAvailable=MemFree+Buffers+Cached - 采集方式（Windows）：计算方法为（内存总量-已用内存量）。通过WindowsAPI GlobalMemoryStatusEx获取。	≥0	GB	不涉及	云服务器	1分钟

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
mem_usedPercent	(Agent) 内存使用率	该指标用于统计测量对象的内存使用率。 - 采集方式（Linux）：通过 /proc/meminfo 文件获取，$(\text{MemTotal} - \text{MemAvailable}) / \text{MemTotal}$ - 若 /proc/meminfo 中显示 MemAvailable，则 $\text{MemUsedPercent} = (\text{MemTotal} - \text{MemAvailable}) / \text{MemTotal}$ - 若 /proc/meminfo 中不显示 MemAvailable，则 $\text{MemUsedPercent} = (\text{MemTotal} - \text{MemFree} - \text{Buffers} - \text{Cached}) / \text{MemTotal}$ - 采集方式（Windows）：计算方法为（已用内存量/内存总量*100%）。	0-100	%	不涉及	云服务器	1分钟
mem_free	(Agent) 空闲内存量	该指标用于统计测量对象的空闲内存量。 - 采集方式（Linux）：通过 /proc/meminfo 获取。 - 采集方式（Windows）：暂不支持。	≥0	GB	不涉及	云服务器	1分钟

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
mem_buffers	(Agent) Buffers 占用量	该指标用于统计测量对象的Buffers内存量。 - 采集方式（Linux）：通过/proc/meminfo获取。用户可以通过top命令查看 KiB Mem:buffers值。 - 采集方式（Windows）：暂不支持。	≥0	GB	不涉及	云服务器	1分钟
mem_cached	(Agent) Cache 占用量	该指标用于统计测量对象Cache内存量。 - 采集方式（Linux）：通过/proc/meminfo获取。用户可以通过top命令查看 KiB Swap:cached Mem值。 - 采集方式（Windows）：暂不支持。	≥0	GB	不涉及	云服务器	1分钟
total_open_files	(Agent) 文件句柄总数	该指标用于统计测量对象的所有进程使用的句柄总和。 - 采集方式（Linux）：通过/proc/{pid}/fd文件汇总所有进程使用的句柄数。 - 采集方式（Windows）：暂不支持。	≥0	Count	不涉及	云服务器	1分钟

操作系统监控指标：磁盘

说明

- 目前仅支持物理磁盘指标的采集，不支持通过网络文件系统协议挂载的磁盘。
- 会默认屏蔽docker相关的挂载点。挂载点前缀如下：
`/var/lib/docker/mnt/paas/kubernetes/var/lib/mesos`

表 17-6 磁盘相关监控指标说明

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
disk_free	(Agent) 磁盘剩余存储量	该指标用于统计测量对象磁盘的剩余存储空间。 - 采集方式（Linux）：执行df-h命令，查看Avail列数据。挂载点前缀路径长度不能超过64个字符，必须以字母开头，只能包含0-9/a-z/A-Z/-/./~。 - 采集方式（Windows）：使用WMI接口GetDiskFreeSpaceExW获取磁盘空间数据。挂载点前缀路径长度不能超过64个字符，必须以字母开头，只能包含0-9/a-z/A-Z/-/./~。	≥0	GB	不涉及	云服务器-挂载点	1分钟

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
disk_total	(Agent) 磁盘存储总量	该指标用于统计测量对象磁盘存储总量。 - 采集方式（Linux）：执行df-h命令，查看Size列数据。挂载点前缀路径长度不能超过64个字符，必须以字母开头，只能包含0-9/a-z/A-Z/-/./~。 - 采集方式（Windows）：使用WMI接口GetDiskFreeSpaceExW获取磁盘空间数据。挂载点前缀路径长度不能超过64个字符，必须以字母开头，只能包含0-9/a-z/A-Z/-/./~。	≥0	GB	不涉及	云服务器-挂载点	1分钟

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
disk_used	(Agent) 磁盘已用存量	该指标用于统计测量对象磁盘的已用存储空间。 - 采集方式（Linux）：执行df-h命令，查看Used列数据。挂载点前缀路径长度不能超过64个字符，必须以字母开头，只能包含0-9/a-z/A-Z/-/./~。 - 采集方式（Windows）：使用WMI接口GetDiskFreeSpaceExW获取磁盘空间数据。挂载点前缀路径长度不能超过64个字符，必须以字母开头，只能包含0-9/a-z/A-Z/-/./~。	≥0	GB	不涉及	云服务器-挂载点	1分钟

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
disk_usedPercent	(Agent) 磁盘使用率	该指标用于统计测量对象磁盘使用率，以百分比为单位。计算方式为: 磁盘已用存储量/磁盘存储总量。 - 采集方式（Linux）：通过计算Used/Size得出。挂载点前缀路径长度不能超过64个字符，必须以字母开头，只能包含0-9/a-z/A-Z/-/./~。 - 采集方式（Windows）：使用WMI接口GetDiskFreeSpaceExW获取磁盘空间数据。挂载点前缀路径长度不能超过64个字符，必须以字母开头，只能包含0-9/a-z/A-Z/-/./~。	0-100	%	不涉及	云服务器-挂载点	1分钟

操作系统监控指标：磁盘 I/O

表 17-7 磁盘 I/O 相关监控指标说明

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
disk_agt_read_bytes_rate	(Agent) 磁盘读速率	该指标用于统计每秒从测量对象读出数据量。 - 采集方式（Linux）： 通过计算采集周期内/proc/diskstats中对应设备第六列数据的变化得出磁盘读速率。 挂载点前缀路径长度不能超过64个字符，必须以字母开头，只能包含0-9/a-z/A-Z/-/./~。 - 采集方式（Windows）： - 使用WMI中Win32_PerfFormattedData_PerfDisk_LogicalDisk对象获取磁盘I/O数据，每采集周期读取一次该对象，读取该对象返回的瞬时值代表该采集周期的指标值。 - 挂载点前缀路径长度不能超过64个字符，必须以字母开头，只能包含0-9/a-z/A-Z/-/./~。 - 高CPU情况下存在获取超时的现象，会导致无法获取监控数据。	≥ 0	byte/s	1024(IEC)	- 云服务器 - 磁盘 - 云服务器 - 挂载点	1分钟

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
disk_agt_read_requests_rate	(Agent) 磁盘读操作速率	该指标用于统计每秒从测量对象读取数据的请求次数。 - 采集方式（Linux）： 通过计算采集周期内/proc/diskstats中对应设备第四列数据的变化得出磁盘读操作速率。 挂载点前缀路径长度不能超过64个字符，必须以字母开头，只能包含0-9/a-z/A-Z/-/./~。 - 采集方式（Windows）： - 使用WMI中Win32_PerfFormattedData_PerfDisk_LogicalDisk对象获取磁盘I/O数据，每采集周期读取一次该对象，读取该对象返回的瞬时值代表该采集周期的指标值。 - 挂载点前缀路径长度不能超过64个字符，必须以字母开头，只能包含0-9/a-z/A-Z/-/./~。 - 高CPU情况下存在获取超时的现象，会导致无法获取监控数据。	≥ 0	Request/s	不涉及	- 云服务器 - 磁盘 - 云服务器 - 挂载点	1分钟

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
disk_agt_write_bytes_rate	(Agent) 磁盘写速率	该指标用于统计每秒写到测量对象的数据量。 - 采集方式（Linux）： 通过计算采集周期内/proc/diskstats中对应设备第十列数据的变化得出磁盘写速率。 挂载点前缀路径长度不能超过64个字符，必须以字母开头，只能包含0-9/a-z/A-Z/-/./~。 - 采集方式（Windows）： - 使用WMI中Win32_PerfFormattedData_PerfDisk_LogicalDisk对象获取磁盘I/O数据，每采集周期读取一次该对象，读取该对象返回的瞬时值代表该采集周期的指标值。 - 挂载点前缀路径长度不能超过64个字符，必须以字母开头，只能包含0-9/a-z/A-Z/-/./~。 - 高CPU情况下存在获取超时的现象，会导致无法获取监控数据。	≥ 0	byte/s	1024(IEC)	- 云服务器-磁盘 - 云服务器-挂载点	1分钟

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
disk_agt_write_requests_rate	(Agent) 磁盘写操作速率	该指标用于统计每秒向测量对象写数据的请求次数。 - 采集方式（Linux）： 通过计算采集周期内/proc/diskstats中对应设备第八列数据的变化得出磁盘写操作速率。 挂载点前缀路径长度不能超过64个字符，必须以字母开头，只能包含0-9/a-z/A-Z/-/./~。 - 采集方式（Windows）： - 使用WMI中Win32_PerfFormattedData_PerfDisk_LogicalDisk对象获取磁盘I/O数据，每采集周期读取一次该对象，读取该对象返回的瞬时值代表该采集周期的指标值。 - 挂载点前缀路径长度不能超过64个字符，必须以字母开头，只能包含0-9/a-z/A-Z/-/./~。 - 高CPU情况下存在获取超时的现象，会导致无法获取监控数据。	≥ 0	Request/s	不涉及	- 云服务器 - 磁盘 - 云服务器 - 挂载点	1分钟

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
disk_readTime	(Agent) 读操作平均耗时	该指标用于统计测量对象磁盘读操作平均耗时。 - 采集方式（Linux）： 通过计算采集周期内/proc/diskstats中对应设备第七列数据的变化得出磁盘读操作平均耗时。 - 挂载点前缀路径长度不能超过64个字符，必须以字母开头，只能包含0-9/a-z/A-Z/-/./~。 - 采集方式（Windows）：暂不支持。	≥ 0	ms/Count	不涉及	- 云服务器 - 磁盘 - 云服务器 - 挂载点	1分钟
disk_writeTime	(Agent) 写操作平均耗时	该指标用于统计测量对象磁盘写操作平均耗时。 - 采集方式（Linux）： 通过计算采集周期内/proc/diskstats中对应设备第十一列数据的变化得出磁盘写操作平均耗时。 - 挂载点前缀路径长度不能超过64个字符，必须以字母开头，只能包含0-9/a-z/A-Z/-/./~。 - 采集方式（Windows）：暂不支持。	≥ 0	ms/Count	不涉及	- 云服务器 - 磁盘 - 云服务器 - 挂载点	1分钟

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
disk_io Utils	(Agent) 磁盘I/O 使用率	该指标用于统计测量对象磁盘I/O使用率。 - 采集方式（Linux）： 通过计算采集周期内/proc/diskstats中对应设备第十三列数据的变化得出磁盘I/O使用率。 挂载点前缀路径长度不能超过64个字符，必须以字母开头，只能包含0-9/a-z/A-Z/-/./~。 - 采集方式（Windows）：暂不支持。	0-100	%	不涉及	- 云服务器 - 磁盘 - 云服务器 - 挂载点	1分钟
disk_q ueue_l ength	(Agent) 平均队 列长度	该指标反映指定时间段内磁盘的繁忙程度，可用于评估磁盘I/O性能，指标值越大代表磁盘越繁忙，I/O性能越差。 - 采集方式（Linux）： 通过计算采集周期内/proc/diskstats中对应设备第十四列数据的变化与指标采集周期时间相除得出指标的值。 挂载点前缀路径长度不能超过64个字符，必须以字母开头，只能包含0-9/a-z/A-Z/-/./~。 - 采集方式（Windows）：暂不支持。	≥ 0	count	不涉及	- 云服务器 - 磁盘 - 云服务器 - 挂载点	1分钟

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
disk_write_bytes_per_operation	(Agent) 平均写操作大小	该指标用于统计指定时间段内，平均每个写 I/O 操作传输的字节数。 - 采集方式（Linux）： 通过计算采集周期内 /proc/diskstats 中对应设备第十列数据的变化与第八列数据的变化相除得出磁盘平均写操作大小。 - 挂载点前缀路径长度不能超过 64 个字符，必须以字母开头，只能包含 0-9/a-z/A-Z/-/./~。 - 采集方式（Windows）：暂不支持。	≥ 0	Byte/operation	不涉及	- 云服务器 - 磁盘 - 云服务器 - 挂载点	1 分钟
disk_read_bytes_per_operation	(Agent) 平均读操作大小	该指标用于统计指定时间段内，平均每个读 I/O 操作传输的字节数。 - 采集方式（Linux）： 通过计算采集周期内 /proc/diskstats 中对应设备第六列数据的变化与第四列数据的变化相除得出磁盘平均读操作大小。 - 挂载点前缀路径长度不能超过 64 个字符，必须以字母开头，只能包含 0-9/a-z/A-Z/-/./~。 - 采集方式（Windows）：暂不支持。	≥ 0	Byte/operation	不涉及	- 云服务器 - 磁盘 - 云服务器 - 挂载点	1 分钟

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
disk_io_svctm	(Agent) 平均I/O服务时长	该指标用于统计指定时间段内，平均每个读或写I/O的操作时长。 - 采集方式（Linux）： 通过计算采集周期内/proc/diskstats中对应设备第十三列数据的变化与第四列数据和第八列数据之和的变化相除得出磁盘平均I/O时长。 - 挂载点前缀路径长度不能超过64个字符，必须以字母开头，只能包含0-9/a-z/A-Z/-/./~。 - 采集方式（Windows）：暂不支持。	≥ 0	ms/op	不涉及	- 云服务器 - 磁盘 - 云服务器 - 挂载点	1分钟
disk_device_used_percent	块设备使用率	该指标用于统计测量对象物理磁盘使用率，以百分比为单位。计算方式为: 所有已挂载磁盘分区已用存储量/磁盘存储总量。 - 采集方式（Linux）：通过汇总每个挂载点的磁盘使用量，再通过磁盘扇区大小和扇区数量计算出磁盘总大小，计算出整体磁盘使用率 - 采集方式（Windows）：暂不支持。	0-100	%	不涉及	云服务器 - 磁盘	1分钟

操作系统监控指标：文件系统

表 17-8 文件系统类监控指标说明

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
disk_fs_rwstate	(Agent) 文件系统读写状态	该指标用于统计测量对象挂载文件系统的读写状态。状态分为：可读写（0）/只读（1）。 采集方式（Linux）：通过读取/proc/mounts中第四列文件系统挂载参数获得。	0: 可读写 1: 只读	不涉及	不涉及	云服务器-挂载点	1分钟
disk_inodesTotal	(Agent) inode空间大小	该指标用于统计测量对象当前磁盘的inode空间量。 采集方式（Linux）：执行df -i命令，查看Inodes列数据。挂载点前缀路径长度不能超过64个字符，必须以字母开头，只能包含0-9/a-z/A-Z/-/./~。	≥ 0	Count	不涉及	云服务器-挂载点	1分钟
disk_inodesUsed	(Agent) inode已使用空间	该指标用于统计测量对象当前磁盘已使用的inode空间量。 采集方式（Linux）：执行df -i命令，查看IUsed列数据。挂载点前缀路径长度不能超过64个字符，必须以字母开头，只能包含0-9/a-z/A-Z/-/./~。	≥ 0	Count	不涉及	云服务器-挂载点	1分钟
disk_inodesUsedPercent	(Agent) inode已使用占比	该指标用于统计测量对象当前磁盘已使用的inode占比。 采集方式（Linux）：执行df -i命令，查看IUse%列数据。挂载点前缀路径长度不能超过64个字符，必须以字母开头，只能包含0-9/a-z/A-Z/-/./~。	0-100	%	不涉及	云服务器-挂载点	1分钟

 说明

Windows系统暂不支持文件系统类监控指标。

操作系统监控指标：网卡

表 17-9 网卡相关监控指标说明

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
net_bit Recv	(Agent) 出网带宽	该指标用于统计测量对象网卡每秒发送的比特数。 - 采集方式（Linux）：通过计算采集周期内/proc/net/dev中的变化得出。 - 采集方式（Windows）：使用WMI中MibIfRow对象获取网络指标数据。	≥ 0	bit/s	10 24(IEC)	云服务器	1分钟
net_bit Sent	(Agent) 入网带宽	该指标用于统计测量对象网卡每秒接收的比特数。 - 采集方式（Linux）：通过计算采集周期内/proc/net/dev中的变化得出。 - 采集方式（Windows）：使用WMI中MibIfRow对象获取网络指标数据。	≥ 0	bit/s	10 24(IEC)	云服务器	1分钟

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
net_packetRecv	(Agent) 网卡包接收速率	该指标用于统计测量对象网卡每秒接收的数据包数。 - 采集方式（Linux）：通过计算采集周期内/proc/net/dev中的变化得出。 - 采集方式（Windows）：使用WMI中MibIfRow对象获取网络指标数据。	≥ 0	Cou nts/ s	不 涉 及	云服务器	1分钟
net_packetSent	(Agent) 网卡包发送速率	该指标用于统计测量对象网卡每秒发送的数据包数。 - 采集方式（Linux）：通过计算采集周期内/proc/net/dev中的变化得出。 - 采集方式（Windows）：使用WMI中MibIfRow对象获取网络指标数据。	≥ 0	Cou nts/ s	不 涉 及	云服务器	1分钟
net_errin	(Agent) 接收误包率	该指标用于统计测量对象网卡每秒接收的错误数据包数量占所接收的数据包的比率。 - 采集方式（Linux）：通过计算采集周期内/proc/net/dev中的变化得出。 - 采集方式（Windows）：暂不支持。	0-100	%	不 涉 及	云服务器	1分钟

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
net_errout	(Agent) 发送误包率	该指标用于统计测量对象网卡每秒发送的错误数据包数量占所发送的数据包的比率。 - 采集方式（Linux）：通过计算采集周期内/proc/net/dev中的变化得出。 - 采集方式（Windows）：暂不支持。	0-100	%	不涉及	云服务器	1分钟
net_dropin	(Agent) 接收丢包率	该指标用于统计测量对象网卡每秒接收并已丢弃的数据包数量占所接收的数据包的比率 - 采集方式（Linux）：通过计算采集周期内/proc/net/dev中的变化得出。 - 采集方式（Windows）：暂不支持。	0-100	%	不涉及	云服务器	1分钟
net_dropout	(Agent) 发送丢包率	该指标用于统计测量对象网卡每秒发送并已丢弃的数据包数量占所发送的数据包的比率。 - 采集方式（Linux）：通过计算采集周期内/proc/net/dev中的变化得出。 - 采集方式（Windows）：暂不支持。	0-100	%	不涉及	云服务器	1分钟

操作系统监控指标：NTP

表 17-10 NTP 类监控指标说明

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
ntp_offset	(Agent) NTP偏移量	该指标用于统计测量对象当前NTP偏移量。 - 采集方式（Linux）：执行 chronyc sources -v 命令，获取偏移量。 - 采集方式（Windows）：暂不支持。	≥ 0	ms	不涉及	云服务器	1分钟

操作系统监控指标：TCP

表 17-11 TCP 类监控指标说明

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
net_tcp_total	(Agent) TCP TOTAL	该指标用于统计测量对象所有状态的TCP连接数总和。 - 采集方式（Linux）：通过 /proc/net/tcp 文件获取到所有状态的TCP连接，再统计每个状态的连接数量。 - 采集方式（Windows）：通过 Windows API GetTcpTable2 获取。	≥ 0	Count	不涉及	云服务器	1分钟

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
net_tcp_established	(Agent) TCP ESTABLISHED	该指标用于统计测量对象处于ESTABLISHED状态的TCP连接数量。 - 采集方式（Linux）：通过/proc/net/tcp文件获取到所有状态的TCP连接，再统计每个状态的连接数量。 - 采集方式（Windows）：通过WindowsAPI GetTcpTable2获取。	≥ 0	Count	不涉及	云服务器	1分钟
net_tcp_sys_sent	(Agent) TCP SYS_SENT	该指标用于统计测量对象处于请求连接状态的TCP连接数量。 - 采集方式（Linux）：通过/proc/net/tcp文件获取到所有状态的TCP连接，再统计每个状态的连接数量。 - 采集方式（Windows）：通过WindowsAPI GetTcpTable2获取。	≥ 0	Count	不涉及	云服务器	1分钟
net_tcp_sys_recv	(Agent) TCP SYS_RECV	该指标用于统计测量对象服务器端收到的请求连接的TCP数量。 - 采集方式（Linux）：通过/proc/net/tcp文件获取到所有状态的TCP连接，再统计每个状态的连接数量。 - 采集方式（Windows）：通过WindowsAPI GetTcpTable2获取。	≥ 0	Count	不涉及	云服务器	1分钟

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
net_tcp_fin_wait1	(Agent) TCP FIN_WAIT1	该指标用于统计测量对象客户端主动关闭且没有收到服务端ACK的TCP连接数量。 - 采集方式（Linux）：通过/proc/net/tcp文件获取到所有状态的TCP连接，再统计每个状态的连接数量。 - 采集方式（Windows）：通过WindowsAPI GetTcpTable2获取。	≥ 0	Count	不涉及	云服务器	1分钟
net_tcp_fin_wait2	(Agent) TCP FIN_WAIT2	该指标用于统计测量对象处于FIN_WAIT2状态的TCP连接数量。 - 采集方式（Linux）：通过/proc/net/tcp文件获取到所有状态的TCP连接，再统计每个状态的连接数量。 - 采集方式（Windows）：通过WindowsAPI GetTcpTable2获取。	≥ 0	Count	不涉及	云服务器	1分钟
net_tcp_time_wait	(Agent) TCP TIME_WAIT	该指标用于统计测量对象处于TIME_WAIT状态的TCP连接数量。 - 采集方式（Linux）：通过/proc/net/tcp文件获取到所有状态的TCP连接，再统计每个状态的连接数量。 - 采集方式（Windows）：通过WindowsAPI GetTcpTable2获取。	≥ 0	Count	不涉及	云服务器	1分钟

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
net_tcp_close	(Agent) TCP CLOSE	该指标用于统计测量对象关闭的或未打开的 TCP 连接数量。 - 采集方式（Linux）：通过 /proc/net/tcp 文件获取到所有状态的 TCP 连接，再统计每个状态的连接数量。 - 采集方式（Windows）：通过 Windows API GetTcpTable2 获取。	≥ 0	Count	不涉及	云服务器	1分钟
net_tcp_close_wait	(Agent) TCP CLOSE_WAIT	该指标用于统计测量对象处于 CLOSE_WAIT 状态的 TCP 连接数量。 - 采集方式（Linux）：通过 /proc/net/tcp 文件获取到所有状态的 TCP 连接，再统计每个状态的连接数量。 - 采集方式（Windows）：通过 Windows API GetTcpTable2 获取。	≥ 0	Count	不涉及	云服务器	1分钟
net_tcp_last_ack	(Agent) TCP LAST_ACK	该指标用于统计测量对象被动关闭等待 ACK 报文的 TCP 连接数量。 - 采集方式（Linux）：通过 /proc/net/tcp 文件获取到所有状态的 TCP 连接，再统计每个状态的连接数量。 - 采集方式（Windows）：通过 Windows API GetTcpTable2 获取。	≥ 0	Count	不涉及	云服务器	1分钟

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
net_tcp_listen	(Agent) TCP LISTEN	该指标用于统计测量对象处于LISTEN状态的TCP连接数量。 - 采集方式（Linux）：通过/proc/net/tcp文件获取到所有状态的TCP连接，再统计每个状态的连接数量。 - 采集方式（Windows）：通过WindowsAPI GetTcpTable2获取。	≥ 0	Count	不涉及	云服务器	1分钟
net_tcp_closing	(Agent) TCP CLOSING	该指标用于统计测量对象处于服务端和客户端同时主动关闭状态的TCP连接数量。 - 采集方式（Linux）：通过/proc/net/tcp文件获取到所有状态的TCP连接，再统计每个状态的连接数量。 - 采集方式（Windows）：通过WindowsAPI GetTcpTable2获取。	≥ 0	Count	不涉及	云服务器	1分钟
net_tcp_retrans	(Agent) TCP重传率	该指标用于统计测量对象重新发送的报文数与总发送的报文数之间的比值。 - 采集方式（Linux）：通过从/proc/net/snmp文件中获取对应的数据，计算采集周期内发送包数和重传包数的比值得出。 - 采集方式（Windows）：重传率通过WindowsAPI GetTcpStatistics获取	0-100	%	不涉及	云服务器	1分钟

操作系统监控指标：GPU

表 17-12 GPU 类监控指标说明

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
gpu_status	(Agent) gpu健康状态	该指标用于统计虚拟机上GPU健康状态，是一个综合指标。 - 采集方式（Linux）：通过调用GPU卡的libnvidia-ml.so.1库文件获取。 - 采集方式（Windows）：通过调用GPU卡的nvml.dll库获取。	0：代表健康 1：代表亚健康 2：代表故障	不涉及	不涉及	- 云服务器 - 云服务器 - GPU	1分钟
gpu_usage_encoder	(Agent) 编码使用率	该指标用于统计该GPU的编码能力使用率。 - 采集方式（Linux）：通过调用GPU卡的libnvidia-ml.so.1库文件获取。 - 采集方式（Windows）：通过调用GPU卡的nvml.dll库获取。	0-100	%	不涉及	- 云服务器 - 云服务器 - GPU	1分钟

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
gpu_usage_decoder	(Agent) 解码使用率	该指标用于统计该GPU的解码能力使用率。 - 采集方式（Linux）：通过调用GPU卡的libnvidia-ml.so.1库文件获取。 - 采集方式（Windows）：通过调用GPU卡的nvml.dll库获取。	0-100	%	不涉及	- 云服务器 - 云服务器 - GPU	1分钟
gpu_volatile_correctable	(Agent) 可纠正ECC错误数量	该指标用于统计该GPU重置以来可纠正的ECC错误数量，每次重置后归0。 - 采集方式（Linux）：通过调用GPU卡的libnvidia-ml.so.1库文件获取。 - 采集方式（Windows）：通过调用GPU卡的nvml.dll库获取。	≥ 0	count	不涉及	- 云服务器 - 云服务器 - GPU	1分钟
gpu_volatile_uncorrectable	(Agent) 不可纠正ECC错误数量	该指标用于统计该GPU重置以来不可纠正的ECC错误数量，每次重置后归0。 - 采集方式（Linux）：通过调用GPU卡的libnvidia-ml.so.1库文件获取。 - 采集方式（Windows）：通过调用GPU卡的nvml.dll库获取。	≥ 0	count	不涉及	- 云服务器 - 云服务器 - GPU	1分钟

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
gpu_aggregate_correctable	(Agent) 累计可纠正 ECC 错误数量	该指标用于统计该 GPU 累计的可纠正 ECC 错误数量。 - 采集方式（Linux）：通过调用 GPU 卡的 libnvidia-ml.so.1 库文件获取。 - 采集方式（Windows）：通过调用 GPU 卡的 nvml.dll 库获取。	≥ 0	count	不涉及	- 云服务器 - 云服务器 - GPU	1 分钟
gpu_aggregate_uncorrectable	(Agent) 累计不可纠正 ECC 错误数量	该指标用于统计该 GPU 累计的不可纠正 ECC 错误数量。 - 采集方式（Linux）：通过调用 GPU 卡的 libnvidia-ml.so.1 库文件获取。 - 采集方式（Windows）：通过调用 GPU 卡的 nvml.dll 库获取。	≥ 0	count	不涉及	- 云服务器 - 云服务器 - GPU	1 分钟
gpu_retired_page_single_bit	(Agent) retired page single bit 错误数量	该指标用于统计该 GPU 当前卡隔离的单比特页的数量。 - 采集方式（Linux）：通过调用 GPU 卡的 libnvidia-ml.so.1 库文件获取。 - 采集方式（Windows）：通过调用 GPU 卡的 nvml.dll 库获取。	≥ 0	count	不涉及	- 云服务器 - 云服务器 - GPU	1 分钟

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
gpu_retired_page_double_bit	(Agent) retired page double bit错误数量	该指标用于统计该GPU当前卡隔离的双比特页的数量。 - 采集方式（Linux）：通过调用GPU卡的libnvidia-ml.so.1库文件获取。 - 采集方式（Windows）：通过调用GPU卡的nvml.dll库获取。	≥ 0	count	不涉及	- 云服务器 - 云服务器 - GPU	1分钟
gpu_performance_state	(Agent) 性能状态	该指标用于统计该GPU的性能状态。 - 采集方式（Linux）：通过调用GPU卡的libnvidia-ml.so.1库文件获取。 - 采集方式（Windows）：通过调用GPU卡的nvml.dll库获取。	P0-P15、P32, - P0：表示最大性能状态 - P15：表示最小性能状态 - P32：表示状态未知	不涉及	不涉及	- 云服务器 - 云服务器 - GPU	1分钟

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
gpu_usage_mem	(Agent) 显存使用率	该指标用于统计该GPU的显存使用率。 - 采集方式（Linux）：通过调用GPU卡的libnvidia-ml.so.1库文件获取。 - 采集方式（Windows）：通过调用GPU卡的nvml.dll库获取。	0-100	%	不涉及	- 云服务器 - 云服务器 - GPU	1分钟
gpu_usage_gpu	(Agent) GPU使用率	该指标用于统计该GPU的算力使用率。 - 采集方式（Linux）：通过调用GPU卡的libnvidia-ml.so.1库文件获取。 - 采集方式（Windows）：通过调用GPU卡的nvml.dll库获取。	0-100	%	不涉及	- 云服务器 - 云服务器 - GPU	1分钟
gpu_free_mem	(Agent) GPU显存剩余量	该指标用于统计该GPU的显存剩余量。 - 采集方式（Linux）：通过调用GPU卡的libnvidia-ml.so.1库文件获取。 - 采集方式（Windows）：通过调用GPU卡的nvml.dll库获取。	≥ 0	MB	不涉及	- 云服务器 - 云服务器 - GPU	1分钟

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
gpu_graphics_clocks	(Agent) GPU显卡时钟频率	该指标用于统计该GPU的显卡（着色器）时钟频率。 - 采集方式（Linux）：通过调用GPU卡的libnvidia-ml.so.1库文件获取。 - 采集方式（Windows）：通过调用GPU卡的nvml.dll库获取。	≥ 0	MHz	不涉及	- 云服务器 - 云服务器 - GPU	1分钟
gpu_memory_clocks	(Agent) GPU内存时钟频率	该指标用于统计该GPU的内存时钟频率。 - 采集方式（Linux）：通过调用GPU卡的libnvidia-ml.so.1库文件获取。 - 采集方式（Windows）：通过调用GPU卡的nvml.dll库获取。	≥ 0	MHz	不涉及	- 云服务器 - 云服务器 - GPU	1分钟
gpu_power_draw	(Agent) GPU功率	该指标用于统计该GPU的功率。 - 采集方式（Linux）：通过调用GPU卡的libnvidia-ml.so.1库文件获取。 - 采集方式（Windows）：通过调用GPU卡的nvml.dll库获取。	NA	W	不涉及	- 云服务器 - 云服务器 - GPU	1分钟

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
gpu_rx_throughput_pci	(Agent) GPU PCI入方向流量	该指标用于统计该GPU的PCI入方向流量。 - 采集方式（Linux）：通过调用GPU卡的libnvidia-ml.so.1库文件获取。 - 采集方式（Windows）：通过调用GPU卡的nvml.dll库获取。	≥ 0	MB/s	不涉及	- 云服务器 - 云服务器 - GPU	1分钟
gpu_sm_clocks	(Agent) GPU流式处理器时钟频率	该指标用于统计该GPU的流式处理器时钟频率。 - 采集方式（Linux）：通过调用GPU卡的libnvidia-ml.so.1库文件获取。 - 采集方式（Windows）：通过调用GPU卡的nvml.dll库获取。	≥ 0	MHz	不涉及	- 云服务器 - 云服务器 - GPU	1分钟
gpu_temperature	(Agent) GPU温度	该指标用于统计该GPU的温度。 - 采集方式（Linux）：通过调用GPU卡的libnvidia-ml.so.1库文件获取。 - 采集方式（Windows）：通过调用GPU卡的nvml.dll库获取。	≥ 0	℃	不涉及	- 云服务器 - 云服务器 - GPU	1分钟

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
gpu_tx_throughput_pci	(Agent) GPU PCI出方向流量	该指标用于统计该GPU的PCI出方向带宽。 - 采集方式（Linux）：通过调用GPU卡的libnvidia-ml.so.1库文件获取。 - 采集方式（Windows）：通过调用GPU卡的nvml.dll库获取。	≥ 0	MB/s	不涉及	- 云服务器 - 云服务器 - GPU	1分钟
gpu_used_mem	(Agent) GPU显存使用量	该指标用于统计该GPU的显存使用量。 - 采集方式（Linux）：通过调用GPU卡的libnvidia-ml.so.1库文件获取。 - 采集方式（Windows）：通过调用GPU卡的nvml.dll库获取。	≥ 0	MB	不涉及	- 云服务器 - 云服务器 - GPU	1分钟
gpu_video_clocks	(Agent) GPU视频时钟频率	该指标用于统计该GPU的视频（包含编解码）时钟频率。 - 采集方式（Linux）：通过调用GPU卡的libnvidia-ml.so.1库文件获取。 - 采集方式（Windows）：通过调用GPU卡的nvml.dll库获取。	≥ 0	MHz	不涉及	- 云服务器 - 云服务器 - GPU	1分钟

操作系统监控指标：NPU

表 17-13 NPU 类监控指标说明

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
npu_device_health	(Agent) NPU健康状况	该指标用于统计虚拟机上NPU卡的健康状态，是一个综合指标。 采集方式（Linux）：通过调用NPU卡的libdcmi.so库文件获取。	0: 代表健康 1: 代表存在一般告警 2: 代表存在重要告警 3: 代表存在紧急告警	不涉及	不涉及	- 云服务器 - 云服务器 - NPU	1分钟

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
npu_util_rate_mem	(Agent) NPU显存使用率	该指标用于统计该NPU的显存使用率。 采集方式（Linux）：通过调用NPU卡的libdcmi.so库文件获取。	0-100	%	不涉及	- 云服务器 - 云服务器 - NPU	1分钟
npu_util_rate_ai_core	(Agent) NPU卡AI核心使用率	该指标用于统计该NPU的AI核心使用率。 采集方式（Linux）：通过调用NPU卡的libdcmi.so库文件获取。	0-100	%	不涉及	- 云服务器 - 云服务器 - NPU	1分钟
npu_util_rate_ai_cpu	(Agent) NPU卡AI CPU使用率	该指标用于统计该NPU的AI CPU的使用率。 采集方式（Linux）：通过调用NPU卡的libdcmi.so库文件获取。	0-100	%	不涉及	- 云服务器 - 云服务器 - NPU	1分钟

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
npu_util_rate_cpu	(Agent) NPU控制CPU使用率	该指标用于统计该NPU的控制CPU的使用率。 采集方式（Linux）：通过调用NPU卡的libdcmi.so库文件获取。	0-100	%	不涉及	- 云服务器 - 云服务器 - NPU	1分钟
npu_util_rate_mem_bandwidth	(Agent) NPU显存带宽使用率	该指标用于统计该NPU的显存的带宽使用率。 采集方式（Linux）：通过调用NPU卡的libdcmi.so库文件获取。	0-100	%	不涉及	- 云服务器 - 云服务器 - NPU	1分钟
npu_frequency_mem	(Agent) NPU显存频率	该指标用于统计该NPU的显存的时钟频率。 采集方式（Linux）：通过调用NPU卡的libdcmi.so库文件获取。	≥ 0	MHz	不涉及	- 云服务器 - 云服务器 - NPU	1分钟

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
npu_freq_ai_core	(Agent) NPU卡AI核心频率	该指标用于统计该NPU AI核心的时钟频率。 采集方式（Linux）：通过调用NPU卡的libdcmi.so库文件获取。	≥ 0	MHz	不涉及	- 云服务器 - 云服务器 - NPU	1分钟
npu_usage_mem	(Agent) NPU显存使用量	该指标用于统计该NPU显存的使用量。 采集方式（Linux）：通过调用NPU卡的libdcmi.so库文件获取。	≥ 0	MB	不涉及	- 云服务器 - 云服务器 - NPU	1分钟
npu_sbe	(Agent) NPU单bit错误数量	该指标用于统计该NPU卡当前的单比特页错误的数量。 采集方式（Linux）：通过调用NPU卡的libdcmi.so库文件获取。	≥ 0	count	不涉及	- 云服务器 - 云服务器 - NPU	1分钟

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
npu_dbe	(Agent) NPU双bit错误数量	该指标用于统计该NPU卡当前的多比特页错误的数量。 采集方式（Linux）：通过调用NPU卡的libdcmi.so库文件获取。	≥ 0	count	不涉及	- 云服务器 - 云服务器 - NPU	1分钟
npu_power	(Agent) NPU功率	该指标用于统计该NPU卡的功率。其中，310卡仅支持显示额定功率，其余卡显示实际功率 采集方式（Linux）：通过调用NPU卡的libdcmi.so库文件获取。	≥ 0	W	不涉及	- 云服务器 - 云服务器 - NPU	1分钟
npu_temperature	(Agent) NPU温度	该指标用于统计该NPU卡当前的温度 采集方式（Linux）：通过调用NPU卡的libdcmi.so库文件获取。	≥ 0	℃	不涉及	- 云服务器 - 云服务器 - NPU	1分钟

 **说明**

Windows系统暂不支持NPU类监控指标。

操作系统监控指标：DAVP

表 17-14 DAVP 类监控指标说明

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
davp_device_health	(Agent) DAVP健康状态	该指标用于统计虚拟机上DAVP卡的健康状态，是一个综合指标。 采集方式（Linux）：通过调用DAVP卡的vatoools工具下的libvaml.so库文件获取。	0：代表健康 1：代表异常	不涉及	不涉及	- 云服务器 - 云服务器 - DAVP	1分钟
davp_util_rate_mem	(Agent) DAVP显存使用率	该指标用于统计该DAVP卡的显存使用率。 采集方式（Linux）：通过调用DAVP卡的vatoools工具下的libvaml.so库文件获取。	0-100	%	不涉及	- 云服务器 - 云服务器 - DAVP	1分钟
davp_usage_mem	(Agent) DAVP显存使用量	该指标用于统计该DAVP卡的显存使用量 采集方式（Linux）：通过调用DAVP卡的vatoools工具下的libvaml.so库文件获取。	≥ 0	MB	不涉及	- 云服务器 - 云服务器 - DAVP	1分钟

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
davp_util_rate_ai_core	(Agent) DAVP卡AI核心使用率	该指标用于统计该DAVP卡的AI核心的使用率。 采集方式（Linux）：通过调用DAVP卡的vatoools工具下的libvaml.so库文件获取。	0-100	%	不涉及	- 云服务器 - 云服务器 - DAVP	1分钟
davp_util_rate_vdsp_core	(Agent) DAVP卡vdsp核心使用率	该指标用于统计该DAVP卡的vdsp核心使用率。 采集方式（Linux）：通过调用DAVP卡的vatoools工具下的libvaml.so库文件获取。	0-100	%	不涉及	- 云服务器 - 云服务器 - DAVP	1分钟
davp_util_rate_enc_core	(Agent) DAVP卡编码核心使用率	该指标用于统计该DAVP的编码核心使用率。 采集方式（Linux）：通过调用DAVP卡的vatoools工具下的libvaml.so库文件获取。	0-100	%	不涉及	- 云服务器 - 云服务器 - DAVP	1分钟

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
davp_util_rate_dec_core	(Agent) DAVP卡解码核心使用率	该指标用于统计该 DAVP卡的解码核心使用率。 采集方式（Linux）：通过调用DAVP卡的vatoools工具下的libvaml.so库文件获取。	0-100	%	不涉及	- 云服务器 - 云服务器 - DAVP	1分钟
davp_sysc_temperature	(Agent) DAVP卡系统模块温度	该指标用于统计该 DAVP卡的系统模块温度。 采集方式（Linux）：通过调用DAVP卡的vatoools工具下的libvaml.so库文件获取。	≥ 0	℃	不涉及	- 云服务器 - 云服务器 - DAVP	1分钟

 **说明**

Windows系统暂不支持DAVP类监控指标。

维度

维度	Key	Value
云服务器	instance_id	云服务器ID。
云服务器 - 磁盘	disk	云服务器磁盘。 该取值可通过云监控服务的“ 查询主机监控维度指标信息 ”获取。

维度	Key	Value
云服务器 - 挂载点	mount_point	云服务器磁盘的挂载点。 该取值可通过云监控服务的“ 查询主机监控维度指标信息 ”获取。
云服务器 - GPU	gpu	GPU类型云服务器中显卡。 该取值可通过云监控服务的“ 查询主机监控维度指标信息 ”获取。
云服务器 - NPU	npu	NPU类型云服务器中显卡。 该取值可通过云监控服务的“ 查询主机监控维度指标信息 ”获取。
云服务器 - DAVP	davp	DAVP类型云服务器，其中搭载了DaoCloud DAVP1 视频加速卡。 该取值可通过云监控服务的“ 查询主机监控维度指标信息 ”获取。

17.4 弹性云服务器支持的进程监控指标（安装 Agent）

功能说明

通过在弹性云服务器中安装Agent插件，可以对主机内的活跃进程进行监控，默认采集活跃进程消耗的CPU、内存，以及打开的文件数量等信息。

本节定义了弹性云服务器上报云监控的进程监控指标。

命名空间

AGT.ECS

进程监控指标说明

对于不同的操作系统、不同的弹性云服务器类型，在安装Agent后均默认支持查看以下进程监控指标。

表 17-15 进程监控指标说明

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
proc_pHashId_cpu	(Agent) 进程 CPU 使用率	进程消耗的CPU百分比，pHashId是（进程名+进程ID）的md5值。 - 采集方式（Linux）：通过计算/proc/pid/stat的变化得出。 - 采集方式（Windows）：通过Windows API GetProcessTimes获取进程CPU使用率。	0-1*CPU核心数	%	不涉及	云服务器	1分钟
proc_pHashId_mem	(Agent) 进程内存使用率	进程消耗的内存百分比，pHashId是（进程名+进程ID）的md5值。 - 采集方式（Linux）：RSS*PAGESIZE/MemTotal RSS: 通过获取/proc/pid/statm第二列得到 PAGESIZE: 通过命令getconf PAGESIZE获取 MemTotal: 通过/proc/meminfo获取 - 采集方式（Windows）：使用Windows API procGlobalMemoryStatusEx获取内存总量，通过GetProcessMemoryInfo获取内存已使用量，计算两者比值得到内存使用率。	0-100	%	不涉及	云服务器	1分钟

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
proc_pHashId_file	(Agent) 进程打开文件数	进程打开文件数，pHashId是（进程名+进程ID）的md5值。 - 采集方式（Linux）：通过执行ls -l /proc/pid/fd可以查看数量。 - 采集方式（Windows）：暂不支持。	≥0	Count	不涉及	云服务器	1分钟
proc_running_count	(Agent) 运行中进程数	该指标用于统计测量对象处于运行状态的进程数。 - 采集方式（Linux）：通过统计 /proc/pid/status 中Status值获取每个进程的状态，进而统计各个状态进程总数。 - 采集方式（Windows）：暂不支持。	≥0	Count	不涉及	云服务器	1分钟
proc_idle_count	(Agent) 空闲进程数	该指标用于统计测量对象处于空闲状态的进程数。 - 采集方式（Linux）：通过统计 /proc/pid/status 中Status值获取每个进程的状态，进而统计各个状态进程总数。 - 采集方式（Windows）：暂不支持。	≥0	Count	不涉及	云服务器	1分钟

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
proc_zombie_count	(Agent) 僵死进程数	该指标用于统计测量对象处于僵死状态的进程数。 - 采集方式（Linux）：通过统计 /proc/pid/status 中Status值获取每个进程的状态，进而统计各个状态进程总数。 - 采集方式（Windows）：暂不支持。	≥0	Count	不涉及	云服务器	1分钟
proc_blocked_count	(Agent) 阻塞进程数	该指标用于统计测量对象被阻塞的进程数。 - 采集方式（Linux）：通过统计 /proc/pid/status 中Status值获取每个进程的状态，进而统计各个状态进程总数。 - 采集方式（Windows）：暂不支持。	≥0	Count	不涉及	云服务器	1分钟
proc_sleeping_count	(Agent) 睡眠进程数	该指标用于统计测量对象处于睡眠状态的进程数。 - 采集方式（Linux）：通过统计 /proc/pid/status 中Status值获取每个进程的状态，进而统计各个状态进程总数。 - 采集方式（Windows）：暂不支持。	≥0	Count	不涉及	云服务器	1分钟

指标	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
proc_total_count	(Agent) 系统进程数	该指标用于统计测量对象的总进程数。 - 采集方式（Linux）：通过统计 /proc/pid/status 中Status值获取每个进程的状态，进而统计各个状态进程总数。 - 采集方式（Windows）：通过psapi.dll系统进程状态支持模块得到进程总数。	≥0	Count	不涉及	云服务器	1分钟
proc_specified_count	(Agent) 指定进程数	该指标用于统计测量对象指定的进程数。 - 采集方式（Linux）：通过统计 /proc/pid/status 中Status值获取每个进程的状态，进而统计各个状态进程总数。 - 采集方式（Windows）：通过psapi.dll系统进程状态支持模块得到进程总数。	≥0	Count	不涉及	- 云服务器 - 云服务器 - 进程	1分钟
specified_process_file	(Agent) 指定进程打开文件数	该指标用于统计测量对象指定进程打开的文件数。 - 采集方式（Linux）：通过执行ls -l /proc/pid/fd 可以查看数量。 - 采集方式（Windows）：暂不支持。	≥0	Count	不涉及	- 云服务器 - 云服务器 - 进程	1分钟

维度

维度	Key	Value
云服务器	instance_id	云服务器ID。
云服务器 - 进程	proc	云服务器的进程。 该取值可通过云监控服务的“ 查询主机监控维度指标信息 ”获取。

17.5 异构类实例安装支持对应监控的 CES Agent（Linux）

操作场景

监控与告警是保证异构云服务器（GPU加速型实例、AI加速型实例）高可靠性、高可用性和高性能的重要功能。

通过在异构类（例如，GPU加速型实例、AI加速型实例）的Linux实例上安装支持对应监控的CES Agent，可以为用户提供系统级、主动式、细颗粒度的监控，包含相关异构指标收集和系统事件上报。

当前支持的异构加速卡及对应的监控指标种类如下：

- GPU监控指标，请参见[操作系统监控指标：GPU](#)。
- NPU监控指标，请参见[操作系统监控指标：NPU](#)。

本章节介绍如何通过安装脚本为异构（GPU加速型、AI加速型）实例安装支持对应监控的CES Agent：

- [操作步骤（单台ECS安装）](#)
- [操作步骤（多台ECS批量安装）](#)

约束与限制

- 仅支持Linux操作系统。
- 使用私有镜像创建的云服务器需手动安装监控组件并[安装驱动](#)。
- 对于GPU监控：
 - 支持GPU监控的Linux公共镜像如[表17-16](#)所示。

表 17-16 支持 GPU 监控的 Linux 版本

类型	版本
CentOS（64bit）	7.6、7.9、8.2
Ubuntu（64bit）	16.04、18.04、20.04
Huawei Cloud Euler（64bit）	2.0

- 支持GPU监控的规格：G6v、G6、P2s、P2v、P2vs、G5、Pi2、Pi1、P1。
- 对于NPU监控：
 - 支持NPU监控的Linux公共镜像如所表17-17示。

表 17-17 支持 NPU 监控的 Linux 版本

类型	版本
CentOS (64bit)	• 7.6: Ai1s、Ai2、Kai1s、Kai2 • 7.7-7.9: Ai2、Kai2
Ubuntu (64bit)	18.04

- 支持NPU监控的规格：Ai1s, Ai2, Kai1s, Kai2。

前提条件

- 已配置DNS和安全组，配置方法参考[如何配置DNS和安全组？](#)。
- 已配置委托，配置方法参考[如何配置委托？](#)。
- 实例已安装对应驱动。
 - GPU加速型实例：已安装GPU驱动。
未安装GPU驱动的云服务器不支持采集GPU指标数据及上报事件。
如果您的弹性云服务器未安装GPU驱动，可参见（[推荐](#)）[自动安装GPU加速型ECS的GPU驱动（Linux）](#)。
 - AI加速型实例：已安装NPU驱动
未安装NPU驱动的云服务器不支持采集NPU指标数据及上报事件。
使用公共镜像创建的AI加速型实例默认已安装特定版本驱动，如果您使用私有镜像创建AI加速型实例，或者因其他原因需要安装驱动，请参考[昇腾文档中心](#)对应版本的《CANN软件安装指南》。

说明

- 安装驱动需使用默认路径。
驱动安装完后，需重启实例，否则可能导致采集指标及上报事件失败。
- 驱动正常安装后，最多10分钟将在控制台看到采集到的指标数据。
- 已安装lspci工具，未安装lspci工具的云服务器影响GPU掉卡事件的上报。
安装lspci工具的方法，请参见（[可选](#)）[安装lspci工具](#)。
- 确保云服务器的安装目录都有读写权限，并且安装成功后的Telescope进程不会被其他软件关闭。

操作步骤（单台 ECS 安装）

本操作以Ubuntu 18.04 64bit操作系统、Pi2规格的GPU加速型实例为例，介绍单台ECS安装支持GPU监控的CES Agent的操作指导。

1. 使用root用户，[远程登录](#)弹性云服务器。
2. 执行以下命令，为单台ECS安装支持GPU监控的CES Agent。
以“华北-北京四”为例，其余区域的安装脚本，请参见[获取安装脚本](#)。


```
cd /usr/local && curl -k -O https://uniagent-cn-north-4.obs.cn-north-4.myhuaweicloud.com/package/agent_install.sh && bash agent_install.sh -r cn-north-4 -u 0.1.5 -t 2.7.5.1 -d agent.ces.myhuaweicloud.com
```

其中，“cn-north-4”表示区域ID，“0.1.5”是uniagent版本号，“2.7.5.1”是telescope版本号。

当显示如下内容，表示支持GPU监控的CES Agent安装成功。

图 17-1 支持 GPU 监控的 CES Agent 安装成功

```
telescope_linux_amd64/  
telescope_linux_amd64/uninstall.sh  
telescope_linux_amd64/install.sh  
telescope_linux_amd64/bin/  
telescope_linux_amd64/bin/conf.json  
telescope_linux_amd64/bin/telescope  
telescope_linux_amd64/bin/conf_ces.json  
telescope_linux_amd64/bin/conf_lts.json  
telescope_linux_amd64/bin/record.json  
telescope_linux_amd64/bin/logs_config.xml  
telescope_linux_amd64/bin/agent  
telescope_linux_amd64/telescoped  
telescope_linux_amd64/telescope-1.0.12-release.json  
Current user is root.  
Current linux release version : CENTOS  
Start to install telescope...  
In chkconfig  
Success to install telescope to dir: /usr/local/telescope.  
Starting telescope...  
Telescope process starts successfully.  
[root@ecs-74e5-7 local]#
```

操作步骤（多台 ECS 批量安装）

本操作以Ubuntu 18.04 64bit操作系统、Pi2规格的GPU加速型实例为例，介绍多台ECS批量安装支持GPU监控的CES Agent的操作指导。

须知

批量安装的多台ECS需要归属于同一个VPC。

1. 使用root用户，[远程登录](#)其中一台弹性云服务器。
2. 执行以下命令，为这一台ECS安装支持GPU监控的CES Agent。
以“华北-北京四”为例，其余区域的安装脚本，请参见[获取安装脚本](#)。

```
cd /usr/local && curl -k -O https://uniagent-cn-north-4.obs.cn-north-4.myhuaweicloud.com/package/agent_install.sh && bash agent_install.sh -r cn-north-4 -u 0.1.5 -t 2.7.5.1 -d agent.ces.myhuaweicloud.com
```

其中，“cn-north-4”表示区域ID，“0.1.5”是uniagent版本号，“2.7.5.1”是telescope版本号。

当支持GPU监控的CES Agent安装成功，且数据采集正常时，可以将此ECS作为跳板机，通过批量安装脚本依次为其他ECS批量安装支持GPU监控的CES Agent。

3. 收集需要批量安装支持GPU监控的CES Agent的所有ECS的IP地址和root用户密码，以iplist.txt格式整理，并上传到ECS跳板机的/usr/local目录下。

iplist.txt格式为“IP地址,root用户密码”，每个记录一行。

示例如下所示（示例中abcd为root用户密码，请按实际值填写）：

```
192.168.1.1,abcd
192.168.1.2,abcd
```

4. 执行以下命令，为多台ECS批量安装支持GPU监控的CES Agent。

以“华北-北京四”为例，其余区域的批量安装脚本，请参见[获取安装脚本](#)。

```
cd /usr/local && curl -k -O https://uniagent-cn-north-4.obs.cn-
north-4.myhuaweicloud.com/package/batch_agent_install.sh && bash
batch_agent_install.sh -r cn-north-4 -u 0.1.5 -t 2.7.5.1 -d
agent.ces.myhuaweicloud.com
```

其中，cn-north-4是RegionID，0.1.5是uniagent版本号，2.7.5.1是telescope版本号。

当显示如下内容，表示支持GPU监控的CES Agent安装成功。

图 17-2 支持 GPU 监控的 CES Agent 安装成功

```
telescope_linux_amd64/
telescope_linux_amd64/uninstall.sh
telescope_linux_amd64/install.sh
telescope_linux_amd64/bin/
telescope_linux_amd64/bin/conf.json
telescope_linux_amd64/bin/telescope
telescope_linux_amd64/bin/conf_ces.json
telescope_linux_amd64/bin/conf_lts.json
telescope_linux_amd64/bin/record.json
telescope_linux_amd64/bin/logs_config.xml
telescope_linux_amd64/bin/agent
telescope_linux_amd64/telescoped
telescope_linux_amd64/telescope-1.0.12-release.json
Current user is root.
Current linux release version : CENTOS
Start to install telescope...
In chkconfig
Success to install telescope to dir: /usr/local/telescope.
Starting telescope...
Telescope process starts successfully.
[root@ecs-74e5-7 local]#
```

获取安装脚本

您可以通过执行以下命令，获取支持GPU监控和NPU监控的CES Agent的安装脚本。

表 17-18 安装脚本的支持区域及获取方式

区域	安装脚本
华北-北京一	单台ECS安装: cd /usr/local && curl -k -O https://uniagent-cn-north-1.obs.cn-north-1.myhuaweicloud.com/package/agent_install.sh && bash agent_install.sh -r cn-north-1 -u 0.1.5 -t 2.7.5.1 -d agent.ces.myhuaweicloud.com 多台ECS批量安装: cd /usr/local && curl -k -O https://uniagent-cn-north-1.obs.cn-north-1.myhuaweicloud.com/package/batch_agent_install.sh && bash batch_agent_install.sh -r cn-north-1 -u 0.1.5 -t 2.7.5.1 -d agent.ces.myhuaweicloud.com
华北-北京四	单台ECS安装: cd /usr/local && curl -k -O https://uniagent-cn-north-4.obs.cn-north-4.myhuaweicloud.com/package/agent_install.sh && bash agent_install.sh -r cn-north-4 -u 0.1.5 -t 2.7.5.1 -d agent.ces.myhuaweicloud.com 多台ECS批量安装: cd /usr/local && curl -k -O https://uniagent-cn-north-4.obs.cn-north-4.myhuaweicloud.com/package/batch_agent_install.sh && bash batch_agent_install.sh -r cn-north-4 -u 0.1.5 -t 2.7.5.1 -d agent.ces.myhuaweicloud.com
华北-乌兰察布一	单台ECS安装: cd /usr/local && curl -k -O https://obs.cn-north-9.myhuaweicloud.com/uniagent-cn-north-9/package/agent_install.sh && bash agent_install.sh -r cn-north-9 -u 0.1.5 -t 2.7.5.1 -d agent.ces.myhuaweicloud.com 多台ECS批量安装: cd /usr/local && curl -k -O https://obs.cn-north-9.myhuaweicloud.com/uniagent-cn-north-9/package/batch_agent_install.sh && bash batch_agent_install.sh -r cn-north-9 -u 0.1.5 -t 2.7.5.1 -d agent.ces.myhuaweicloud.com
华南-广州	单台ECS安装: cd /usr/local && curl -k -O https://uniagent-cn-south-1.obs.cn-south-1.myhuaweicloud.com/package/agent_install.sh && bash agent_install.sh -r cn-south-1 -u 0.1.5 -t 2.7.5.1 -d agent.ces.myhuaweicloud.com 多台ECS批量安装: cd /usr/local && curl -k -O https://uniagent-cn-south-1.obs.cn-south-1.myhuaweicloud.com/package/batch_agent_install.sh && bash batch_agent_install.sh -r cn-south-1 -u 0.1.5 -t 2.7.5.1 -d agent.ces.myhuaweicloud.com
华东-上海一	单台ECS安装: cd /usr/local && curl -k -O https://uniagent-cn-east-3.obs.cn-east-3.myhuaweicloud.com/package/agent_install.sh && bash agent_install.sh -r cn-east-3 -u 0.1.5 -t 2.7.5.1 -d agent.ces.myhuaweicloud.com 多台ECS批量安装: cd /usr/local && curl -k -O https://uniagent-cn-east-3.obs.cn-east-3.myhuaweicloud.com/package/batch_agent_install.sh && bash batch_agent_install.sh -r cn-east-3 -u 0.1.5 -t 2.7.5.1 -d agent.ces.myhuaweicloud.com
华东-上海二	单台ECS安装: cd /usr/local && curl -k -O https://uniagent-cn-east-2.obs.cn-east-2.myhuaweicloud.com/package/agent_install.sh && bash agent_install.sh -r cn-east-2 -u 0.1.5 -t 2.7.5.1 -d agent.ces.myhuaweicloud.com 多台ECS批量安装: cd /usr/local && curl -k -O https://uniagent-cn-east-2.obs.cn-east-2.myhuaweicloud.com/package/batch_agent_install.sh && bash batch_agent_install.sh -r cn-east-2 -u 0.1.5 -t 2.7.5.1 -d agent.ces.myhuaweicloud.com

区域	安装脚本
西南-贵阳 —	单台ECS安装: cd /usr/local && curl -k -O https://uniagent-cn-southwest-2.obs.cn-southwest-2.myhuaweicloud.com/package/agent_install.sh && bash agent_install.sh -r cn-southwest-2 -u 0.1.5 -t 2.7.5.1 -d agent.ces.myhuaweicloud.com 多台ECS批量安装: cd /usr/local && curl -k -O https://uniagent-cn-southwest-2.obs.cn-southwest-2.myhuaweicloud.com/package/batch_agent_install.sh && bash batch_agent_install.sh -r cn-southwest-2 -u 0.1.5 -t 2.7.5.1 -d agent.ces.myhuaweicloud.com
中国-香港	单台ECS安装: cd /usr/local && curl -k -O https://uniagent-ap-southeast-1.obs.ap-southeast-1.myhuaweicloud.com/package/agent_install.sh && bash agent_install.sh -r ap-southeast-1 -u 0.1.5 -t 2.7.5.1 -d agent.ces.myhuaweicloud.com 多台ECS批量安装: cd /usr/local && curl -k -O https://uniagent-ap-southeast-1.obs.ap-southeast-1.myhuaweicloud.com/package/batch_agent_install.sh && bash batch_agent_install.sh -r ap-southeast-1 -u 0.1.5 -t 2.7.5.1 -d agent.ces.myhuaweicloud.com
亚太-曼谷	单台ECS安装: cd /usr/local && curl -k -O https://uniagent-ap-southeast-2.obs.ap-southeast-2.myhuaweicloud.com/package/agent_install.sh && bash agent_install.sh -r ap-southeast-2 -u 0.1.5 -t 2.7.5.1 -d agent.ces.myhuaweicloud.com 多台ECS批量安装: cd /usr/local && curl -k -O https://uniagent-ap-southeast-2.obs.ap-southeast-2.myhuaweicloud.com/package/batch_agent_install.sh && bash batch_agent_install.sh -r ap-southeast-2 -u 0.1.5 -t 2.7.5.1 -d agent.ces.myhuaweicloud.com
亚太-新加坡	单台ECS安装: cd /usr/local && curl -k -O https://uniagent-ap-southeast-3.obs.ap-southeast-3.myhuaweicloud.com/package/agent_install.sh && bash agent_install.sh -r ap-southeast-3 -u 0.1.5 -t 2.7.5.1 -d agent.ces.myhuaweicloud.com 多台ECS批量安装: cd /usr/local && curl -k -O https://uniagent-ap-southeast-3.obs.ap-southeast-3.myhuaweicloud.com/package/batch_agent_install.sh && bash batch_agent_install.sh -r ap-southeast-3 -u 0.1.5 -t 2.7.5.1 -d agent.ces.myhuaweicloud.com
亚太-雅加达	单台ECS安装: cd /usr/local && curl -k -O https://obs.ap-southeast-4.myhuaweicloud.com/uniagent-ap-southeast-4/package/agent_install.sh && bash agent_install.sh -r ap-southeast-4 -u 0.1.5 -t 2.7.5.1 -d agent.ces.myhuaweicloud.com 多台ECS批量安装: cd /usr/local && curl -k -O https://obs.ap-southeast-4.myhuaweicloud.com/uniagent-ap-southeast-4/package/batch_agent_install.sh && bash batch_agent_install.sh -r ap-southeast-4 -u 0.1.5 -t 2.7.5.1 -d agent.ces.myhuaweicloud.com
非洲-约翰内斯堡	单台ECS安装: cd /usr/local && curl -k -O https://uniagent-af-south-1.obs.af-south-1.myhuaweicloud.com/package/agent_install.sh && bash agent_install.sh -r af-south-1 -u 0.1.5 -t 2.7.5.1 -d agent.ces.myhuaweicloud.com 多台ECS批量安装: cd /usr/local && curl -k -O https://uniagent-af-south-1.obs.af-south-1.myhuaweicloud.com/package/batch_agent_install.sh && bash batch_agent_install.sh -r af-south-1 -u 0.1.5 -t 2.7.5.1 -d agent.ces.myhuaweicloud.com

区域	安装脚本
拉美-墨西哥城二	单台ECS安装: <pre>cd /usr/local && curl -k -O https://uniagent-la-north-2.obs.la-north-2.myhuaweicloud.com/package/agent_install.sh && bash agent_install.sh -r la-north-2 -u 0.1.5 -t 2.7.5.1 -d agent.ces.myhuaweicloud.com</pre> 多台ECS批量安装: <pre>cd /usr/local && curl -k -O https://uniagent-la-north-2.obs.la-north-2.myhuaweicloud.com/package/batch_agent_install.sh && bash batch_agent_install.sh -r ap-southeast-3 -u 0.1.5 -t 2.7.5.1 -d agent.ces.myhuaweicloud.com</pre>
拉美-圣地亚哥	单台ECS安装: <pre>cd /usr/local && curl -k -O https://obs.la-south-2.myhuaweicloud.com/uniagent-la-south-2/package/agent_install.sh && bash agent_install.sh -r la-south-2 -u 0.1.5 -t 2.7.5.1 -d agent.ces.myhuaweicloud.com</pre> 多台ECS批量安装: <pre>cd /usr/local && curl -k -O https://obs.la-south-2.myhuaweicloud.com/uniagent-la-south-2/package/batch_agent_install.sh && bash batch_agent_install.sh -r ap-southeast-3 -u 0.1.5 -t 2.7.5.1 -d agent.ces.myhuaweicloud.com</pre>
中东-利雅得	单台ECS安装: <pre>cd /usr/local && curl -k -O https://uniagent-me-east-1.obs.me-east-1.myhuaweicloud.com/package/agent_install.sh && bash agent_install.sh -r me-east-1 -u 0.1.5 -t 2.7.5.1 -d agent.ces.myhuaweicloud.com</pre> 多台ECS批量安装: <pre>cd /usr/local && curl -k -O https://uniagent-me-east-1.obs.me-east-1.myhuaweicloud.com/package/batch_agent_install.sh && bash batch_agent_install.sh -r ap-southeast-3 -u 0.1.5 -t 2.7.5.1 -d agent.ces.myhuaweicloud.com</pre>

（可选）安装 lspci 工具

1. 登录弹性云服务器。
2. 更新镜像源，获取安装依赖。
更多内容，请参见[如何使用华为云开源镜像配置yum源\(x86_64和ARM\)?](#)
3. 执行以下命令，安装lspci工具。
 - CentOS系统：
yum install pciutils
 - Ubuntu系统：
apt install pciutils
4. 执行以下命令，查看安装结果。
lspci -d 10de:

图 17-3 安装结果

```
[root@ecs-~]# lspci -d 10de:
00:0d.0 VGA compatible controller: NVIDIA Corporation TU104GL [Tesla T4] (rev a1)
```

17.6 异构类实例安装支持对应监控的 CES Agent（Windows）

操作场景

监控与告警是保证异构云服务器（GPU加速型实例、AI加速型实例）高可靠性、高可用性和高性能的重要功能。

通过在异构类（GPU加速型）的Windows实例上安装支持对应监控的CES Agent，可以为用户提供系统级、主动式、细颗粒度的监控，包含指标收集和系统事件上报。

当前支持的异构加速卡及对应的监控指标种类为GPU监控指标，请参见[操作系统监控指标：GPU](#)。

本章节介绍如何通过安装脚本为GPU加速型实例安装新版支持GPU监控的CES Agent。

约束与限制

- 仅支持Windows操作系统，且仅部分Windows镜像版本支持GPU监控。

表 17-19 支持 GPU 监控的 Windows 版本

类型	版本
Windows（64bit）	Windows Server 2016 标准版 64位
	Windows Server 2016 数据中心版 64位
	Windows Server 2019 标准版 64位
	Windows Server 2019 数据中心版 64位

- 支持的规格：G6v、G6、P2s、P2v、P2vs、Pi2、Pi1、P1。
- 不支持监听Windows类型GPU加速型实例的Xid事件。
- 使用私有镜像创建的云服务器需手动安装监控组件并[安装驱动](#)。

前提条件

- 已配置DNS和安全组，配置方法参考[如何配置DNS和安全组？](#)。
 - 已配置委托，配置方法参考[如何配置委托？](#)。
 - 已安装GPU驱动，未安装GPU驱动的云服务器不支持采集GPU指标数据及上报事件。
- 如果您的弹性云服务器未安装GPU驱动，可参见[（推荐）自动安装GPU加速型ECS的GPU驱动（Windows）](#)。

📖 说明

- 安装GPU驱动需使用默认路径。
GPU驱动安装完后，需重启GPU加速型实例，否则可能导致采集GPU指标及上报GPU事件失败。
- GPU驱动正常安装后，最多10分钟将在控制台看到采集到的GPU指标数据。
- 需使用具有Administrator权限的账户进行安装，例如Administrator用户。
- 确保云服务器的安装目录都有读写权限，并且安装成功后的Telescope进程不会被其他软件关闭。

操作步骤

本操作以Windows Server 2019 标准版 64位操作系统、Pi2规格的GPU加速型实例为例，介绍单台ECS安装新版支持GPU监控的CES Agent的操作指导。

1. 使用Administrator用户，[远程登录](#)弹性云服务器。
2. 在浏览器地址栏输入地址，下载安装脚本。

以“华东-上海一”为例，安装脚本地址为：

https://uniagent-cn-east-3.obs.cn-east-3.myhuaweicloud.com/package/install_amd64.exe

其余区域的安装脚本，请参见[获取安装脚本](#)。

3. （可选）在以下路径，卸载旧版本支持GPU监控的CES Agent。

C:\Program Files\uniagent\script\uninstall.bat

4. 以管理员身份打开cmd命令窗口，在“install_amd64.exe”下载目录下，执行以下命令安装支持GPU监控的CES Agent安装脚本。

install_amd64.exe [-r RegionID] [-u UniagentVersion] [-t TelescopeVersion] [-d AgentApiDomain]

命令示例：

install_amd64.exe -r cn-east-3 -u 0.1.5 -t 2.7.5.1 -d agent.ces.myhuaweicloud.com

其中，

- RegionID: cn-east-3
- UniagentVersion: 0.1.5
- TelescopeVersion: 2.7.5.1
- AgentApiDomain: agent.ces.myhuaweicloud.com

📖 说明

如果命令执行后出现“Access is denied”，可能是由于未以管理员身份打开cmd命令窗口导致，请切换为管理员身份重新执行命令。

当界面显示“Install service success”或“Install agent successfully”时，说明支持GPU监控的CES Agent安装成功并启动。

图 17-4 支持 GPU 监控的 CES Agent 安装成功

```
C:\Users\Administrator\Downloads>install_amd64.exe -r cn-east-3 -u 0.1.5 -t 2.5.2.1 -d agent.ces.myhuaweicloud.com
Download uniagent package successfully, url: https://uniagent-cn-east-3.obs.cn-east-3.myhuaweicloud.com:443/package/uniagent_windows_amd64_0.1.5.zip...
Run cmd: del /s /q C:\Progra~1\uniagent\uniagent_windows_amd64.zip
Run cmd: xcopy C:\Progra~1\uniagent\uniagent_windows_amd64 C:\Progra~1\uniagent /s /e /y
Run cmd: cd C:\Progra~1\uniagent
Run cmd: C:\Progra~1\uniagent\bin\uniagent.exe install
Run cmd: rd /s /q C:\Progra~1\uniagent\uniagent_windows_amd64
Download telescope package successfully, url: https://uniagent-cn-east-3.obs.cn-east-3.myhuaweicloud.com:443/extension/telescope/telescope-2.5.2.1.tar.gz...
Run cmd: del /s /q C:\Progra~1\uniagent\telescope.tar.gz
Run cmd: copy C:\Progra~1\uniagent\telescope\manifest.json C:\Progra~1\uniagent\extension\holder\telescope\manifest.json /y
Run cmd: C:\Progra~1\uniagent\telescope\windows_bin\install.bat
Run cmd: rd /s /q C:\Progra~1\uniagent\telescope
Install agent successfully, the program is about to exit...
```

获取安装脚本

您可以通过以下地址，下载获取新版支持CES监控Agent的安装脚本。

表 17-20 安装脚本的支持区域及获取地址

区域	安装脚本
华北-北京一	https://uniagent-cn-north-1.obs.cn-north-1.myhuaweicloud.com/package/install_amd64.exe
华北-北京四	https://uniagent-cn-north-4.obs.cn-north-4.myhuaweicloud.com/package/install_amd64.exe
华北-乌兰察布一	http://obs.cn-north-9.myhuaweicloud.com/uniagent-cn-north-9/package/install_amd64.exe
华南-广州	https://uniagent-cn-south-1.obs.cn-south-1.myhuaweicloud.com/package/install_amd64.exe
华东-上海一	https://uniagent-cn-east-3.obs.cn-east-3.myhuaweicloud.com/package/install_amd64.exe
华东-上海二	https://uniagent-cn-east-2.obs.cn-east-2.myhuaweicloud.com/package/install_amd64.exe
西南-贵阳一	https://uniagent-cn-southwest-2.obs.cn-southwest-2.myhuaweicloud.com/package/install_amd64.exe
中国-香港	https://uniagent-ap-southeast-1.obs.ap-southeast-1.myhuaweicloud.com/package/install_amd64.exe
亚太-曼谷	https://uniagent-ap-southeast-2.obs.ap-southeast-2.myhuaweicloud.com/package/install_amd64.exe
亚太-新加坡	https://uniagent-ap-southeast-3.obs.ap-southeast-3.myhuaweicloud.com/package/install_amd64.exe
亚太-雅加达	https://obs.ap-southeast-4.myhuaweicloud.com/uniagent-ap-southeast-4/package/install_amd64.exe
非洲-约翰内斯堡	https://uniagent-af-south-1.obs.af-south-1.myhuaweicloud.com/package/install_amd64.exe
拉美-墨西哥城二	https://uniagent-la-south-2.obs.la-south-2.myhuaweicloud.com/package/install_amd64.exe

区域	安装脚本
拉美-圣地亚哥	https://uniagent-la-north-2.obs-la-north-2.myhuaweicloud.com/package/install_amd64.exe

17.7 设置告警规则

操作场景

通过设置弹性云服务器告警规则，用户可自定义监控目标与通知策略，及时了解弹性云服务器运行状况，从而起到预警作用。

设置弹性云服务器的告警规则包括设置告警规则名称、监控对象、监控指标、告警阈值、监控周期和是否发送通知等参数。本节介绍了设置弹性云服务器告警规则的具体方法。

前提条件

设置告警规则操作，需要您具有CES FullAccess角色权限，若提示权限不足，请联系管理员进行授权，详细内容，请参见[权限管理](#)。

操作步骤

1. 登录管理控制台。
2. 单击管理控制台左上角的，选择区域和项目。
3. 选择“管理与监管 > 云监控服务”。
4. 在左侧导航树栏，选择“告警 > 告警规则”。
5. 在“告警规则”界面，单击“创建告警规则”。
也可以选择已有的告警规则进行修改，设置弹性云服务器的告警规则。
6. 在“创建告警规则”界面，根据界面提示配置参数。
关键参数如下，更多配置参数信息，请参见[创建告警规则和通知](#)：
 - 告警名称：系统会随机产生一个名称，也可以进行修改。
 - 资源类型：弹性云服务器
 - 维度：云服务器

说明

如果为GPU加速型实例创建告警规则，“维度”选择“云服务器-GPU”。

- 监控范围：告警规则适用的资源范围，可选择全部资源、资源分组或指定资源。
- 触发规则：根据需要可选择关联模板、导入已有模板或自定义创建。

说明

选择关联模板后，所关联模板内容修改后，该告警规则中所包含策略也会跟随修改。

- 告警策略：触发告警规则的告警策略。
7. 根据界面提示，配置告警通知参数。

如果要配置通过邮件、短信、HTTP和HTTPS向用户发送告警通知，则设置“发送通知”为开启。

更多配置参数信息，请参见[创建告警规则和通知](#)。

- 配置完成后，单击“立即创建”，完成告警规则的创建。

说明

更多关于弹性云服务器监控规则的信息，请参见[《云监控用户指南》](#)。

17.8 查看监控指标

操作场景

云服务平台提供的云监控，可以对弹性云服务器的运行状态进行日常监控。您可以通过管理控制台，直观地查看弹性云服务器的各项监控指标。

由于监控数据的获取与传输会花费一定时间，因此，云监控显示的是当前时间5~10分钟前的弹性云服务器状态。如果您的弹性云服务器刚刚创建完成，请等待5~10分钟后查看监控数据。

前提条件

- 弹性云服务器正常运行。
关机、故障、删除状态的弹性云服务器，无法在云监控中查看其监控指标。当弹性云服务器再次启动或恢复后，即可正常查看。

说明

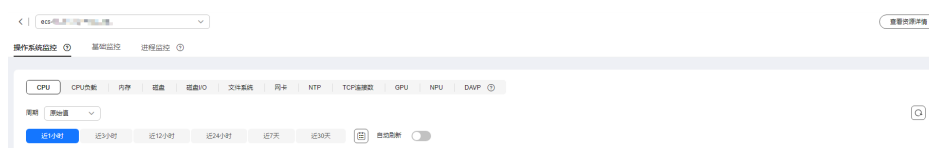
关机、故障24小时的弹性云服务器，云监控将默认该弹性云服务器不存在，并在监控列表中删除，不再对其进行监控，但告警规则需要用户手动清理。

- 弹性云服务器已对接云监控，即已在云监控页面设置告警规则。
对接云监控之前，用户无法查看到未对接资源的监控数据。具体操作，请参见[设置告警规则](#)。
- 弹性云服务器已正常运行一段时间（约10分钟）。
对于新创建的弹性云服务器，需要等待一段时间，才能查看上报的监控数据和监控视图。

操作步骤

- 登录管理控制台，进入[ECS列表页](#)。
- 在弹性云服务器列表中的右上角，输入弹性云服务器名称、IP地址或ID，并进行搜索。
- 在弹性云服务器“监控”列，单击“”，可查看当前弹性云服务器的监控数据。
- 在弹出的监控指标页面右上角，单击“查看更多指标详情”，查看弹性云服务器的完整监控数据，包含操作系统监控、基础监控以及进程监控。

图 17-5 监控数据



5. 在弹性云服务器监控区域，您可以通过选择时长，查看对应时间的监控数据。
当前支持查看弹性云服务器“近1小时”、“近3小时”、“近12小时”、“近24小时”、“近7天”的监控数据。

18 使用 CTS 审计 ECS 操作事件

18.1 ECS 支持云审计的关键操作

操作场景

平台提供了云审计服务。通过云审计服务，您可以记录与云服务器相关的操作事件，便于日后的查询、审计和回溯。

前提条件

已开通云审计服务。

支持审计的关键操作列表

表 18-1 云审计服务支持的云服务器操作列表

操作名称	资源类型	事件名称
创建云服务器	ecs	createServer createServerV2 createServerV21
删除云服务器	ecs	deleteServer deleteServerV2 deleteServerV21 deleteVmByNative
启动云服务器	ecs	startServer
重启云服务器	ecs	rebootServer
关闭云服务器	ecs	stopServer
添加云服务器网卡	ecs	addNic

操作名称	资源类型	事件名称
删除云服务器网卡	ecs	deleteNic delNic
挂载磁盘	ecs	attachVolume attachVolumeV2
挂载磁盘（EVS页面触发）	ecs	attachVolume
卸载磁盘	ecs	detachVolume
重装操作系统	ecs	reinstallOs reinitOs
切换操作系统	ecs	changeOs reinitOs
变更规格	ecs	resizeServer
配置虚拟机自动恢复标签	ecs	addAutoRecovery
删除虚拟机自动恢复标签	ecs	deleteAutoRecovery
更新元数据/设置指定key的元数据 （不包含委托名称）	ecs	updateMetadata
更新元数据/设置指定key的元数据 （包含委托名称）	ecs	updateMetadataAndSe rverAgency
更新委托	ecs	updateServerAgency
获取VNC远程登录	ecs	remoteConsole
修改云服务器信息	ecs	updateServer
迁移虚拟机	ecs	migrateServer
创建FPGA镜像	aei	createFpgaImage
删除FPGA镜像	aei	deleteFpgaImage
关联FPGA镜像	aei	associateFpgaImage
解关联FPGA镜像	aei	disassociateFpgaImage
注册FPGA镜像	aei	registerFpgaImage
中断竞价计费型实例	server	interruptServer
虚拟机状态管理操作（OpenStack Nova API）	server	operateServer
添加/删除/更新标签	ecsTags	dealUnifiedTags

18.2 查询 ECS 审计事件

操作场景

用户进入云审计服务创建管理类追踪器后，系统开始记录云服务资源的操作。在创建数据类追踪器后，系统开始记录用户对OBS桶中数据的操作。云审计服务管理控制台会保存最近7天的操作记录。

本节介绍如何在云审计服务管理控制台查看或导出最近7天的操作记录。

- [在新版事件列表查看审计事件](#)
- [在旧版事件列表查看审计事件](#)

使用限制

- 单账号跟踪的事件可以通过云审计控制台查询。多账号的事件只能在账号自己的事件列表页面去查看，或者到组织追踪器配置的OBS桶中查看，也可以到组织追踪器配置的CTS/system日志流下面去查看。
- 用户通过云审计控制台只能查询最近7天的操作记录。如果需要查询超过7天的操作记录，您必须配置转储到对象存储服务（OBS）或云日志服务（LTS），才可在OBS桶或LTS日志组里面查看历史事件信息。否则，您将无法追溯7天以前的操作记录。
- 云上操作后，1分钟内可以通过云审计控制台查询管理类事件操作记录，5分钟后才可通过云审计控制台查询数据类事件操作记录。
- CTS新版事件列表不显示数据类审计事件，您需要在旧版事件列表查看数据类审计事件。
- 云审计控制台对用户的操作事件日志保留7天，过期自动删除，不支持人工删除。

在新版事件列表查看审计事件

1. 登录管理控制台。
2. 单击左上角 ，选择“管理与监管 > 云审计服务 CTS”，进入云审计服务页面。
3. 单击左侧导航树的“事件列表”，进入事件列表信息页面。
4. 事件列表支持通过高级搜索来查询对应的操作事件，您可以在筛选器组合一个或多个筛选条件：
 - 事件名称：输入事件的名称。
 - 事件ID：输入事件ID。
 - 资源名称：输入资源的名称，当该事件所涉及的云资源无资源名称或对应的API接口操作不涉及资源名称参数时，该字段为空。
 - 资源ID：输入资源ID，当该资源类型无资源ID或资源创建失败时，该字段为空。
 - 云服务：在下拉框中选择对应的云服务名称。
 - 资源类型：在下拉框中选择对应的资源类型。
 - 操作用户：在下拉框中选择一个或多个具体的操作用户。

- 事件级别：可选项为“normal”、“warning”、“incident”，只可选择其中一项。
 - normal：表示操作成功。
 - warning：表示操作失败。
 - incident：表示比操作失败更严重的情况，例如引起其他故障等。
- 企业项目ID：输入企业项目ID。
- 访问密钥ID：输入访问密钥ID（包含临时访问凭证和永久访问密钥）。
- 时间范围：可选择查询最近1小时、最近1天、最近1周的操作事件，也可以自定义最近7天内任意时间段的操作事件。

说明

您可以参考[云审计服务应用示例](#)，来学习如何查询具体的事件。

5. 在事件列表页面，您还可以导出操作记录文件、刷新列表、设置列表展示信息等。
 - 在搜索框中输入任意关键字，按下Enter键，可以在事件列表搜索符合条件的数据。
 - 单击“导出”按钮，云审计服务会将查询结果以.xlsx格式的表格文件导出，该.xlsx文件包含了本次查询结果的所有事件，且最多导出5000条信息。
 - 单击按钮，可以获取到事件操作记录的最新信息。
 - 单击按钮，可以自定义事件列表的展示信息。启用表格内容折行开关，可让表格内容自动折行，禁用此功能将会截断文本，默认停用此开关。
6. 关于事件结构的关键字段详解，请参见《云审计服务用户指南》中的[事件结构](#)和[事件样例](#)。
7. （可选）在新版事件列表页面，单击右上方的“返回旧版”按钮，可切换至旧版事件列表页面。

在旧版事件列表查看审计事件

1. 登录管理控制台。
2. 单击左上角，选择“管理与监管 > 云审计服务 CTS”，进入云审计服务页面。
3. 单击左侧导航树的“事件列表”，进入事件列表信息页面。
4. 用户每次登录云审计控制台时，控制台默认显示新版事件列表，单击页面右上方的“返回旧版”按钮，切换至旧版事件列表页面。
5. 事件列表支持通过筛选来查询对应的操作事件。当前事件列表支持四个维度的组合查询，详细信息如下：
 - 事件类型、云服务、资源类型和筛选类型，在下拉框中选择查询条件。
 - 筛选类型按资源ID筛选时，还需手动输入某个具体的资源ID。
 - 筛选类型按事件名称筛选时，还需选择某个具体的事件名称。
 - 筛选类型按资源名称筛选时，还需选择或手动输入某个具体的资源名称。

- 操作用户：在下拉框中选择某一具体的操作用户，此操作用户指用户级别，而非租户级别。筛选操作用户时，支持单选、多选或全部选择。
- 事件级别：可选项为“所有事件级别”、“Normal”、“Warning”、“Incident”，只可选择其中一项。
- 时间范围：可选择查询最近1小时、最近1天、最近1周的操作事件，也可以自定义最近7天内任意时间段的操作事件。

📖 说明

您可以参考[云审计服务应用示例](#)，来学习如何查询具体的事件。

6. 选择完查询条件后，单击“查询”。
7. 在事件列表页面，您还可以导出操作记录文件和刷新列表。
 - 单击“导出”按钮，云审计服务会将查询结果以CSV格式的表格文件导出，该CSV文件包含了本次查询结果的所有事件，且最多导出5000条信息。
 - 单击按钮，可以获取到事件操作记录的最新信息。
8. 在事件的“是否篡改”列中，您可以查看该事件是否被篡改：
9. 在需要查看的事件左侧，单击展开该记录的详细信息。

事件名称	资源类型	云服务	资源ID	资源名称	事件级别	操作用户	操作时间	操作
createDockerConfig	dockerlogincmd	SWR	--	dockerlogincmd	normal		2023/11/16 10:54:04 GMT+08:00	查看事件
request trace_id code trace_name resource_type trace_rating api_version message source_ip domain_id trace_type								
createDockerConfig, Method: POST Url=/v2/manage/utills/secret, Reason:								
ApiCall								

10. 在需要查看的记录右侧，单击“查看事件”，会弹出一个窗口显示该操作事件结构的详细信息。

查看事件

```
{
  "request": "",
  "trace_id": "676d4ae3-842b-11ee-9299-9159eee6a3ac",
  "code": "200",
  "trace_name": "createDockerConfig",
  "resource_type": "dockerlogincmd",
  "trace_rating": "normal",
  "api_version": "",
  "message": "createDockerConfig, Method: POST Url=/v2/manage/utills/secret, Reason:",
  "source_ip": "",
  "domain_id": "",
  "trace_type": "ApiCall",
  "service_type": "SWR",
  "event_type": "system",
  "project_id": "",
  "response": "",
  "resource_id": "",
  "tracker_name": "system",
  "time": "2023/11/16 10:54:04 GMT+08:00",
  "resource_name": "dockerlogincmd",
  "user": {
    "domain": {
      "name": "",
      "id": ""
    }
  }
}
```

11. 关于事件结构的关键字段详解，请参见《云审计服务用户指南》中的[事件结构](#)和[事件样例](#)。

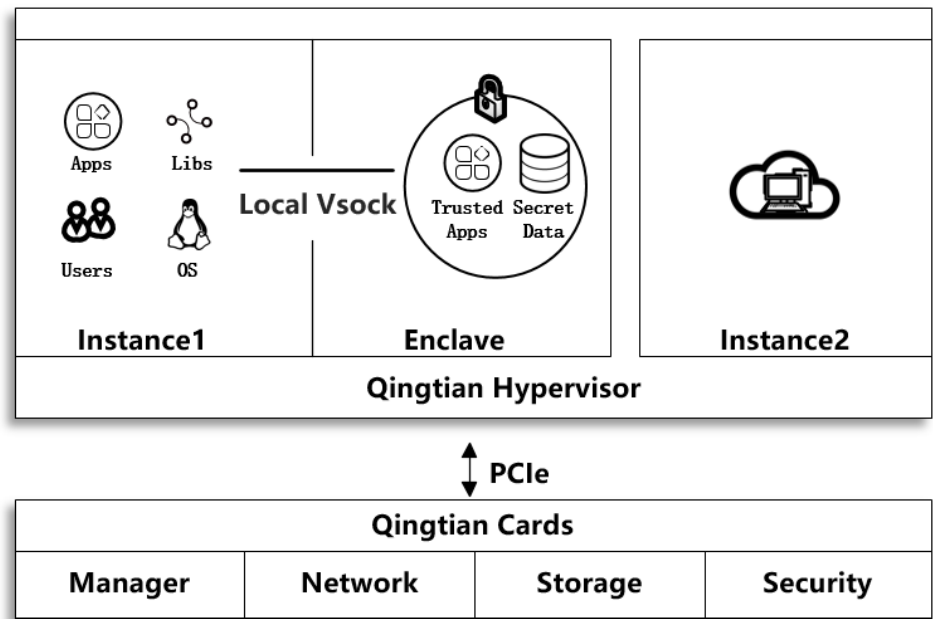
12. （可选）在旧版事件列表页面，单击右上方的“体验新版”按钮，可切换至新版事件列表页面。

19 QingTian Enclave 管理

19.1 QingTian Enclave 简介

19.1.1 什么是 QingTian Enclave

- 在现有的基于QingTian架构的虚拟机产品中，我们增加了一个置于其内部的，安全的、完全隔离的虚拟机，这个虚拟机我们称之为QingTian Enclave虚拟机，外部对这个QingTian Enclave虚拟机具备所有权的虚拟机，我们称之为父虚拟机。QingTian Enclave是完全独立的虚拟机，无持久化存储、交互式访问或外部网络连接。父虚拟机与QingTian Enclave之间通过安全的本地通道进行通信。即使是父虚拟机上的root用户，也不能访问QingTian Enclave或通过 SSH 连接到QingTian Enclave。
- QingTianHypervisor可以将QingTian Enclave的CPU 和内存与父虚拟机的CPU和内存资源隔离开，提供给您一个完全隔离的可执行环境，显著减少了攻击面。因此，使用QingTian Enclave，您能保护敏感的核心数据和应用程序，为您在QingTian Enclave中运行的服务增加安全保障。
- QingTian Enclave还提供了证明（Attestation）的功能，您可以通过该功能验证QingTian Enclave实例的可信度量值。[华为云密钥管理服务（Key management Service，简称KMS）](#)为QingTian证明功能提供了内在支持，您能限制应用程序必须在预期的QingTian Enclave运行环境中才能调用KMS API处理敏感数据。



约束条件

QingTian Enclave有以下约束：

虚拟机名称	限制要求
父虚拟机（主虚拟机）	1. 至少预留2个vCPU，至少预留512M内存空间。 2. 必须为Linux操作系统。
QingTian Enclave（从虚拟机）	1. 裸金属实例不支持QingTian Enclave。 2. 必须为Linux操作系统。 3. 启动QingTian Enclave最低内存规格为128M，并且不能小于Enclave镜像文件（Enclave Image File，简称EIF）文件大小的4倍。 4. 当在配置文件中，为QingTian Enclave配置2M大页的内存管理方式时，QingTian Enclave启动支持的最大内存为512M。 5. 当在配置文件中，为QingTian Enclave配置1G大页的内存管理方式时，QingTian Enclave最大内存为256G。 6. QingTian Enclave所使用的内存和CPU都必须隔离自同一个NUMA节点。 7. vcpu数量配置需要为偶数，最高不超过父虚拟机单NUMA node cpu数量减 2；总数量最高不超过62。 8. 在QingTian Enclave中运行的应用程序需要和OS（内核，ramdisk，init程序）一起被打包成QingTian Enclave镜像。

📖 说明

内存和CPU资源隔离的详细内容，请参见[资源隔离](#)。

父虚拟机和QingTian Enclave关系：

1. 每个父虚拟机可以创建最多两个QingTian Enclave。
2. 不支持与父虚拟机共物理内核。
3. 只有在父虚拟机处于运行状态时，QingTian Enclave才处于运行状态。如果父虚拟机被停止或终止，则QingTian Enclave被终止。
4. QingTian Enclave分配的资源（内存和CPU等），都是从父虚拟机中分割出来的，内存区间要求是2M/1G对齐的连续物理区间。

另外还需要注意：

1. 支持QingTian Enclave特性的父虚拟机规格：c7t、kc2
2. 支持QingTian Enclave特性的局点：华北-北京四、华东-上海一、华南-广州、亚太-新加坡、土耳其-伊斯坦布尔
3. 如果您在QingTian Enclave中的业务被意外终止，您需要手动重新运行该业务
4. QingTian Enclave的默认配置为使用1G大页，具有1G内存，2vcpu
5. QingTian Enclave父虚拟机的最小规格是8vCPU，16G内存

计费标准

在公测期间，使用QingTian Enclave并不会收取额外费用，您只需要支付ECS的购买费用。

相关服务

QingTian Enclave与以下华为云服务集成：

1. 密钥管理服务

密钥管理服务（KMS）是华为云数据加密服务族中的一个核心服务。KMS提供可用性高的密钥生成、存储、管理和审计解决方案。KMS密钥由硬件安全模块HSM保护，并与许多华为云数据存储服务集成。您可以借此服务开发自己的安全的数据应用。

2. 华为统一身份认证服务

统一身份认证（Identity and Access Management，简称IAM）是华为云提供权限管理的基础服务，可以帮助您安全地控制华为云服务和资源的访问权限。

19.1.2 QingTian Enclave 概念

- QingTian Enclave

QingTian Enclave是完全隔离的虚拟机，它的内存和CPU来自于其父虚拟机被预先隔离出来的资源。QingTian Enclave既没有外部网络，也没有持久化存储。父虚拟机内的进程、应用程序、内核或者用户都无法访问QingTian Enclave中的资源。

- 父虚拟机

父虚拟机是一个能够将其CPU及内存资源隔离分配给QingTian Enclave的ECS实例。这些资源能够在QingTian Enclave的生存周期内被其使用。启动QingTian Enclave成功后，该QingTian Enclave只能与其父虚拟机进行安全通信。

- QingTian Enclave镜像文件

QingTian Enclave镜像文件（.eif）提供了启动QingTian Enclave并在其中运行QingTian Enclave应用程序所需的系统信息，包括Linux操作系统、其他第三方库和QingTian Enclave应用程序。镜像创建详情见[Linux系统上QingTian Enclave应用的开发](#)。
- QingTian命令行工具

作为华为云QingTian命令行工具（qt CLI），在QingTian Enclave使用场景中，qt CLI可以用于创建、关闭和查询QingTian Enclave信息。qt CLI必须在父虚拟机上安装和使用。详情见[QingTian CLI（qt CLI）](#)。
- Enclave SDK

Enclave SDK由一系列开源库组成，以使用户开发自己的QingTian Enclave应用程序。它集成了一些与华为云KMS交互的接口，例如加解密和产生随机数等，并为远程证明提供了内在支持。
- QingTian密码学证明

QingTian密码学证明是QingTian Enclave在与KMS服务交互时证明自己合法性的过程。它依赖QingTianHypervisor产生的具有数字签名的证明文档。一个QingTian Enclave证明文档内包含的具体信息可以作为第三方服务认证及鉴权的条件。您可以在IAM服务中使用kms:RecipientAttestation相关条件键值（condition key）来控制对KMS服务特定接口操作的访问权限，例如生成随机数或者加解密操作。
- 证明文档

证明文档（Attestation Document）由QingTianHypervisor产生并签名，其文件内容为QingTian Enclave的信息，包括PCR、密码摘要以及用户声明。外部服务可以通过证明文件来验证QingTian Enclave的身份是否可信。用户可以利用证明文档构建自己的可信系统，也可以与KMS交互时使用。详情可见[证明文档](#)。
- qt-proxy

qt-proxy是一个运行在父虚拟机上的网络代理服务。用户可以使用这个服务，使父虚拟机转发来自于QingTian Enclave的网络包，实现QingTian Enclave与外界进行通信。这是QingTian Enclave用来与外部服务交互的唯一通信渠道。
- qproxy

qproxy提供了tcp和vsock网络包的转换能力，相比qt-proxy，用户的网络代码无需修改就可以运行在QingTian Enclave中，详情请参见[QingTian Enclave网络代理工具](#)。
- qlog

qlog提供了导出QingTian Enclave中指定文件到父虚拟机中的能力，有利于客户导出QingTian Enclave中的业务日志，方便后续运维。
- PCR

平台配置寄存器（Platform configuration registers, PCRs）是QingTian Enclave独有的可信度量值。一部分在QingTian Enclave创建时自动产生，用于验证QingTian Enclave自创建以来的完整性，另一部分可以由用户自己定义以确保QingTian Enclave能够运行在他所希望执行的平台上。另外，Attestation Document包含了相关的PCR，用户可以使用PCR作为IAM访问控制策略的条件键（condition key），以实现更为严格的访问控制。详情可见[PCR简介](#)。
- 本地连接通道

本地连接通道（Local Vsock Connection）是QingTian Enclave实例与父虚拟机之间唯一的，安全的本地通信通道。

- QingTian安全模块

QingTian安全模块（QingTian Security Module, QTSM）整体由qt-sm-lib函数库和qt-sm-server服务组成。您可以在您的QingTian Enclave 应用程序中调用qt-sm-lib用户态接口，qt-sm-server会处理具体的QTSM请求并将返回相应结果。qt-sm-lib提供的用户态接口包括查询指定index对应的PCR值（qt-sm-describe_pcr），扩展指定index的PCR值（qt-sm-extend_pcr），锁定指定index的PCR值（qt-sm-lock_pcr），批量锁定指定index的PCR值（qt-sm-lock_pcrs），获取QTSM信息（qt-sm-get_describe）和获取已签名的证明文档（qt-sm-get_attestation）。

19.2 快速入门

以下教程将引导您了解并使用QingTian Enclave特性，包括如何启动QingTian Enclave父虚拟机，如何构建QingTian Enclave镜像文件，如何查询正在运行的QingTian Enclave，以及停止QingTian Enclave。

1. 购买一台弹性云服务器作为QingTian Enclave的父虚拟机，“操作系统”选择Linux类型系统镜像，并勾选“Enclave”。
2. 连接到QingTian Enclave父虚拟机，详细操作，请参见[Linux ECS登录方式概述](#)。
3. 配置QingTian Enclave父虚拟机。

- 若选择Huawei Cloud EulerOS 2.0镜像：

- i. 在父虚拟机中安装qt CLI工具和必要外围组件。

使用qt CLI工具需要安装必要的python模块，详情请参见[安装qt CLI](#)。

```
yum install qt-enclave-bootstrap  
yum install virtio-qtbox  
yum install qingtian-tool
```

其中，

- virtio-qtbox：安装enclave相关驱动
- qt-enclave-bootstrap：包含enclave镜像文件制作的必要文件
- qingtian-tools：用于管理enclave生命周期

- ii. 在qt-enclave-env.conf配置文件中按需配置隔离参数，详情请参见[qt-enclave-env工具介绍](#)。

建议一次性隔离出较大内存资源预留给QingTian Enclave使用，避免反复隔离，造成系统内存碎片化，隔离服务重启失败。

```
vim /etc/qingtian/enclave/qt-enclave-env.conf
```

将“memory_mib”设置为“8192”，“cpu_count”设置为“2”，详细内容如下：

```
# qingtian enclave configuration file.  
  
# Which hugepage size to reserve for qingtian enclave  
# can only configure it by 2 (2MB hugepage size) or 1024 (1GB hugepage size)  
hugepage_size: 1024  
  
# How much memory to allocate for qingtian enclave (in MiB).  
memory_mib:8192  
  
# User can use cpu_count to set how many CPUs need to be reserved.  
# Or cpu_list to set which CPUs need to be reserved.  
#  
# cpu_count and cpu_list conflict with each other. Only use exactly one of them.
```

```
#
# How many CPUs to reserve for qingtian enclave.
cpu_count:2

# Which CPUs to reserve for qingtian enclave. You can configure it like below:
# 2,3 means reserving CPUs 2, 3, and you can also use 2-5 to reserve 2 through 5.
# cpu_list:2,3
```

iii. 启动资源隔离服务。

```
systemctl start qt-enclave-env
```

如果出现隔离服务失败，无法申请到足够内存，可能存在内存碎片，建议先重启虚拟机，再执行隔离服务。

- 若选择Ubuntu 22.04镜像：

i. 下载华为云QingTian Enclave代码。

ii. 目前，支持Ubuntu 22.04镜像的分支为：<https://gitee.com/HuaweiCloudDeveloper/huawei-qingtian.git>。

```
cd /home
git clone https://gitee.com/HuaweiCloudDeveloper/huawei-qingtian.git
cd /home/huawei-qingtian
```

iii. 安装所需依赖。

```
apt-get update -y
apt install libgnutls28-dev libcjson-dev libglib2.0-dev -y
```

iv. 编译virtio-qtbox。

```
cd /home/huawei-qingtian/virtio-qtbox
make
make install
```

v. 编译qingtian-tools工具包。

```
cd /home/huawei-qingtian/qingtian-tools
make
make install
```

vi. 编译qt-proxy包。

```
cd /home/huawei-qingtian/qingtian-tools/qt-proxy
make
make install
```

vii. 安装qt-enclave-bootstrap包。

因为需要编译内核，若无特殊需要，可以将Huawei Cloud EulerOS的qt-enclave-bootstrap包解压后至对应路径。

```
apt install alien -y
cd /home
wget https://repo.huaweicloud.com/hce/2.0/updates/x86_64/Packages/qt-enclave-bootstrap-1.0-34.hce2.x86_64.rpm
alien -d qt-enclave-bootstrap-1.0-34.hce2.x86_64.rpm
dpkg -i qt-enclave-bootstrap_1.0-35_amd64.deb
```

4. 为QingTian Enclave父虚拟机安装必要的Python包。

```
pip3 install docker knack
```


图 19-1 安装结果

```
[root@ ~]# pip3 install docker knack
WARNING: When the --extra-index-url option is used, the installation package is downloaded from an unverified URL. Exercise caution when using this option.
WARNING: Running pip install with root privileges is generally not a good idea. Try `pip3 install --user` instead.
Collecting docker
  Downloading docker-7.1.0-py3-none-any.whl (147 kB)
Collecting knack
  Downloading knack-0.12.0-py3-none-any.whl (60 kB)
Requirement already satisfied: requests>=2.26.0 in /usr/local/lib/python3.9/site-packages (from docker) (2.32.3)
Requirement already satisfied: urllib3>=1.26.0 in /usr/local/lib/python3.9/site-packages (from docker) (2.2.3)
Collecting packaging
  Downloading packaging-25.0-py3-none-any.whl (66 kB)
Collecting tabulate
  Downloading tabulate-0.9.0-py3-none-any.whl (35 kB)
Collecting argcomplete
  Downloading argcomplete-3.6.2-py3-none-any.whl (43 kB)
Collecting jmespath
  Downloading jmespath-1.0.1-py3-none-any.whl (20 kB)
Collecting pygments
  Downloading pygments-2.19.1-py3-none-any.whl (1.2 MB)
Requirement already satisfied: pyyaml in /usr/local/lib64/python3.9/site-packages (from knack) (6.0.2)
Requirement already satisfied: idna<4,>=2.5 in /usr/local/lib/python3.9/site-packages (from requests>=2.26.0->docker) (3.10)
Requirement already satisfied: certifi>=2017.4.17 in /usr/local/lib/python3.9/site-packages (from requests>=2.26.0->docker) (2024.8.30)
Requirement already satisfied: charset-normalizer<4,>=2 in /usr/local/lib64/python3.9/site-packages (from requests>=2.26.0->docker) (3.4.0)
Installing collected packages: tabulate, pygments, packaging, jmespath, argcomplete, knack, docker
Successfully installed argcomplete-3.6.2 docker-7.1.0 jmespath-1.0.1 knack-0.12.0 packaging-25.0 pygments-2.19.1 tabulate-0.9.0
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behaviour with the system package manager. It is recommended to use a virtual environment instead: https://pip.pypa.io/warnings/venv
```

5. 在父虚拟机中安装Docker程序，我们推荐使用二进制的方式进行Docker安装，可以在Docker官方网站下载需要版本。
 - a. 以27.0.1版本为例下载Docker：
`wget https://download.docker.com/linux/static/stable/x86_64/docker-27.0.1.tgz`
 - b. 对下载的压缩包进行解压操作：
`tar xzf docker-27.0.1.tgz`
 - c. 解压完成后将docker目录下所有文件复制到/usr/bin目录下：
`cp docker/* /usr/bin`
 - d. 启动docker服务，并将日志等级设置为error等级：
`dockerd -l error --config-file ${/path/to/your/daemon.json} &`

📖 说明

在启动dockerd时需要配置额外配置文件：\${/path/to/your/daemon.json}

详细内容，请参考[设置镜像加速器](#)。

- e. 验证Docker版本：
`docker version`
 - f. 运行hello-world容器，查看Docker是否安装正确：
`docker run hello-world`
6. 构建QingTian Enclave镜像。
 - a. 使用以下**hello_enclave.sh**脚本作为QingTian Enclave应用程序：

```
#!/bin/bash
while true
do
    echo "hello enclave!"
    sleep 2
done
```

Dockerfile内容如下：

```
FROM ubuntu:latest
COPY hello_enclave.sh /root/hello_enclave.sh
CMD ["/root/hello_enclave.sh"]
```

上述示例是直接向虚拟终端或者串口设备打印业务信息，仅适用于在调试（debug）模式下运行。在日常运维时，为了保证系统安全，建议您将业务信息重定向到文件，然后再转发到父虚拟机中，详情请参见[QingTian Enclave日志转发工具](#)。

例如，将QingTian Enclave中的/tmp/hello_enclave_output导出到父虚拟机的指定路径中：


```
CMD ["/root/hello_enclave.sh > /tmp/hello_enclave_output"]
```

- b. 确认脚本有可执行权限：

```
chmod +x hello_enclave.sh
```

- c. 构建一个名为hello-enclave的Docker镜像：

```
docker build -f Dockerfile -t hello-enclave .
```

- d. 使用qt enclave make-img命令将Docker镜像转换为名为hello-enclave.eif的QingTian Enclave镜像：

```
qt enclave make-img --docker-uri hello-enclave --eif hello-enclave.eif
```

输出为：

```
# qt enclave make-img --docker-uri hello-enclave --eif hello-enclave.eif
{
  "digest": "SHA384",
  "PCR0":
"63bf78ece7d2388ff773d0cad2ebc9a3070359db46d567ba271ff8adfb8b0b091be4ff4d5dda3f1c83
109096e3656f3b",
  "PCR8":
"000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000"
}
```

现在已经构建了名为hello-enclave.eif的QingTian Enclave镜像，命令包含了一系列PCR值，包括PCR0和PCR8（该例子中制作镜像时并没有指定证书和密钥，所以PCR8为0）。这些哈希值是在Enclave镜像构建时产生的测量值，它们通常作为预期的测量值（相对于证明文档中所包含的启动时测量值而言）。

- e. 通过以下命令生成证书对：

```
openssl ecparam -out private-key.pem -name secp384r1 -genkey
openssl req -new -key private-key.pem -out ssl.csr
openssl x509 -req -days 365 -in ssl.csr -signkey private-key.pem -out server.pem
```

- f. 通过生成的证书和密钥生成对应的EIF文件：

```
qt enclave make-img --docker-uri hello-enclave --eif hello-enclave.eif --private-key private-
key.pem --signing-certificate server.pem
```

7. 运行QingTian Enclave实例。

现在可以使用以下命令来运行QingTian Enclave镜像：

```
qt enclave start --mem 1024 --cpus 2 --eif hello-enclave.eif --cid 4 --debug-mode
```

该实例运行在debug-mode，关于debug-mode详情可见[qt enclave子命令介绍](#)。

您会看到以下输出：

```
# qt enclave start --cpus 2 --mem 1024 --eif hello-enclave.eif --cid 4 --debug-mode
Started enclave with EnclaveID : 0, EnclaveCID : 4, NumberOfCPUs : 2, MemoryMiB : 1024
{
  "EnclaveID": 0,
  "EnclaveCID": 4,
  "NumberOfCPUs": 2,
  "MemoryMiB": 1024,
  "LaunchMode": "debug"
}
```

在该教程中，我们为QingTian Enclave实例分配了2个vCPU和1024M内存，并指定其cid为4，该cid可作为QingTian Enclave实例与父虚拟机实例之间的本地套接字的IP地址。

8. 查询正在运行的QingTian Enclave

按以上步骤创建完QingTian Enclave实例后，可以以下命令查询他是否在运行：

```
qt enclave query --enclave-id 0
# qt enclave query --enclave-id 0
[[
  "EnclaveID": 0,
  "ProcessID": 29990,
  "EnclaveCID": 4,
```

```
"NumberOfCPUs": 2,  
"MemoryMiB": 1024,  
"LaunchMode": "debug"  
}]
```

该命令可以用于查询QingTian Enclave相关信息，包括EnclaveID、ProcessID、EnclaveCID、vCPU数量、内存数量以及其运行模式。因为该实例是以debug模式启动的，所以可以用qt enclave console 命令查看QingTian Enclave的只读控制台输出。

```
hello enclave!  
hello enclave!  
hello enclave!  
hello enclave!
```

您将观察到终端每隔2秒打印一次hello enclave!。

9. 停止正在运行的QingTian Enclave实例

如果您想停止运行以上的QingTian Enclave实例，可以使用以下命令：

```
# qt enclave stop --enclave-id 0  
stop enclave 0 successfully  
{  
  "EnclaveID": 0  
}
```

19.3 典型使用案例

在这个章节中，我们将介绍一个QingTian Enclave的使用场景。其中包含了一些角色和基本的工作流程，同时使用了华为云数据加密服务（DEW）的KMS子服务，华为云统一身份认证服务（IAM）和华为云对象存储服务（OBS）。

19.3.1 工作流程

相关角色

在这个QingTian Enclave使用场景里，涉及到了以下几个角色：

- 安全员：拥有对机密数据和华为云KMS密钥的控制权限。作为华为云账号的所有者，他具有最高权限，例如他可以创建IAM用户并为其设置最小权限，创建加密密钥和加密敏感数据等。在本场景中，我们还假设安全员同时承担了Enclave镜像构建的工作，他获得预期的Enclave镜像度量值PCR0和PCR8，并在IAM授权策略中使用这些度量值作为条件键。
- 父虚拟机管理员：作为被安全员授权的运维人员，他拥有父虚拟机实例的访问权限，并能管理QingTian Enclave实例的生命周期。他使用安全员构建好的QingTian Enclave镜像文件来启动QingTian Enclave实例。
- QingTian Enclave应用程序开发人员：开发在QingTian Enclave中运行的应用程序。在该案例中，该应用程序需要从华为OBS服务的Bucket1获取密文对象，然后调用kms-decrypt接口对密文进行解密，进行数据处理后，最后将结果输出到Bucket2。

在指定目录下，下载huawei qingtian enclave源码：

```
cd /home  
git clone https://gitee.com/HuaweiCloudDeveloper/huawei-qingtian.git
```

数据和环境准备

接下来，我们将概述一下关于数据加密、证明设置和QingTian Enclave实例创建的相关流程。

1. 安全员在华为云数据加密服务的密钥管理子服务中创建KMS密钥。详细内容，请参见[创建密钥](#)。
2. 安全员使用KMS密钥加密一段敏感数据（例如银行卡信息）。详细信息可以参考华为云数据加密服务帮助文档中API参考章节中的应用示例：[加解密小量数据](#)。
3. 安全员使用obsutil命令行工具将加密后的密文上传到华为云对象存储服务（OBS）的一个桶中。详细信息可以参考华为云对象存储服务帮助文档工具指南章节：[上传对象](#)。
4. 安全员编写并打包QingTian Enclave开发程序：制作Docker镜像，然后使用qt命令行工具将Docker镜像转换成QingTian Enclave镜像文件。可以参考QingTian Enclave镜像文件制作。并记录创建QingTian Enclave镜像文件时生成的PCR0和PCR8。
5. 安全员将PCR0和PCR8设置为IAM访问控制策略的条件键（控制kms-decrypt API）。

在IAM控制台，使用管理员权限账号创建自定义身份策略，详细操作，请参见[创建自定义策略](#)。

要配置的自定义策略内容如下：

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms::generateRandom",
        "kms:cmk:createDataKey",
        "kms:cmk:decryptData",
        "kms:cmk:decryptDataKey"
      ],
      "Condition": {
        "StringEqualsIgnoreCase": {
          "kms:RecipientAttestation/PCR0": [
            "8f2cbfb3930e59c6de5c4caff0a3f4c0457e8956bfb4556a7ca1f5f4614a741eeee39ae10447eb5baee48d49e6c1cb6c",
            "ff7ba807a385b49fc1c3346bb47215aef503dee6df22d32f733e22b90a9bc4b22424ca7de1a3537ac9608d7ebe461d67",
            "a28e765550d6ad1188860d30167b1fdb9e29c8da825543861bc76ef1e8427fac6b444ec6a1847fc2c22deae8170c2e67"
          ],
          "kms:RecipientAttestation/PCR8": [
            "a9add94b0ecbbd992bade2176370ecf3bfed2cb39b2ec547512b5174279799f2036fa0b8577bdaf503836178bd11ee2"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:cmk:encryptData",
        "kms:cmk:encryptDataKey"
      ]
    }
  ]
}
```

在自定义身份策略示例中，配置了如下参数：

- kms提供的随机数：kms::generateRandom

- 数据密钥: kms::cmk:createDataKey
- 数据解密: kms:cmk:decryptData
- 解密数据密钥: kms:cmk:decryptDataKey
- 加密数据密钥: kms:cmk:encryptDataKey
- 数据加密接口: kms:cmk:encryptData;

其中, kms:RecipientAttestation/PCR0和kms:RecipientAttestation/PCR8的条件键, 在制作QingTian Enclave镜像时确定, 且同时支持多个值。

6. 父虚拟机管理员启动父虚拟机并设置启动qt-proxy服务, 用于转发QingTian Enclave KMS网络请求, 然后使用QingTian Enclave镜像启动QingTian Enclave。其中, KMS在不同区域的终端节点可通过[地区和终端节点](#)获取。

远程证明和数据解密

下面我们将概述在QingTian Enclave应用程序的执行流程。

1. 通过qproxy服务, QingTian Enclave应用程序将密文从华为OBS桶中下载到QingTian Enclave实例中。
2. Enclave应用程序产生一对RSA公私钥 (pubKey, priKey), 用于建立与KMS服务之间的端到端数据加密 (它并不需要依赖HTTPS)。然后使用QingTian Enclave SDK调用KMS提供的支持AttestationDocument (证明文档) 作为入参的kms-decrypt API。证明文档中包括QingTian Enclave的PCR值和应用程序产生的加密公钥 (pubKey)。
3. 华为云KMS接收并验证证明文档是否由QingTianAttestation PKI签发。在kms-decrypt API的访问控制检查中, 会将证明文档中的PCR值与IAM授权策略中的PCR值进行比较, 如果匹配成功则允许调用该接口, 否则拒绝访问。
4. KMS将数据解密后, 然后用AttestationDocument提供的pubKey对数据进行重新加密后发送回QingTian Enclave应用程序。QingTian Enclave应用程序使用priKey对接收到的密文数据进行解密。

示例代码可以参考: <https://gitee.com/HuaweiCloudDeveloper/huawei-qingtian/tree/master/enclave/qt-sm-sdk-c/samples>。

19.3.2 构建 QingTian Enclave 镜像

在开发人员开发完成一个QingTian Enclave应用程序后, 还需要在一个可信赖的环境中构建QingTian Enclave镜像文件 (.eif)。该镜像文件提供了启动QingTian Enclave实例所需要的所有信息, 包括应用程序代码、运行时依赖、操作系统和文件系统等。在本节我们将说明如何创建QingTian Enclave镜像文件。

1. 制作docker源镜像

用户将开发好的enclave应用程序及其相关的执行环境打包成docker镜像。详情可见[Linux系统上QingTian Enclave应用的开发](#)。

2. 获取镜像库中的镜像

本章将使用docker仓中提供的ubuntu镜像为例。从docker中获取镜像源 (虚拟机内需要配置网络才可查询)。查询镜像源命令:

```
docker search ubuntu
```

将ubuntu镜像pull到本地:

```
docker pull ubuntu
```

镜像pull到本地后可以通过以下命令查询到:

```
docker image ls
```

如果您使用本地docker镜像，可以直接进行步骤3镜像转换。

3. 镜像转换

接下来，您需要将docker镜像转换为QingTian Enclave镜像。

- a. （可选）通过（openssl或其他工具）创建私钥（private-key.pem）和证书（server.pem）。

```
openssl ecparam -out private-key.pem -name secp384r1 -genkey
openssl req -new -key private-key.pem -out ssl.csr
openssl x509 -req -days 365 -in ssl.csr -signkey private-key.pem -out server.pem
```

说明

为保证安全性，目前仅支持椭圆曲线算法和secp384r1椭圆曲线。

- b. 将docker镜像转换为QingTian Enclave镜像。

qt make-img命令中的必要参数为docker源镜像和创建后生成的QingTian Enclave目标镜像。

```
# qt enclave make-img --docker-uri ubuntu --eif /home/docker/ubuntu.eif --private-key /home/
docker/private-key.pem --signing-certificate
/home/docker/server.pem
{
    "digest":    "SHA384",
    "PCR0":
    "b8c59692da8a5bcb739a83d15a0ceca670bd78da06cb2250ec70548f72254e674419e9888db9c036
4a9b88dd58017a62"
    "PCR8":
    "dbf4a7f9fab7f18619b5899c407081981ad6762fb9a809da78548821b5021965423181584acd7b20
1703376f1133a546"
}
```

至此，QingTian Enclave可用的EIF镜像已制作完成。您将获得一组散列PCR0和PCR8，这些散列值用作预期的Enclave度量值，它们可用于IAM授权策略中的条件键，以实现KMS API的条件访问控制。详情可见[PCR简介](#)。

19.3.3 启动 QingTian Enclave

资源隔离

启动QingTian Enclave虚拟机之前，您首先要在父虚拟机内隔离资源供QingTian Enclave虚拟机使用。隔离的资源包括cpu个数和内存大小，可以通过在虚拟机内访问修改`*/etc/qingtian/enclave/qt-enclave-env.conf`配置文件指定需要隔离的资源：

```
#1G大页
hugepage_size:1024
#内存1G.
memory_mib:1024
# cpu个数
cpu_count:2
# cpu列表
# cpu_list:2,3
```

我们建议您最好不要反复启动资源隔离服务，否则将会出现大页内存不足，导致QingTian Enclave无法正常启动或者隔离服务无法正常启动。本教程中保持默认值不变，使用1G大页，隔离2个vCPU和1G内存。确认配置文件参数之后执行以下命令：

```
systemctl restart qt-enclave-env.service
```

其中`*/etc/qingtian/enclave/qt-enclave-env.conf`配置文件中的配置项之间有约束条件，详情可见[qt-enclave-env服务介绍](#)。

启动 QingTian Enclave

在父虚拟机内，使用`qt enclave start`命令创建QingTian Enclave虚拟机，该命令中需要指定QingTian Enclave虚拟机镜像文件。在QingTian Enclave虚拟机启动后，QingTian Enclave应用程序及其依赖项会被从该镜像文件中引导到QingTian Enclave虚拟机中。这里以创建一个拥有2个vCPU，1G内存，CID为4的QingTian Enclave虚拟机为例：

```
[root@localhost ~]# qt enclave start --cpus 2 --mem 1024 --eif /home/docker/ubuntu.eif --cid 4
Started enclave with EnclaveID : 0, EnclaveCID : 4, NumberOfCPUs : 2, MemoryMiB : 1024
{
  "EnclaveID": 0,
  "EnclaveCID": 4,
  "NumberOfCPUs": 2,
  "MemoryMiB": 1024,
  "LaunchMode": "debug"
}
```

在该实例中，原镜像ubuntu中的CMD语句为/bin/bash，因此QingTian Enclave启动之后将会执行该语句，执行完成后将退出并关闭。

19.4 密码学证明

QingTian Enclave支持密码学证明。QingTian Enclave支持通过密码学证明过程来证明其身份并与外部服务建立信任。证明过程需要使用证明文档，它包含对QingTian Enclave运行环境的可信度量值。您可以使用这些度量值在外部服务中创建访问控制策略，以控制特定QingTian Enclave实例对指定操作的访问权限。

您可以通过使用QingTian Enclave SDK从QingTianHypervisor获取证明文档，该证明文档包含相关的度量值及数字签名。QingTian Enclave应用可以在向外部服务发送请求时携带该证明文档。当外部服务收到该请求时，会验证证明文档中包含的度量值是否匹配预期的度量值，以决定是否允许Enclave应用的访问请求或建立安全。

19.4.1 PCR 简介

QingTian Enclave的度量值是由标准可信度量运算得到的一组哈希值（Hashes）组成，这组哈希值保存在QingTian安全模块（QingTian Security Module, QTSM）的平台配置寄存器（Platform configuration registers, PCR）。

说明

QingTian Enclave度量值最多可支持32个PCR。QingTian系统占用index 0~15的PCR，用户的Enclave应用可使用index 16~31的PCR。

使用debug-mode启动Enclave时，不进行镜像校验。QingTian系统的index 0~15的PCR默认全为零避免打印泄漏。用户的Enclave应用可继续使用index 16~31的PCR。

系统 PCR

PCR	度量内容	备注
PCR0	QingTian Enclave镜像文件	QingTian Enclave镜像文件本身，不包括证书与签名信息。

PCR	度量内容	备注
PCR3	IAM Agency	分配给父虚拟机实例的IAM Agency的连续度量值。确保父虚拟机具有正确的IAM Agency时，证明流程才能成功。 用户通过页面设置，当前仅在父虚拟机启动时下发一次，重置后需重启虚拟机生效。
PCR4	父虚拟机Instance UUID	父虚拟机UUID的连续度量值。确保只有当父虚拟机具有特定的UUID时，证明过程才会成功。
PCR8	QingTian Enclave镜像文件签名证书	QingTian Enclave镜像文件的签名证书。

当前QingTian Enclave提供的度量值支持PCR0和PCR8，后续会进行扩展。

1. PCR0是对QingTian Enclave镜像文件的度量值，在镜像制作完成时，PCR0的值就是确定的。以下是PCR0实例：

```
EXTEND_PCR: index: 0
EXTEND_PCR: data:
0d1ae7330f437ee563178df30a7c7b7634125d31cac14f6784933db5e90080008438b38fdbb39c886ffe058
6ab099b56
EXTEND_PCR res: data:
b8c59692da8a5bcb739a83d15a0ceca670bd78da06cb2250ec70548f72254e674419e9888db9c0364a9b8
8dd58017a62
```

2. 为了进一步加强QingTian Enclave的安全策略，您可以创建IAM Agency并将其附加到父虚拟机。在KMS密钥策略的条件密钥中使用IAM Agency的SHA384哈希值作为PCR3。这样做可确保只有在具有正确IAM Agency的实例上运行的QingTian Enclave才能针对KMS密钥执行特定的KMS操作。您可以使用任何能够将字符串转换为SHA384哈希的工具生成哈希。以下是PCR3实例：

```
$IAM_AGENCY="iam::6c031a4leefc480bb60f20c003891fcd:agency:cddd"; \
python -c"import hashlib, sys; \
h=hashlib.sha384(); h.update(b'\0'*48); \
h.update('$IAM_AGENCY'.encode('utf-8')); \
print(h.hexdigest())"
```

3. PCR4基于父虚拟机UUID的SHA384计算值。因此，您可以在启动父虚拟机后生成PCR。您可以使用任何能够将字符串转换为SHA384哈希的工具生成此哈希。以下是PCR4实例：

```
$INSTANCE_ID="ecb23eec- 51d4-462f-8dbd-63bfbae7869b"; \
python -c"import hashlib, sys; \
h=hashlib.sha384(); h.update(b'\0'*48); \
h.update('$INSTANCE_ID'.encode('utf-8')); \
print(h.hexdigest())"
```

4. PCR8是对QingTian Enclave镜像文件的签名证书的度量值，用户可以选择用自己的证书和私钥对镜像文件进行签名。只有当镜像文件使用了签名证书和私钥进行签名，才会有对应的PCR8。使用PCR8可以确认是镜像是通过特定的签名证书来进行签名的，即使镜像文件改变，只要指定的签名证书不变，PCR8就不会变化。以下是PCR8实例：

```
EXTEND_PCR: index: 8
EXTEND_PCR: data:
```



```
c5b3e075e00c261e7fc364f1541067b2a42d4b793225ab10e5cfb8eaca31b3d598af9dd2e491828c2569a9
953401abcb
EXTEND_PCR res: data:
4f8b066ce5ac24150612ba9a55bbb9211f626152ada40ede160f4d7ecbfa214c2a549181f6611a3d16a12e
c88a577a01
```

19.4.2 证明文档

证明文档用于证明QingTian Enclave实例的可信度量结果。证明文档由QingTianHypervisor生成，文档内容包括PCR列表、QingTianPKI证书链、密码算法声明以及Enclave应用自定义数据。证明文档由华为云QingTian Attestation PKI（Public Key Infrastructure）签署。

QingTianHypervisor生成的证明文档以简明二进制对象表示（CBOR）进行编码，并用CBOR Object Signing and Encryption（COSE）进行签名。关于CBOR，详情可见[RFC 8949: Concise Binary Object Representation（CBOR）](#)。

关于QingTian Enclave证明文档结构，我们遵循CDDL规范（RFC 8610）描述如下：

```
AttestationDocument = {
  module_id: text,           ; 安全模块编号
  timestamp: uint .size 8,   ; 时间戳
  digest: digest,           ; 摘要算法
  pcrs: { + index => pcr },  ; PCR列表
  certificate: cert,         ; Enclave证明文档的签名证书
  cabundle: [* cert],       ; QingTianPKI证书链
  ? user_data: user_data,    ; 可选，应用相关的数据
  ? nonce: user_data,        ; 可选，不重复使用的数值
  ? pubkey: user_data,       ; 可选，应用程序相关的公钥
}

cert = bytes .size (1..4096) ; DER编码证书
user_data = bytes .size (0..4096)
pcr = bytes .size (48)       ; PCR内容
index = 0..31
digest = "SHA384"
```

证明文档中的可选参数（pubkey，user_data和nonce）可以支持QingTian Enclave与外部实体之间运行自定义（或自协商）的应用级安全协议。比如，QingTian Enclave应用可以创建一个非对称密钥对（PriKey, PubKey），并通过QingTian Enclave证明文档来提供对PubKey的可信证明，那么外部实体就可以基于该PubKey证明来运行一些自定义的可信密钥分发、可信密钥协商等应用级安全协议。

19.4.3 文档签名验证

接下来，我们将介绍证明文档的验证过程。当您从QingTianHypervisor请求证明文档时，您将会收到一个包含已签名证明文档的二进制blob。已签名的证明文档是一个由CBOR编码，COSE签名的对象。整个验证过程包括以下几个步骤：

1. 解码CBOR对象并将其映射到COSE_Sign1结构中
2. 从COSE_Sign1结构中提取证明文档
3. 验证证书文档中CA证书链的有效性
4. 验证证明文档的数字签名的有效性

证明文档由华为云QingTianAttestation PKI签署。华为云QingTian根证书可以从https://qingtian-enclave.obs.myhuaweicloud.com/huawei_qingtian-enclaves_root-G1.zip 下载获取，该压缩文件的SHA256的摘要值为：

```
99e9203a64cfb0c6495afd815051e97bea8a37895dc083d715674af64adeadfe
```


QingTianAttestation PKI根证书的有效期为30年，根证书主体（Subject）的格式如下：

```
CN=huaweicloud.qingtian-enclaves, C=CN, O=Huawei Technologies, OU=Huawei Cloud
```

COSE 与 CBOR

COSE_Sign1签名结构通常被使用在为消息进行单一签名的场景，其内容和签名的相关参数都放在受保护的header中。COSE_Sign1数据结构是一个CBOR数组，该数组包括如下字段：

```
[
  protected header;    // 被保护的header信息
  unprotected header;  // 不被保护的header信息
  payload;             // 被签名的数据，attestation doc的CBOR封装数据
  signature;           // 签名
]
```

在证明文档的上下文中，该数组示例为：

```
18(
  // COSE_Sign1 CBOR标签
  {1: -35}, // 算法: ECDS 384
  {},       // 空
  attestation doc, // 证明文档
  signature,      // 签名
)
```

验证证书

验证证书链是证书有效性验证过程中不可或缺的一部分。证明文档中的CA Bundle包含了根证书和中间证书的证书列表，并按以下顺序提供：

```
[ ROOT_CERT - INTERM_1 - INTERM_2 ... -INTERM_N ]
  0         1         2         N
```

为了验证目标证书TARGET_CERT（即证明文档中的Certificate）的有效性，对于某些证书验证工具而言，您可能需要按如下顺序构造证书验证列表：

```
[ TARGET_CERT - INTERM_N - INTERM_N-1 ... - ROOT_CERT]
```

19.4.4 结合华为云 KMS 服务

华为云KMS服务内置了对QingTian Enclave证明的支持。通过使用QingTian Enclave SDK中包含的华为云KMS API，您可以在QingTian Enclave实例中基于QingTian Enclave证明来执行华为云KMS操作，比如解密、生成随机数和加密等操作。华为云KMS服务提取来自QingTian Enclave的证明文档并根据预设的IAM授权策略对其进行访问权限控制。

比如，如下是一个IAM授权策略的举例。该授权策略允许调用KMS的解密数据或解密数据密钥功能API，但限制条件是要求请求者必须在QingTian Enclave环境中运行，且Enclave的度量值PCR0和PCR8都必须和指定的PCR值相同。

设置IAM授权策略成功导出的json信息如下：

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:cmk:decrypt",
        "kms:dek:decrypt"
      ]
    }
  ]
}
```

```
    ],
    "Resource": "*",
    "Condition": {
      "StringEqualsIgnoreCase": {
        "kms:RecipientAttestation/PCR0": [
          "c5158cb6ee9dbb0ead648c3dc80e472c85e0d67f19fb53fbd3fb94c3371aec63cdb93b80d727a7084248873b1d8e8b41"
        ],
        "kms:RecipientAttestation/PCR8": [
          "705afb1012d27f4e07a25e674e6a17dec57305e29cd412184b7bcb78d9e67f16a0cc26d8706a4fab418a5da5788bc949"
        ]
      }
    }
  }
]
```

json信息说明：

- Action：对应身份策略内容的操作。
- Resource：该身份策略可以获取的资源。
- *：表示所有资源均可获取。
- Condition：请求条件。使用QingTian Enclave时支持使用PCR0、PCR3、PCR4、PCR8的任意组合作为请求条件，示例中使用的是PCR0和PCR8。

创建用户组的操作指导，请参见：[创建用户组并授权](#)

创建自定义策略的操作指导，请参见：[创建自定义策略](#)

19.5 QingTian Enclave 应用开发

一个功能完备的QingTian Enclave应用程序至少包括如下两个部分：

1. 一个运行在父虚拟机内安全不敏感的应用程序。
2. 一个运行在Enclave环境中安全敏感的应用程序。

由于QingTian Enclave环境的独立性，QingTian Enclave环境中的应用程序和运行在父虚拟机中的应用程序间只能通过唯一的vsock通道进行通信。

19.5.1 Linux 系统上 QingTian Enclave 应用的开发

QingTian Enclave SDK

QingTian Enclave SDK由一系列开源库组成，以便您开发自己的QingTian Enclave应用程序。其中包括QingTian安全模块（QingTian Security Module，QTSM）提供的qt-sm-lib函数库。此外，SDK集成了KMS接口，该接口内置了获取证明文档及调用华为云KMS相关服务的功能。在典型使用案例里，我们描述了在QingTian Enclave调用KMS解密接口的示例。

表 19-1 接口介绍

类型	接口	接口描述
libqtsm 接口	qtsm_describe_pcr	查询指定index的PCR数据信息
	qtsm_extend_pcr	扩展指定index对应的PCR值
	qtsm_lock_pcr	锁定指定index的PCR数据信息
	qtsm_lock_pcrs	批量锁定指定index对应的PCR值
	qtsm_get_describe	获取qtsm信息
	qtsm_get_attestation	获取Attestation Doc
	qtsm_get_random	获取硬件随机数
KMS接口	kms_generate_datakey_blocking	生成新的密钥对，获取公钥与私钥
	kms_generate_datakey_blocking_with_proxy	集成qtproxy代理的密钥对获取接口
	kms_gen_random_blocking	获取随机数
	kms_gen_random_blocking_with_proxy	集成qtproxy代理的随机数获取接口
	kms_decrypt_data_blocking	解密数据
	kms_decrypt_data_blocking_with_proxy	集成qtproxy代理的解密数据接口

源码可以在开源仓库<https://gitee.com/HuaweiCloudDeveloper/huawei-qingtian/tree/master/enclave>免费获取，您可以基于测试示例开发自己的QingTian Enclave应用程序。

Vsock 通信示例

本节主要通过vsock示例来介绍如何在Linux环境下开发QingTian Enclave应用程序。本节中提供的vsock程序只支持在Linux环境下运行。

通过该vsock程序，可以帮助开发者了解到父虚拟机和QingTian Enclave间如何进行消息传递从而实现双方交互。该vsock程序带有Server和Client参数，通过指定该参数可以指定父虚拟机或者QingTian Enclave虚拟机扮演相应角色。在该vsock程序中，客户端程序会发送一段简单的文本信息通过vsock通道传递给服务端程序，同时服务端程序会监听相应的vsock通道，一旦收到来自客户端的消息后，会将其收到的消息打印在终端界面上。

在下面介绍中，我们将说明如何让QingTian Enclave扮演服务端等待并接收来自客户端父虚拟机的hello world信息：

1. 编写一个SocketCommunication.py程序：
- ```
#!/usr/local/env python3
import argparse
import socket
```

```
import sys

CID_DEFAULT = 3
PORT_DEFAULT = 9999
TIMEOUT = 5
BLACKLOG_DEFAULT = 5

class Client:
 def __init__(self, cid, port):
 self.clientAddr = (cid, port)
 self.connect()

 def connect(self):
 self.socket = socket.socket(socket.AF_VSOCK, socket.SOCK_STREAM)
 self.socket.settimeout(TIMEOUT)
 print("connecting to the server")
 try:
 self.socket.connect(self.clientAddr)
 except socket.error:
 print("client's socket connection err")
 sys.exit(1)

 def send(self, msg):
 print("client sends hello to the server")
 self.socket.sendall(msg)

 def disconnect(self):
 self.socket.close()

 def receiveData(self):
 while True:
 try:
 message = self.socket.recv().decode()
 except (socket.error, UnicodeDecodeError):
 break
 if message:
 print(message, end = " ", flush = True)
 print()

def clientHandler(args):
 client = Client(args.cid, args.port)
 message = "Hello world"
 client.send(message.encode())
 client.disconnect()

class Server:
 def __init__(self, port):
 self.socket = socket.socket(socket.AF_VSOCK, socket.SOCK_STREAM)
 self.serverAddr = (socket.VMADDR_CID_ANY, port)
 self.socket.bind(self.serverAddr)
 self.socket.listen(BLACKLOG_DEFAULT)

 def receiveData(self):
 while True:
 print("waiting for a connection")
 (conn, clientAddr) = self.socket.accept()
 try:
 print("connection from ", clientAddr)
 while True:
 try:
 data = conn.recv(256).decode()
 except (socket.error, UnicodeDecodeError):
 break
 if data:
 print("data: ", data)
 else:
 print("connection close")
 break
 finally:
 pass
```

```
conn.close()

def serverHandler(args):
 server = Server(args.port)
 server.receiveData()

def main():
 parser = argparse.ArgumentParser(description = "Hello world demo", prog='SocketCommunication')
 subparsers = parser.add_subparsers(description = "Communication roles")
 parserClient = subparsers.add_parser("Client", description = "Client",
 help = "Communicate with server using a given cid and port.")
 parserClient.add_argument("-c", "--cid", default = CID_DEFAULT, type = int, help = "Client's Cid")
 parserClient.add_argument("-p", "--port", default = PORT_DEFAULT, type = int, help = "Client's
port")
 parserClient.set_defaults(func = clientHandler)
 parserServer = subparsers.add_parser("Server", description = "Server", help = "Listen on a given
port")
 parserServer.add_argument("-p", "--port", default = PORT_DEFAULT, type = int, help = "Server's
Port")
 parserServer.set_defaults(func = serverHandler)
 if len(sys.argv) < 2:
 parser.print_usage()
 sys.exit(1)
 args = parser.parse_args()
 args.func(args)

if __name__ == "__main__":
 main()
```

2. 创建一个Dockerfile文件，内容如下：

```
#start the Docker image from ubuntu
FROM ubuntu:22.04
WORKDIR /home/builder
COPY vsocket example
COPY . vsocket
install relative dependencies
RUN apt-get update && \
 apt-get install python3 -y && \
 apt-get install gcc -y && \
 apt-get install gawk -y
Launch a client
CMD ["python3", "/home/builder/vsocket/SocketCommunication.py", "Server", "-p 9999"]
```

3. 构建docker镜像：

```
sudo docker build -t vsock-sample-client -f Dockerfile .
```

4. 将docker镜像转化为QingTian Enclave镜像：

```
qt enclave make-img --docker-uri vsock-sample-client --eif vsock_sample.eif
```

5. 使用vsock\_sample.eif以debug模式启动QingTian Enclave：

```
qt enclave start --cpus 2 --mem 4096 --eif vsock_sample.eif --debug-mode --cid 4
```

然后使用qt enclave console命令查看QingTian Enclave内只读终端输出：

```
qt enclave console --enclave-id 0
waiting for a connection
```

6. 然后另起一个父虚拟机终端，启动客户端程序：

```
python3 SocketCommunication.py Client -c 4 -p 9999
```

7. 当服务端程序收到来自vsock的消息后，会打印如下消息到终端上：

```
connection from (3, 4180219645)
data: Hello world
connection close
waiting for a connection
```

### KMS 接口调用和权限配置示例

本节主要基于开源示例代码来介绍如何在QingTian Enclave应用程序中调用KMS接口并配置权限。本节中提供的示例程序只支持在Linux环境下运行。

在配置前，请先购买一台C7t规格的弹性云服务器作为QingTian Enclave父虚拟机并完成相关配置，详细内容，请参见[快速入门](#)。

- 从gitee仓库下载huawei-qingtian-enclave代码。  
本示例以qtsm-java-sdk为例进行介绍。
  - 执行以下命令，下载huawei-qingtian-enclave代码。

```
cd /home
git clone https://gitee.com/heathjay/huawei-qingtian.git
```

执行以下命令，切到newjay-java-sdk分支。

```
cd /home/huawei-qingtian
git checkout newjay-java-sdk
```
- 根据用例，获取相关参数。  
测试可参考：<https://gitee.com/HuaweiCloudDeveloper/huawei-qingtian/pulls/21/files>。  
[表19-2](#)中获取的参数需填入测试文件文件中。

表 19-2 KMS 接口参数

| 参数名称       | 含义                | 获取方式                               |
|------------|-------------------|------------------------------------|
| ak         | Access Key ID     | 详细内容，请参见 <a href="#">API签名指南</a> 。 |
| sk         | Secret Access Key |                                    |
| project_id | 项目ID              | 获取方法请参见 <a href="#">获取项目ID</a> 。   |
| key_id     | KMS中的keyID        | 无                                  |
| host       | KMS endpoint      | 无                                  |

- 通过IAM创建自定义身份策略。  
使用管理员权限账号创建自定义身份策略“enclave-test-kms-api”，详细操作，请参见[创建自定义策略](#)。  
需要配置的自定义策略内容如下：

```
{
 "Version": "5.0",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "kms::generateRandom",
 "kms:cmk:createDataKey",
 "kms:cmk:decryptData",
 "kms:cmk:decryptDataKey"
],
 "Condition": {
 "StringEqualsIgnoreCase": {
 "kms:RecipientAttestation/PCR0": [
```

```
"8f2cbfb3930e59c6de5c4caff0a3f4c0457e8956bfb4556a7ca1f5f4614a741eeee39ae10447eb5baee48d49e6c1cb6c",

"ff7ba807a385b49fc1c3346bb47215aef503dee6df22d32f733e22b90a9bc4b22424ca7de1a3537ac9608d7ebe461d67",

"a28e765550d6ad1188860d30167b1fdb9e29c8da825543861bc76ef1e8427fac6b444ec6a1847fc2c22dae8170c2e67"
],
 "kms:RecipientAttestation/PCR8": [

"a9add94b0ecbbd992baded2176370ecf3bfed2cb39b2ec547512b5174279799f2036fa0b8577bdaf503836178bd11ee2"
]
}
}
},
{
 "Effect": "Allow",
 "Action": [
 "kms:cmk:encryptData",
 "kms:cmk:encryptDataKey"
]
}
]
```

其中，PCR0和PCR8的值需要在完成QingTian Enclave镜像制作后，进行配置。

4. 创建IAM用户并授予权限。
- a. 在IAM控制台，单击“体验新版控制台”。

b. 在“用户”页面创建IAM用户“enclave-test-kms-uers”并授予“enclave-test-kms-api”权限。

图 19-2 创建 IAM 用户（1）



图 19-3 创建 IAM 用户（2）



图 19-4 为用户授权



- c. 获取“enclave-test-kms-uers”用户的AK、SK。  
在用户的“安全设置”页签可新增并下载访问密钥，请参见[创建IAM用户的访问密钥](#)。  
从下载的访问密钥文件中，可获取用户的AK、SK取值。
- d. 将AK、SK赋值到测试程序对应参数。  
测试程序：/home/huawei-qingtian/enclave/qt-sm-sdk-java/kms-cms-java/com/huawei/src/test/TestKmsCmsProxy.java

图 19-5 赋值 AK、SK

```
9
10 public class TestKmsCmsProxy {
11 public static final String TAG = "TestCmsKmsProxy";
12 public static void main(String[] args) {
13 /* cid is a fixed number of 3, port should be consistent with the port in the qt-
14 proxy.conf file,
15 * and it is the configuration for the vsock channel, which facilitates communica-
16 tion between the
17 * enclave and the host.
18 */
19 int vsockCid = 3;
20 int vsockPort = 8000;
21 /* The security server needs to create a new user with permissions of encryption,
22 please refer to
23 * the user manual on the website of the Huawei Cloud to get this user's ak sk.
24 */
25 // String ak = System.getenv("HUAWEICLOUD_SDK_AK");
26 // String sk = "xxxxxxxxxxxxxx";
27 String ak = "xxxxxxxxxxxxxx";
28 String sk = "xxxxxxxxxxxxxx";
29 /* KMS tenant-side domain name */
30 // String host = System.getenv("HUAWEICLOUD_SDK_HOST");
31 String host = "kms.xxx.myhuaweicloud.com";
32 }
33 }
```

- 5. 获取KMS的Endpoint节点。
  - a. 通过[地区和终端节点](#)获取KMS在不同区域的终端节点。
  - b. 将KMS的Endpoint赋值到文件huawei-qingtian/enclave/qt-sm-sdk-java/kms-cms-java/com/huawei/src/test/TestKmsCmsProxy.java中对应的host字符串变量：

图 19-6 赋值 Endpoint

```
17 int vsockCid = 3;
18 int vsockPort = 8000;
19 /* The security server needs to create a new user with permissions of encryption,
20 please refer to
21 * the user manual on the website of the Huawei Cloud to get this user's ak sk.
22 */
23 // String ak = System.getenv("HUAWEICLOUD_SDK_AK");
24 // String sk = "xxxxxxxxxxxxxx";
25 String ak = "xxxxxxxxxxxxxx";
26 String sk = "xxxxxxxxxxxxxx";
27 /* KMS tenant-side domain name */
28 // String host = System.getenv("HUAWEICLOUD_SDK_HOST");
29 String host = "kms.xxx.myhuaweicloud.com";
30 String host = "kms.xxx.myhuaweicloud.com";
31 /* The security officer needs to purchase an elastic cloud server with the enclav
```



## 6. 获取项目ID。

- 通过控制台获取项目ID，详细操作，请参见[获取项目ID](#)。
- 将获取的项目ID赋值到文件/home/huawei-qingtian/enclave/qtsm-sdk-java/kms-cms-java/com/huawei/src/test/TestKmsCmsProxy.java中对应的uriPrefix字符串变量：

图 19-7 赋值项目 ID

```
32 /* The security officer needs to purchase an elastic cloud server with the enclav
 e service.
33 * The security officer needs to go to the unified identity authentication servic
 e center of Huawei Cloud
34 * to create a new project.,to get project ID, then uriPrefix is /v1.0/{project I
 D}/kms/
35 */
36 // String uriPrefix = System.getenv("HUAWEICLOUD_SDK_URI");
37 //String uriPrefix = "/v1.0/{project ID}/kms/";
38 String uriPrefix = "/v1.0/{project ID}/kms/";
```

## 7. 获取密钥ID。

- 通过数据加密控制台，创建密钥并获取ID。详细操作，请参见[创建自定义密钥](#)。
- 将获取的密钥ID赋值到文件/home/huawei-qingtian/enclave/qtsm-sdk-java/kms-cms-java/com/huawei/src/test/TestKmsCmsProxy.java中对应的uriPrefix字符串变量：

图 19-8 赋值密钥 ID

```
50 System.out.println("Failed to get environment variables.");
51 System.exit(1);
52 }
53 SigParams params = new SigParams(ak, sk, host, uriPrefix);
54 /* Create a new key in the kms service for data encryption and obtain the k
 y ID
55 */
56 //String keyid = System.getenv("HUAWEICLOUD_SDK_KEY");
57 String keyid = "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX";
58 KeyIdHandle keyIdHandle = new KeyIdHandle(keyid, keyid.length());
59 int rndLen = 256;
60 int datakey_length = 512; // plainkey_len = 512 / 8
```

- 使用密钥加密一段明文，例如“hello world! ”，详细操作，请参见[使用自定义密钥在线加解密小数据](#)。
- 将加密后的密文填写到文件/home/huawei-qingtian/enclave/qtsm-sdk-java/kms-cms-java/com/huawei/src/test/TestKmsCmsProxy.java中对应的dataInputStr中：

图 19-9 填写密文

```
113 // String dataInputStr = "AgB4AKTnZ65G0a++oGmcbPUsFDv6zte5W7" +
114 // "uJVX8nuolXzcNBW8IrkHu1/+fktAVEhfcv" +
115 // "zkUUES53yUsJSxdXmE/CQ9YzubwciuYojo" +
116 // "apgPIWS40TzjQwZGE4ZD0tZjM2NS00ODI5" +
117 // "LWJhYmEt0TU0Y2M5ODAS0DQxAAAAAFaRji" +
118 // "0PS075Mjh1DhcvIWE+I+MZ5CqvqycJXND" +
119 // "mfBk"; /* hello world! */
120 String dataInputStr = "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX";
121 try {
122 /* call kms_decrypt_data api */
123 ReturnChars plaintext = LibCmsKmsProxyNative.kmsDecryptDataBlockingWithProxy(
 params, keyIdHandle, dataInputStr, vsockCid, vsockPort, data_out_len);
124 if (plaintext.getRc() != KMS_SUCCESS.getValue()) {
125 System.out.println(funTAG + "DecryptData fail error code is " + plaintext
 .getRc());
```

- 进入到/home/huawei-qingtian/enclave/qtsm-sdk-java/kms-cms-java/scripts目录，执行sh build\_image.sh脚本构建QingTian Enclave镜像。

图 19-10 执行脚本

[illegible]

在该目录下有文件kms-demo.eif，包含pcr0和pcr8的值。

9. 生成镜像签名密钥和公钥。

```
openssl ecparam -out private-key.pem -name secp384r1 -genkey
openssl req -new -key private-key.pem -out ssl.csr
openssl x509 -re1 -days 365 -in ssl.csr -signkey private-key.pem -out server.pem
```

10. 启动proxy工具。

```
/usr/local/bin/qingtian/enclave/qt_proxy -l 8000 -a kms.ap-southeast-3.myhuaweicloud.com -p 443 &
```

11. 使用nc-vsock工具登录Enclave，进行调试。

- a. 由于该用例的QingTian Enclave中启动了一个vsock的服务端（监听9999端口），所以可以从QingTian Enclave父虚拟机内通过vsock客户端登录到Enclave进行调试。

[huawei-qingtian/enclave/qtsm-sdk-java/kms-cms-java/scripts/build\\_kms\\_demo.sh](https://gitee.com/huawei-qingtian/enclave/qtsm-sdk-java/kms-cms-java/scripts/build_kms_demo.sh)

- b. 使用nc-vsock进入Enclave。

```
/home/huawei-qingtian/nc-vsock/nc-vsock 4 9999
```

**图 19-11 进入 Enclave**

```
[root@ecs-6b79 scripts]# /root/huawei-qingtian/nc-vsock/nc-vsock 4 9999
sh: 0: can't access tty; job control turned off
#
```

- c. 在enclave中执行如下命令:

```
cd /home/builder/enclave/qtsm-sdk-java/kms-cms-java/target
We can perform it manually
java -cp ../lib/lombok-1.18.26.jar../lib/junit-4.13.1.jar -Djava.library.path=../lib
com.huawei.src.test.TestKmsCmsProxy
```

图 19-12 报错信息

```
* Connection #0 to host kms.ap-southeast-3.mhyaueaicloud.com left intact
HTTP status: 403
KMS response content:
{"error":{"error_msg":"The user role has no permission to access the interface. User: iam::c90494f3fa3a44cf95607da97fae75b1:user:enclave-test-kms-users is not authorized to perform: kms:cmk:createDataKey on resource: kms:ap-southeast-3:c90494f3fa3a44cf95607da97fae75b1:keyId:a64d0c3d-4a53-4a4c-b0f6-b88f35f1f32a because no identity-based policy allows the kms:cmk:createDataKey action"},"encoded_authorization_message":"EGShcClz3bV0aGvhC30TMxogYzkwNDk0ZjNmYnY1NDIyZjZkLnk1NjA2ZGE5N2ZhZTcyYjEgogYQpIdiOTMwfnJkNmHgg==.ewZcWbRheOE4WuQa30xCSIFfYa7cTcAq0fVIdyaECdwy900nMPdJ3C8d0Th7Vp0BbQq3DuJ3pe0X7Id0b52VyK2ZKnQNFx4bZ4L3oX05vMPaexmECmtDjCi0LE8gF0iUy/Au1p4EhJhR27dKkwwXlFtIFJBVOBCLLT4Ce/7LVmJpK3SL/E5DaadhLlBf8hLVDOEppjUJC4roVWS0c0g0fWJsh3c0fIT1xAXBvdvr3QJGXHeB9i1LnR4CmjDksnnw7B9W9YUjz9TMgtqPwIzgHGANGC+Dur/irdGt5mVCRBTBj1mIfqfa2hymbG6dH4lKMeLR0qbHgm+AK8U9rVf6Gh0cANDHsK1yZt/0SHemoVXRGFDoTUmHPk90MBV1R80uAR23r4xZ49Wgh3dJ4LLnCA68c6R4E62/6P/kqcbv1QWVTS0Shnc48/H40k191z7u2wmxmNpV1P8bNkR+MnJ1G6vMqZxN+0i1z0lANV3E8Gm
```

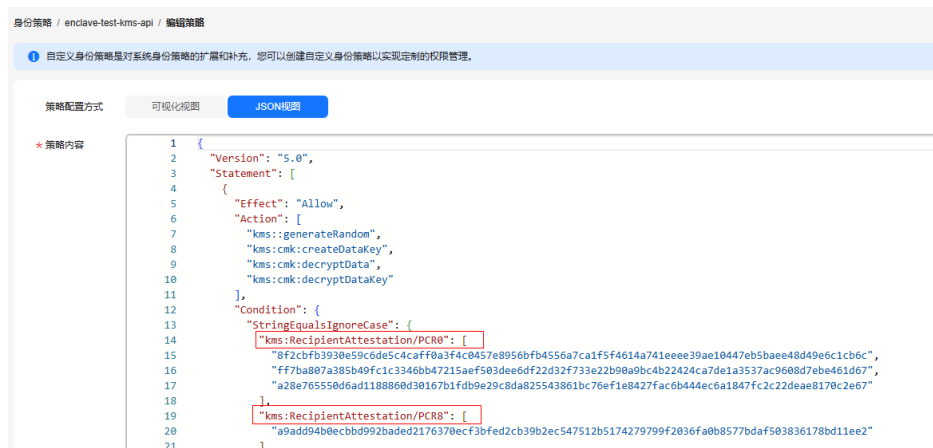
执行命令后,

- 若发现该用户无权限，如**图19-12**所示。需根据Enclave镜像的PCR0和PCR8修改自定义策略策略，执行步骤**11.d**

- 若执行成功，执行步骤。
- d. （可选）修改自定义策略，大概30秒~90秒生效。

执行命令后，若发现该用户无权限，如图19-12所示。需根据Enclave镜像的PCR0和PCR8修改自定义策略策略。

图 19-13 修改自定义策略



- e. 在enclave中重新执行如下命令，调试KMS接口：  
cd /home/builder/enclave/qtsm-sdk-java/kms-cms-java/target  
# We can perform it manually  
java -cp ../lib/lombok-1.18.26.jar:/lib/junit-4.13.1.jar -Djava.library.path=../lib  
com.huawei.src.test.TestKmsCmsProxy
- f. KMS接口调试成功，查看调试结果。

图 19-14 解密接口

```
TestCmsKmsProxy [testKmsDecryptData] after native kmsDecryptDataBlocking data_output length is 1000
hello world!
```

图 19-15 数据密钥接口

```
key_id is:
a64c0d3c-4a53-4a4c-b0f6-b88f3f51f32a
len of plain_datakey is 512
plain_datakey is:
e6bcd1de9ba14ddac256838dc4c085a092316c8e06a6807f1c2beeb5f08d6f2f4fcbec54e644a375e2b26a0813587
18c2c4ca8b377397354e6082d52766408d1
len of cipher_datakey is 376
cipher_datakey is:
303530303834303037633535373265303437316436326432623132666338393430353939383339646434613535316
63430376461396262383323766656665343133653439316632663431396231373535666564646462666536393539
33383733326230633563383663386431303531653733636332323138343035353038303736316130366435396666
43838653963666334613862643332373063663537326266396433376164623464613234323739303262636263434
383234393437363133363334363333303634333336333264333436313335333332643334363133343633326436323
330363633363264363233383338363633333636333533313636333333236313030303030303030313431333313231
313130306630653064306330623061303930383037303630353034303330323031363663336163376131633134346
638373265303638336435323639656639633065313935623032663062386635343462393261303033373839323737
66363532
unix socket listening...
```

图 19-16 随机数接口

```
len of rnd_data is 32
random data is:
38 12 77 b5 ae 2b c0 47 2e c5 c4 7e d4 7b e7 b6 5b 9c 80 1f 01 d5 fe ac 6a f1 60 11 2c TestCm
sKmsProxy [testKmsGenRandom]the length of random data is 32
TestCmsKmsProxy [testKmsGenRandom]the randomData is:
381277b5ae2bc0472ec5c47ed47be7b65b9c801f01d5feac6af160112cd23389
d2 33 89
```

## 19.5.2 QingTian Enclave 网络代理工具

### QingTian Enclave 网络代理工具（qproxy）概述

qproxy（QingTian Enclave proxy）是QingTian Enclave的网络代理工具。借助此工具，您可以无需任何改动，直接将部署在基于QingTian架构虚拟机中的网络业务移植到QingTian Enclave中，实现传统网络业务的无感迁移。

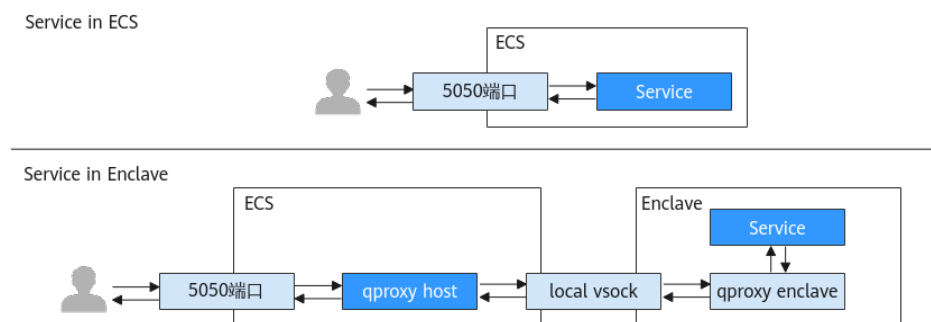
qproxy是一个可执行的二进制文件，需要在父虚拟机和QingTian Enclave中通过不同的命令运行：

- 在父虚拟机中，通过执行“`/path/to/qproxy host --config=/path/to/config_qproxy.toml <cid>`”命令启用qproxy。
- 在QingTian Enclave中，通过执行“`/path/to/qproxy enclave --config=/path/to/config_qproxy.toml`”命令启用qproxy。

以一个简单的网络服务为例，网络服务直接部署在虚拟机中，负责处理来自最终用户的请求。最终用户通过该服务暴露的端口，发起网络请求，等待服务响应。在将该网络服务迁移至QingTian Enclave之后，通过qproxy代理，可以提供和原本网络服务相同的 service。

使用同一个qproxy二进制文件，通过`qlog host`和`qlog enclave`命令，使其分别运行在父虚拟机和QingTian Enclave中，两者会建立基于local vsock的通信链路。父虚拟机中的qproxy组件会监听5050端口，接收用户请求，并通过local vsock将收到的请求转发给QingTian Enclave中的qproxy组件。该组件会将请求发送到QingTian Enclave中监听的5050端口。网络服务处理完成之后，响应数据会原路返回。

图 19-17 网络服务无感迁移至 QingTian Enclave



本文介绍qproxy的操作步骤。

### 前提条件

- 获取qproxy源码。  
克隆QingTian Enclave代码仓。  

```
git clone https://gitee.com/HuaweiCloudDeveloper/huawei-qingtian.git
```
- 获取cargo工具链。
  - 执行以下命令安装rustup。  

```
curl --proto 'https' --tlsv1.2 -sSf https://sh.rustup.rs | sh
```
  - 安装完成后执行以下命令加载rustup。  

```
source $HOME/.cargo/env
```

- c. 执行以下命令验证rustc和cargo安装成功。  
rustc -V  
cargo -V

3. qproxy的前置依赖。

表 19-3 前置依赖

| 依赖项                | 最低测试版本 |
|--------------------|--------|
| cargo              | 1.77.0 |
| libcbor            | 0.10.2 |
| libssl (libcrypto) | 3.0.0  |
| libcurl            | 4.0.0  |

4. QingTian Enclave的环境准备。

a. 安装qt CLI工具和其他必要rpm包。  
b. 安装Docker。  
c. 安装python3以及几个必要的python module : docker和knack。  
详细内容，请参考[快速入门](#)和[安装qt CLI](#)。

操作步骤

步骤1 构建qproxy。

生成的qproxy程序在目录qingtian-tools/qproxy/target/release下。

```
cargo build --release
```

步骤2 创建工作目录。

新建工作目录workspace，将qproxy程序拷贝到workspace下，后续创建的文件都放在workspace中。

```
mkdir -p /home/workspace
cp ./qproxy /home/workspace/
```

步骤3 配置config\_qproxy.toml。

在workspace目录中创建config\_qproxy.toml文件，内容如下：

```
[[inbound_connections]]
host_port = 5050
enclave_port = 5050
vsock_port = 9995

[[inbound_connections]]
host_port = 5443
enclave_port = 5443
vsock_port = 9994

[log_location]
host_log = "host.log" # qproxy host log name, e.g./var/log/qproxy/host.log
enclave_log = "enclave.log" # qproxy enclave log name, e.g./var/log/qproxy/enclave.log
log_level = "info" # qproxy logger level, e.g. "off", "info", "warn", "error", "debug", "trace"
host_log_dir = "/var/log/qproxy" # qproxy host log dir, and its default value is "/var/log/qproxy"
enclave_log_dir = "/var/log/qproxy" # qproxy enclave log dir, and its default value is "/var/log/qproxy"
```

#### 步骤4 制作含qproxy的QingTian Enclave镜像。

1. 在workspace目录中创建http请求测试脚本app.sh:

```
#!/bin/bash

PORT=5050

while true; do
 echo -e "HTTP/1.1 200 OK\nContent-Type: text/plain\n\nHello world!" | nc -l 127.0.0.1 $PORT
done
```

2. 赋予app.sh执行权限，在workspace目录中执行以下命令:

```
chmod +x app.sh
```

3. 在workspace目录中创建start.sh脚本:

```
#!/bin/bash
ip link set lo up
/root/qproxy enclave --config=/root/config_qproxy.toml &
/root/app.sh
```

4. 赋予start.sh执行权限，在workspace目录中执行以下命令:

```
chmod +x start.sh
```

5. 在workspace目录中创建Dockerfile文件:

```
FROM ubuntu:22.04
COPY ./qproxy /root/qproxy
COPY ./config_qproxy.toml /root/config_qproxy.toml
COPY ./start.sh /root/start.sh
COPY ./app.sh /root/app.sh
RUN apt-get update && \
 apt-get install -y netcat-openbsd && \
 apt-get install -y iproute2
CMD "/root/start.sh"
```

6. 制作docker镜像，在workspace目录中运行以下命令:

```
docker build -f Dockerfile -t test_qproxy_enclave .
```

7. 制作QingTian Enclave镜像，在workspace目录中运行以下命令:

```
qt enclave make-img --docker-uri test_qproxy_enclave --eif test_qproxy_enclave.eif
```

#### 步骤5 启动qproxy。

1. 启动一台QingTian Enclave，在workspace目录中运行以下命令:

```
qt enclave start --cpus 2 --mem 1024 --cid 4 --eif test_qproxy_enclave.eif
```

2. 启动父虚拟机中的qproxy，在workspace目录中运行以下命令:

```
./qproxy host --config=./config_qproxy.toml 4 &
```

3. 父虚拟机中执行curl命令:

```
curl localhost:5050
```

可以看到终端输出"Hello world!"。

#### 步骤6 qproxy环境变量设置。

qproxy包含两分子命令，一部分在QingTian Enclave ( qproxy enclave ) 中运行，另一部分在父虚拟机 ( qproxy host ) 中运行。

通过设置环境变量RUST\_LOG可以控制二进制文件的日志输出信息等级。

- 设置RUST\_LOG=OFF，日志信息会全部关闭不显示。
- 设置RUST\_LOG=info，日志信息会显示info，warn和error三个级别的信息。
- 默认情况下，只会显示warn和error两个级别的日志信息。
- 可以通过查看[EnvFilter文档](#)获取更多信息。

----结束

## qproxy 帮助信息

### qproxy help

```
$ qproxy --help
Usage: qproxy <COMMAND>

Commands:
 host The part of qproxy that runs outside the enclave
 enclave The part of qproxy that runs inside the enclave
 check-config Check the qproxy configuration file
 help Print this message or the help of the given subcommand(s)

Options:
 -h, --help Print help
 -V, --version Print version
```

### qproxy enclave help

```
$ qproxy enclave --help
The part of qproxy that runs inside the enclave

Usage: qproxy enclave [OPTIONS]

Options:
 --parent-cid <PARENT_CID>
 The CID of the parent VM of this enclave

 [env: QPROXY_PARENT_CID=]
 [default: 3]

 --config <CONFIG>
 Path to the configuration file

 -t, --threads <THREADS>
 Number of threads the async runtime is allowed to use

 [env: TOKIO_WORKER_THREADS=]

 --control-port <CONTROL_PORT>
 The port where to listen for control messages from the enclave

 Leave at default value unless you know what you are doing

 [env: QPROXY_CONTROL_PORT=]
 [default: 6666]
 [0..=65535]

 -h, --help
 Print help (see a summary with '-h')
```

### qproxy host help

```
$ qproxy host --help
The part of qproxy that runs outside the enclave

Usage: qproxy host [OPTIONS] <CID>

Arguments:
 <CID>
 The CID of the enclave

 [env: QPROXY_LISTEN_CID=]

Options:
 --config <CONFIG>
 Path to the configuration file

 -t, --threads <THREADS>
```

```
Number of threads the async runtime is allowed to use

[env: TOKIO_WORKER_THREADS=]

--ipv4
 Only resolve IPv4 addresses

--ipv6
 Only resolve IPv6 addresses

--control-port <CONTROL_PORT>
 The port where to listen for control messages from the enclave

 Leave at default value unless you know what you are doing

[env: QPROXY_CONTROL_PORT=]
[default: 6666]
[0..=65535]

-h, --help
 Print help (see a summary with '-h')
```

配置信息（Config）

配置参数解释

- outbound\_connections: 配置转发QingTian Enclave外发流量到外部特定服务（hostname/IP）及其端口。
- inbound\_connections: 配置转发父虚拟机指定端口收到的流量到QingTian Enclave中。

表 19-4 配置参数解释

| Bound                | Variable     | Type   | Description                                                                                |
|----------------------|--------------|--------|--------------------------------------------------------------------------------------------|
| outbound_connections | hostname     | String | 用于转发流量的主机名（hostname），可以是IP地址，例如：hostname = "api.myservice.com"。                            |
|                      | vssock_port  | u32    | QingTian Enclave内vssock要使用的端口，必须唯一，并且不能和qproxy端口冲突。                                        |
|                      | tcp_port     | u32    | 服务器转发流量的端口（将连接到hostname:port），不能和qproxy端口冲突（默认是8080）。                                      |
| inbound_connections  | host_port    | u32    | 主机端（host）qproxy将会监听的端口，如host_port = 80，主机端qproxy将会监听0.0.0.0:80。                            |
|                      | enclave_port | u32    | QingTian Enclave端qproxy将会监听的端口，如enclave_port = 80，QingTian Enclave端qproxy将会监听127.0.0.1:80。 |
|                      | vssock_port  | u32    | QingTian Enclave内vssock要使用的端口，必须唯一，并且不能和qproxy端口冲突。                                        |

日志文件配置



表 19-5 日志文件配置

| Variable        | Type   | Description                                                                                                   |
|-----------------|--------|---------------------------------------------------------------------------------------------------------------|
| host_log        | String | qproxy在主机端（ host ）日志文件名称, 例如：<br>host_log = "host.log"表示主机端（ host ）qproxy日志文件名为host.log。                      |
| enclave_log     | String | qproxy在QingTian Enclave端日志文件名称, 例如：<br>enclave_log = "enclave.log"表示QingTian Enclave中qproxy日志文件名为enclave.log。 |
| log_level       | String | qproxy日志级别, 例如：log_level = "info"表示显示信息，警告和错误。全部级别有 "off", "info", "warn", "error", "debug", "trace"。         |
| host_log_dir    | String | qproxy在主机端（ host ）日志目录，默认是<br>"/var/log/qproxy"                                                               |
| enclave_log_dir | String | qproxy在QingTian Enclave端日志目录，默认是<br>"/var/log/qproxy"                                                         |

配置文件参考

```
[[outbound_connections]]
hostname = "api.myservice.com"
vsock_port = 7777
tcp_port = 443

[[outbound_connections]]
hostname = "another.api.com"
vsock_port = 7778
tcp_port = 5555

[[inbound_connections]]
host_port = 80
enclave_port = 80
vsock_port = 9000

[[inbound_connections]]
host_port = 443
enclave_port = 443
vsock_port = 9001

[log_location]
host_log = "host.log"
enclave_log = "enclave.log"
log_level = "info"
host_log_dir = "/var/log/qproxy"
enclave_log_dir = "/var/log/qproxy"
```

19.5.3 QingTian Enclave 日志转发工具

QingTian Enclave 日志转发工具（qlog）概述

qlog（QingTian Enclave log）是QingTian Enclave的运维工具。QingTian Enclave是运行在QingTian架构虚拟机中完全隔离的子虚拟机，即使是root用户也不能直接通过ssh登入。因此，为了方便运维人员监控运行在QingTian Enclave中的业务和定位问题，我们推出了qlog工具。qlog可以收集QingTian Enclave虚拟机中指定的日志文件

和资源使用情况，并将结果发送到父虚拟机中。目前qlog支持收集QingTian Enclave中的资源使用情况包括CPU使用率和内存使用率。

qlog是一个可执行二进制文件，需要在父虚拟机中和QingTian Enclave中通过不同的命令运行：

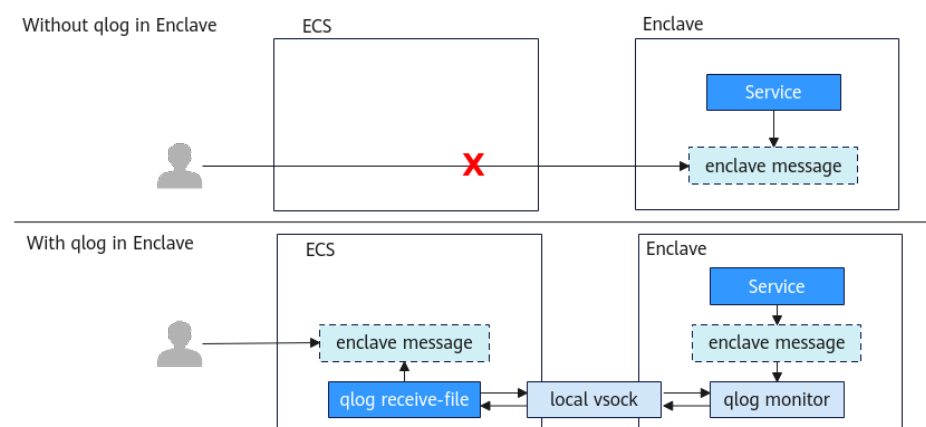
- 在父虚拟机中，通过执行“`/path/to/qlog receive-file <cid>/path/to/config_qlog.toml`”命令启用qlog。
- 在QingTian Enclave中，通过执行“`/path/to/qlog monitor /path/to/config_qlog.toml`”命令启用qlog。

传统虚拟机中业务的日志会直接存储在类似“`/var/log/service.log`”的目录文件当中。

在将业务移植到QingTian Enclave中之后，通过qlog工具，可以将上述日志文件（“`/var/log/service.log`”）导出到父虚拟机当中。

使用同一个qlog二进制文件，通过**qlog receive-file**和**qlog monitor**命令，使其分别运行在父虚拟机和QingTian Enclave中，两者会建立基于local vsock的通信链路。运行在QingTian Enclave中的qlog组件会收集指定的业务日志或QingTian Enclave的资源使用情况，将收集到的数据发送给父虚拟机中的qlog组件。父虚拟机中的qlog组件再将接收到的数据储存到指定的文件中，如“`/var/log/qlog/service.log`”。

图 19-18 网络服务无感迁移至 QingTian Enclave



本文介绍qlog的操作步骤。

## 前提条件

1. 获取qlog程序。  
克隆QingTian Enclave代码仓。  

```
git clone https://gitee.com/HuaweiCloudDeveloper/huawei-qingtian.git
```
2. 获取cargo工具链。
  - a. 执行下述命令安装rustup  

```
curl --proto 'https' --tlsv1.2 -sSf https://sh.rustup.rs | sh
```
  - b. 安装完成后执行下述命令加载rustup  

```
source $HOME/.cargo/env
```
  - c. 执行下述命令验证rustc和cargo安装成功  

```
rustc -V
cargo -V
```

## 3. qlog的前置依赖。

表 19-6 前置依赖

| 依赖项   | 最低测试版本 |
|-------|--------|
| glibc | 2.34   |
| cargo | 1.77.0 |

## 4. QingTian Enclave的环境准备。

- 安装qt CLI工具和其他必要rpm包。
- 安装Docker。
- 安装python3以及几个必要的python module : docker和knack。

详细内容，请参考[快速入门](#)和[安装qt CLI](#)。

## 操作步骤

### 步骤1 构建qlog。

进入qingtian-tools/qlog目录中，执行cargo命令：

```
cargo build --release
```

生成的qlog程序在目录qingtian-tools/qlog/target/release下。

### 步骤2 创建工作目录。

新建工作目录workspace，将qlog程序拷贝到workspace下，后续创建的文件都放在workspace中。

### 步骤3 配置config\_qlog.toml。

在workspace目录中创建config\_qlog.toml文件，内容如下：

```
port: 6000
workspace: /var/log/qlog
server_logfile: server.log
client_logfile: client.log
server_threads: 4
client_threads: 1
log_level: info
rotate_size: 65536
rotate_num: 10
monitor_items:
 - name: service #业务名
 monitor_type: file
 monitor_path: /var/log/service.log #QingTian Enclave中业务日志的路径
 outputfile: service.log #同步到父虚拟机中的日志文件名
 - name: resource
 monitor_type: resource
 monitor_interval: 15
 outputfile: resource.log
```

### 步骤4 制作含qlog的QingTian Enclave镜像。

- 在workspace目录中创建start.sh脚本：

```
#!/bin/bash
/root/qlog monitor /root/config_qlog.toml &
```

```
LOG_FILE="/var/log/service.log"
LOG_MESSAGE="Hello, service."

while true; do
 TIMESTAMP=$(date '+%Y-%m-%d %H:%M:%S')
 echo "$TIMESTAMP - $LOG_MESSAGE" >> "$LOG_FILE"
 sleep 3
done
```

2. 赋予start.sh脚本执行权限，在workspace目录中执行下述命令：  
chmod +x start.sh
3. 在workspace目录中创建Dockerfile文件，内容如下：  
FROM ubuntu:22.04  
COPY ./qlog /root/qlog  
COPY ./config\_qlog.toml /root/config\_qlog.toml  
COPY ./start.sh /root/start.sh  
CMD /root/start.sh
4. 赋予start.sh执行权限，在workspace目录中执行以下命令：  
chmod +x start.sh
5. 制作docker镜像，在workspace目录中运行以下命令：  
docker build -f Dockerfile -t test\_qlog\_enclave .
6. 制作QingTian Enclave镜像，在workspace目录中运行以下命令：  
qt enclave make-img --docker-uri test\_qlog\_enclave --eif test\_qlog\_enclave.eif

#### 步骤5 启动qlog。

1. 启动一台QingTian Enclave，在workspace目录中运行下述命令：  
qt enclave start --cpus 2 --mem 1024 --cid 4 --eif test\_qlog\_enclave.eif
2. 启动父虚拟机中的qlog，在workspace目录中运行下述命令：  
./qlog receive-file 4 ./config\_qlog.toml &
3. 父虚拟机中执行下述命令，查看service日志：  
tail -F /var/log/qlog/service.log  
可以看到每3s，打印一行日志"Hello, service."。
4. 父虚拟机中执行下述命令，查看QingTian Enclave中资源使用情况：  
tail -F /var/log/qlog/resource.log  
可以看到每15s，打印一次CPU使用率和内存使用率。

----结束

## qlog 帮助信息

### qlog help

```
$ qlog --help
A tool to monitor logs and resource usage over a Vsock connection

Usage: qlog <COMMAND>

Commands:
 monitor Monitor resource usage
 receive-file Receive data from qlog monitor
 help Print this message or the help of the given subcommand(s)

Options:
 -h, --help Print help
```

### qlog monitor help

```
$ qlog help monitor
Monitor logs and/or resource usage

Usage: qlog monitor [OPTIONS] <CONFIG>
```

Arguments:  
    <CONFIG> A configuration file in yaml format, which defines items to be monitored

Options:  
    -c, --cid <CID> CID to listen on (defaults to VMADDR\_CID\_ANY) [default: 4294967295]  
    -h, --help       Print help

qlog receive-file help

\$ qlog help receive-file  
Receive data from qlog monitor

Usage: qlog receive-file [OPTIONS] <CID> <CONFIG>

Arguments:  
    <CID>     Enclave VM's CID  
    <CONFIG> A configuration file in yaml format, which defines items to be monitored

Options:  
    -w, --workspace <WORKSPACE> Set to workspace if specified, prior to configuration file  
    -h, --help                    Print help

配置信息（Config）

表 19-7 配置参数解释

| Variable       | Type   | Description                                                |
|----------------|--------|------------------------------------------------------------|
| port           | u32    | vsoc端口                                                     |
| workspace      | String | 写入进程日志和监控数据的工作空间                                           |
| server_logfile | String | 将服务器端（qlog monitor）进程日志写入 <workspace>/<server_logfile>     |
| client_logfile | String | 将客户端（qlog receive-file）进程日志写入 <workspace>/<client_logfile> |
| server_threads | u32    | 服务器端（qlog monitor）线程数量                                     |
| client_threads | u32    | 客户端（qlog receive-file）线程数量                                 |
| log_level      | String | 日志等级（TRACE/DEBUG/INFO/WARN/ERROR/OFF）                      |
| rotate_size    | u32    | 可选参数：日志文件转储大小，默认是2MB                                       |
| rotate_num     | u32    | 可选参数：日志文件转储时，保留旧日志文件数量，默认是10                               |

| Variable      | Type   | Description |
|---------------|--------|-------------|
| monitor_items | Vector | 监控事物列表      |

表 19-8 监控项参数解释

| Variable         | Type   | Description                                          |
|------------------|--------|------------------------------------------------------|
| name             | String | 事物名称                                                 |
| monitor_type     | String | 监控类型：file表示日志文件，resource表示资源使用                       |
| monitor_path     | String | 可选参数，QingTian Enclave中要监控的日志文件路径，monitor_type只能是file |
| monitor_internel | u32    | 可选参数，资源监视间隔时间，单位是秒，默认值是15，monitor_type只能是resource    |
| outputfile       | String | 监控数据文件名称，写入监控数据的路径是 <workspace>/<outputfile>         |

配置文件参考

```
port: 6000
workspace: /var/log/qlog
server_logfile: server.log
client_logfile: client.log
server_threads: 4
client_threads: 1
log_level: info
rotate_size: 65536
rotate_num: 10
monitor_items:
 - name: item1
 monitor_type: file
 monitor_path: /var/log/item1.log
 outputfile: output1.log
 - name: item2
 monitor_type: file
 monitor_path: /var/log/item2.log
 outputfile: output2.log
 - name: item3
 monitor_type: file
 monitor_path: /var/log/item3.log
 outputfile: output3.log
 - name: item4
 monitor_type: file
 monitor_path: /var/log/item4.log
 outputfile: output4.log
 - name: item5
```

```
monitor_type: resource
monitor_interval: 15
outputfile: output5.log
```

## 19.6 QingTian CLI ( qt CLI )

### 19.6.1 安装 qt CLI

如果您使用其他Linux镜像，请通过华为云QingTian开源仓库进行编译安装。如果您使用Huawei Cloud EulerOS系统镜像时，通过以下命令直接安装：

```
yum install qingtian-tool
```

该rpm包中包含两个工具:

qt-enclave-env: 提供资源隔离功能, QingTian Enclave虚拟机创建之前需要隔离指定内存供enclave虚拟机使用, 以保证QingTian Enclave虚拟机空间的绝对安全。

qt CLI: 是一个QingTian命令行工具。您可以使用qt CLI制作QingTian Enclave虚拟机启动所需要的EIF镜像, 和管理QingTian Enclave虚拟机生命周期。

注意：在使用qt CLI之前，您需要预先安装python3以及几个必要的python模块：docker 和knack。可以参考以下命令进行安装：

```
pip3 install docker knack
```

### 19.6.2 qt-enclave-env 工具介绍

qt-enclave-env是一个service，service启动后从qt-enclave-env.conf配置文件中读取需要隔离的资源信息，并执行资源隔离操作。隔离操作需要在创建QingTian Enclave虚拟机之前执行。

接下来我们将介绍该服务的配置文件/etc/qingtian/enclave/qt-enclave-env.conf:

```
#enclave虚拟机隔离大页内存类型，可配置2或1024，分别表示2M大页或1G大页
hugepage_size:1024
配置需要隔离的内存大小，数值需要为hugepage_size的整数倍。
memory_mib:1024
配置需要隔离的cpu个数，该配置项与cpu_list互斥，二者只能配置一个，否则service启动失败
cpu_count:2
配置需要隔离的cpu列表，可填入0以外的其他cpu id，该配置项与cpu_count互斥，二者只能配置一个，否则
service启动失败
cpu list:2,3
```

需要注意的是：qt-enclave-env服务预留大页内存是否成功受父虚拟机本身内存碎片化影响，系统长时间运行或者反复重启qt-enclave-env可能导致无法预留出足够的大页内存。推荐的使用方式是在系统刚启动时，启动一次qt-enclave-env预留足够的内存即可。

### 19.6.3 qt enclave 子命令介绍

qt为一级命令，其下目前包含enclave一个二级子命令:

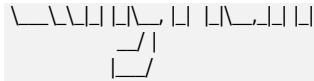
```
[root@localhost ~]# qt
```

$\overline{f} \_ \backslash (\bar{\phantom{x}})$        $\overline{| \_ - } (\bar{\phantom{x}})$

| | | | \_ \_ \_ \_ \_ \_ | | \_ \_ \_ \_ \_ \_

| | | | | ' \ / ' \ / ' \ / ' \ /

| | \_ | | | | | | | ( ) | | | | ( ) | | |



Welcome to the cool QingTian new CLI!

enclave : Enclave life-circle management.

qt enclave 中提供 enclave 相关的镜像制作、拉起、销毁、查询 QingTian Enclave 等子命令：

```
[root@localhost ~]# qt enclave
usage: qt enclave [-h] {make-img,start,stop,query,console} ...
qt enclave: error: the following arguments are required: _subcommand
enclave command line interface
[root@localhost ~]# qt enclave -h
```

#### Group

qt enclave : Enclave life-circle management.

#### Commands:

console : Console an enclave via the enclave-id while debugging.  
make-img : Make an eif image from a docker image.  
query : Query an enclave via the enclave-id or query all enclaves.  
start : Start an enclave via an eif image.  
stop : Stop an enclave via the enclave-id.

## qt enclave make-img

该命令用于将用户制作好的 docker 镜像转换为 QingTian Enclave 虚拟机可用的镜像，命令格式如下：

```
[root@localhost ~]# qt enclave make-img -h
```

#### Command

qt enclave make-img : Make an eif image from a docker image.

#### Arguments

--docker-uri [Required]  
--eif [Required]  
--private-key  
--signing-certificate

#### Global Arguments

--debug : Increase logging verbosity to show all debug logs.  
--help -h : Show this help message and exit.  
--only-show-errors : Only show errors, suppressing warnings.  
--output -o : Output format. Allowed values: json, jsonc, none, table, tsv, yaml, yamlc. Default: json.  
--query : JMESPath query string. See <http://jmespath.org/> for more information and examples.  
--verbose : Increase logging verbosity. Use --debug for full debug logs.

#### Examples

Given docker-uri and eif to make an eif image

```
qt enclave make-img --docker-uri [DOCKER-URI] --eif [EIF]
```

Make an eif image with private-key and signing-certificate

```
qt enclave make-img --docker-uri [DOCKER-URI] --eif [EIF] --private-key [PRIVATE-KEY] --signing-certificate [SIGNING-CERTIFICATE]
```

必选项：--docker-uri，指定 Docker 存储库中 Docker 映像的统一资源标识符（URI）。可以通过 docker image ls 命令查询当前本地镜像 uri。

必选项：--eif，提供路径名称用于存放生成后的 EIF 镜像

可选项：--private-key，提供对 QingTian Enclave 镜像进行签名的私钥绝对路径，如果指定了 PRIVATE-KEY，要求必须同时指定签名密钥 SIGNING-CERTIFICATE；



可选项: `--signing-certificate`, 提供对QingTian Enclave镜像进行签名的证书绝对路径, 如果指定了SIGNING-CERTIFICATE, 如要同时指定签名密钥PRIVATE-KEY;

命令行返回值: 如果配置了以上两项证书可选项, 必须保证证书有效。证书有效情况下命令输出将包括额外的PCR0, PCR8散列值用于度量Enclave镜像与签名证书。证书无效, 镜像创建失败。

创建镜像命令示例:

```
[root@localhost docker]# qt enclave make-img --docker-uri ubuntu --eif /home/docker/ubuntu.eif --private-key /home/docker/private-key.pem --signing-certificate /home/docker/server.pem
{
 "digest": "SHA384",
 "PCR0": "b8c59692da8a5bcb739a83d15a0ceca670bd78da06cb2250ec70548f72254e674419e9888db9c0364a9b88dd58017a62",
 "PCR8": "dbf4a7f9fab7f18619b5899c407081981ad6762fb9a809da78548821b5021965423181584acd7b201703376f1133a546"
}
```

## qt enclave start

该命令用于创建QingTian Enclave虚拟机, 命令格式如下:

```
[root@localhost ~]# qt enclave start -h
```

### Command

qt enclave start : Start an enclave via an eif image.

### Arguments

--cid : Default: 4.  
--eif [Required]  
--cpus : Default: 2.  
--debug-mode  
--mem : Default: 1024.

### Global Arguments

--debug : Increase logging verbosity to show all debug logs.  
--help -h : Show this help message and exit.  
--only-show-errors : Only show errors, suppressing warnings.  
--output -o : Output format. Allowed values: json, jsonc, none, table, tsv, yaml, yamlc. Default: json.  
--query : JMESPath query string. See <http://jmespath.org/> for more information and examples.  
--verbose : Increase logging verbosity. Use --debug for full debug logs.

### Examples

Given an eif image, an unused cid, the number of cpus and memory needed  
qt enclave start [--cpus CPUS] [--mem MEM] --eif EIF [--cid CID]

可选项: `--cpus`, 指定要分配给enclave虚拟机的vCPU数量, 不能大于隔离的cpu数目, 未配置使用默认值2;

可选项: `--mem`, 指定分配给QingTian Enclave虚拟机的内存大小 (MB), 不能大于隔离内存大小, 需大于QingTian Enclave镜像大小, 未配置使用默认值1024MB;

必选项: `--eif`, 指定EIF镜像路径;

可选项: `--cid`, 设置QingTian Enclave虚拟机cid, 用于指定父虚拟机与QingTian Enclave虚拟机间vsock通信的socket IP。可用的cid范围为: 4-4294967294, 未配置使用默认值4;

可选项: `--debug-mode`, 指定是否在调试模式下启动QingTian Enclave实例, 该模式下使用全部为0的PCR散列值, 可以收集打印QingTian Enclave虚拟机内部日志;

命令行返回值：创建成功后输出创建的QingTian Enclave虚拟机详细信息。

Enclave虚拟机启动命令示例：

```
qt enclave start --cpus 2 --mem 1024 --eif /home/docker/ubuntu.eif --cid 4
```

## qt enclave query

该命令用于在父虚拟机内查询当前已创建的QingTian Enclave虚拟机信息，命令格式如下：

```
[root@localhost ~]# qt enclave query -h
```

### Command

qt enclave query : Query an enclave via the enclave-id or query all enclaves.

### Arguments

--enclave-id

### Global Arguments

--debug : Increase logging verbosity to show all debug logs.

--help -h : Show this help message and exit.

--only-show-errors : Only show errors, suppressing warnings.

--output -o : Output format. Allowed values: json, jsonc, none, table, tsv, yaml, yamlc.  
Default: json.

--query : JMESPath query string. See <http://jmespath.org/> for more information and examples.

--verbose : Increase logging verbosity. Use --debug for full debug logs.

### Examples

Given an enclave-id to query an enclave

```
qt enclave query --enclave-id [ENCLAVE-ID]
```

Query all enclaves without enclave-id

```
qt enclave query
```

可选项：--enclave-id，query时带此参数则查询指定QingTian Enclave虚拟机信息，否则查询全部当前已存在QingTian Enclave虚拟机信息；

命令行返回值，查询到的QingTian Enclave虚拟机信息：

- EnclaveID：QingTian Enclave虚拟机的id号；
- ProcessID：父虚拟机中持有QingTian Enclave资源的进程号PID；
- EnclaveCID：QingTian Enclave虚拟机与父虚拟机通信使用的vsock socket id；
- NumberOfCPUs：从父虚拟机分配给QingTian Enclave虚拟机的vCPU个数；
- MemoryMiB：从父虚拟机分配给QingTian Enclave虚拟机的内存大小(MB)；

QingTian Enclave虚拟机查询命令示例：

```
[root@localhost ~]# qt enclave query
```

```
[[{"EnclaveID": 0,
 "ProcessID": 29990,
 "EnclaveCID": 4,
 "NumberOfCPUs": 2,
 "MemoryMiB": 1024,
 "LaunchMode": "debug"}]]
```

若当前无QingTian Enclave虚拟机存在，则该命令查询返回空；

带--enclave-id参数查询场景，若指定enclave-id的QingTian Enclave虚拟机不存在，查询命令返回空。

## qt enclave stop

该命令用于在父虚拟机内销毁已创建的QingTian Enclave虚拟机，命令格式如下：

```
[root@localhost ~]# qt enclave stop -h
```

### Command

qt enclave stop : Stop an enclave via the enclave-id.

### Arguments

--enclave-id [Required]

### Global Arguments

--debug : Increase logging verbosity to show all debug logs.

--help -h : Show this help message and exit.

--only-show-errors : Only show errors, suppressing warnings.

--output -o : Output format. Allowed values: json, jsonc, none, table, tsv, yaml, yamlc. Default: json.

--query : JMESPath query string. See <http://jmespath.org/> for more information and examples.

--verbose : Increase logging verbosity. Use --debug for full debug logs.

### Examples

Given an enclave-id to stop an enclave

```
qt enclave stop --enclave-id [ENCLAVE-ID]
```

必选项：--enclave-id，指定需要销毁的QingTian Enclave虚拟机的enclave-id

命令行返回值：成功返回销毁成功，销毁失败无返回。

QingTian Enclave虚拟机销毁命令示例：

```
[root@localhost ~]# qt enclave stop --enclave-id 1
stop 1 success
```

## qt enclave console

在启动QingTian Enclave时，指定为debug-mode时，用于在父虚拟机中查看QingTian Enclave中的只读控制台输出，命令格式如下：

```
[root@localhost ~]# qt enclave console -h
```

### Command

qt enclave console : Console an enclave via the enclave-id while debugging.

### Arguments

--enclave-id [Required]

### Global Arguments

--debug : Increase logging verbosity to show all debug logs.

--help -h : Show this help message and exit.

--only-show-errors : Only show errors, suppressing warnings.

--output -o : Output format. Allowed values: json, jsonc, none, table, tsv, yaml, yamlc. Default: json.

--query : JMESPath query string. See <http://jmespath.org/> for more information and examples.

--verbose : Increase logging verbosity. Use --debug for full debug logs.

### Examples

Given an enclave-id to console an enclave

```
qt enclave console --enclave-id [ENCLAVE-ID]
```

必选项：--enclave-id，指定需要获取只读控制台输出的QingTian Enclave虚拟机的enclave-id。

命令执行成功后，会打印QingTian Enclave虚拟机的只读控制台输出，如下所示：

```
hello enclave!
hello enclave!
hello enclave!
hello enclave!
```

您可以使用ctrl+c的方式退出该命令。需要注意的是，在同一时间我们只允许一个qt enclave console命令作用于一个指定的QingTian Enclave实例。

19.7 错误码

| 错误码 | 错误信息                                                     | 描述                         | 处理措施                            |
|-----|----------------------------------------------------------|----------------------------|---------------------------------|
| 01  | Missing necessary argument.                              | 必要参数缺失                     | 请您对命令参数进行检查                     |
| 02  | Invalid argument provided.                               | 无效参数                       | 请您对命令参数进行检查                     |
| 03  | File operation failure.                                  | 文件操作错误                     | 请您检查目标文件或目录是否存在                 |
| 04  | loctl get sandbox capacity failure.                      | loctl获取 sandbox capacity错误 | 请您联系华为云技术支撑人员帮您处理               |
| 05  | loctl define sandbox failure.                            | loctl定义 sandbox错误          | 请您联系华为云技术支撑人员帮您处理               |
| 06  | Invalid parameters provided in configuration file.       | 配置文件中存在无效参数                | 请您检查对应配置文件                      |
| 07  | Missing necessary parameters in configuration file.      | 配置文件中缺少必要参数                | 请您检查对应配置文件                      |
| 08  | Mmap memory failure.                                     | Mmap内存错误                   | 请您联系华为云技术支撑人员帮您处理               |
| 09  | loctl add memory failure.                                | loctl增加内存错误                | 请您联系华为云技术支撑人员帮您处理               |
| 10  | Load image failure because provided memory is too small. | 加载镜像错误，可能是因为设置的内存大小不够      | 请您在启动QingTian Enclave时，增加内存参数设置 |
| 11  | loctl add cpu failure.                                   | loctl增加vcpu错误              | 请您联系华为云技术支撑人员帮您处理               |
| 12  | Lock acquire failure.                                    | 请求锁失败                      | 请您检查qt CLI日志信息，查看对应锁文件权限是否正常    |
| 13  | Socket initialization failure.                           | Socket初始化失败                | 请您联系华为云技术支撑人员帮您处理               |

| 错误码 | 错误信息                                          | 描述                          | 处理措施                                                    |
|-----|-----------------------------------------------|-----------------------------|---------------------------------------------------------|
| 14  | Socket binding failure.                       | Socket绑定错误                  | 请您联系华为云技术支撑人员帮您处理                                       |
| 15  | Socket listen failure.                        | Socket监听错误                  | 请您联系华为云技术支撑人员帮您处理                                       |
| 16  | Socket accept failure.                        | Socket执行接收错误                | 请您联系华为云技术支撑人员帮您处理                                       |
| 17  | Write heartbeat to the enclave failure.       | 给QingTian Enclave写入心跳信息出错   | 请您联系华为云技术支撑人员帮您处理                                       |
| 18  | Read heartbeat from the enclave failure.      | 读取QingTian Enclave心跳信息出错    | 请您联系华为云技术支撑人员帮您处理                                       |
| 19  | loctl start an enclave failure.               | loctl启动QingTian Enclave失败   | 请您联系华为云技术支撑人员帮您处理                                       |
| 20  | Wait heartbeat timeout.                       | 等待心跳信息超时                    | 请您在启动QingTian Enclave时，增加内存参数配置；如未能解决，请您联系华为云技术支撑人员帮您处理 |
| 21  | Get json print object failure.                | 获取json打印对象失败                | 请您检查cjson库是否正常                                          |
| 22  | Write enclave's configuration file failure.   | 生成QingTian Enclave配置文件失败    | 请您查看qt CLI日志信息，排查相关文件权限；如未能解决，请您联系华为云技术支撑人员帮您处理         |
| 23  | Socket connection failure                     | Socket连接错误                  | 请您联系华为云技术支撑人员帮您处理                                       |
| 24  | Write cmd to the enclave server failure.      | 向QingTian Enclave后台服务写入命令失败 | 请您联系华为云技术支撑人员帮您处理                                       |
| 25  | Read message from the enclave server failure. | 获取QingTian Enclave后台服务信息失败  | 请您联系华为云技术支撑人员帮您处理                                       |
| 26  | Create cJSON object failure.                  | 创建cjson对象失败                 | 请您检查cjson库是否正常                                          |
| 27  | Create cJSON array failure.                   | 创建cjson数组失败                 | 请您检查cjson库是否正常                                          |

| 错误码 | 错误信息                                                         | 描述                                  | 处理措施                                            |
|-----|--------------------------------------------------------------|-------------------------------------|-------------------------------------------------|
| 28  | The required enclave is not running.                         | 被请求的QingTian Enclave实例并没有在运行        | 请您使用qt enclave query命令查看目前正在运行的QingTian Enclave |
| 29  | Invalid enclave pid.                                         | 无效的Enclave PID                      | 请您联系华为云技术支撑人员帮您处理                               |
| 30  | Add number into cJSON object failure.                        | 向cjson打印对象中增加数字失败                   | 请您检查cjson库是否正常                                  |
| 31  | Add string into cJSON object failure.                        | 向cjson打印对象中增加字符串失败                  | 请您检查cjson库是否正常                                  |
| 32  | The required enclave is not running in the debug mode.       | 被请求的QingTian Enclave实例没有运行在debug模式下 | 请您使用qt enclave query 查询该QingTian Enclave运行模式    |
| 33  | Enclave console read failure.                                | QingTian Enclave console 命令读取失败     | 请您联系华为云技术支撑人员帮您处理                               |
| 34  | Write img header failure.                                    | 创建镜像时，写入镜像头文件失败                     | 请您联系华为云技术支撑人员帮您处理                               |
| 35  | Write cmdline failure.                                       | 创建镜像时，写入cmdline失败                   | 请您联系华为云技术支撑人员帮您处理                               |
| 36  | Write kernel failure.                                        | 创建镜像时，写入kernel失败                    | 请您联系华为云技术支撑人员帮您处理                               |
| 37  | Write initrd failure.                                        | 创建镜像时，写入initrd失败                    | 请您联系华为云技术支撑人员帮您处理                               |
| 38  | Write certificate failure.                                   | 创建镜像时，写入证书失败                        | 请您联系华为云技术支撑人员帮您处理                               |
| 39  | Get pcr failure.                                             | 获取PCR值失败                            | 请您联系华为云技术支撑人员帮您处理                               |
| 40  | Add signature failure.                                       | 创建镜像时，对镜像签名出错                       | 请您联系华为云技术支撑人员帮您处理                               |
| 41  | Check enclave image info failure while building an eif file. | 构建eif镜像时检查到enclave镜像信息异常            | 请您联系华为云技术支撑人员帮您处理                               |
| 42  | The required enclave is in maintenance state.                | 被请求的QingTian Enclave实例正处于维护阶段       | 请您联系华为云技术支撑人员帮您处理                               |

| 错误码 | 错误信息                           | 描述        | 处理措施            |
|-----|--------------------------------|-----------|-----------------|
| 43  | The cid has already been used. | cid已经在使用中 | 请您重新指定未在使用中的cid |

## 19.8 常见问题

### 19.8.1 通用类

#### 什么是 QingTian Enclave?

QingTian Enclave是基于QingTian架构虚拟机产品所提供的的一个安全特性。借助QingTian Enclave提供的隔离、高度受限的环境，客户可以部署其安全敏感型应用程序，缩小其攻击面。

#### 为什么需要使用 QingTian Enclave?

QingTian Enclave在普通的ECS实例中提供了隔离的计算环境，以处理高度敏感的数据。

QingTian Enclave是完全独立的虚拟机，无持久化存储、交互式访问或外部网络连接，您的ECS实例通过安全的本地通道与QingTian Enclave之间进行通信。

#### 什么时候需要使用 QingTian Enclave?

当您需要处理安全敏感型数据，并希望处理该数据的过程与有权访问您实例的用户、应用程序或者三方库隔离时，您应该使用QingTian Enclave。

您可以利用QingTian Enclave开发和运行各种程序，以应对不同的使用场景，比如个人隐私信息处理，专有代码和算法运算，多方计算等。

#### 如何开始使用 QingTian Enclave?

您可以参考QingTian Enclave[快速入门](#)，来开启您的QingTian Enclave开发之旅。

#### 什么是内存和 CPU 隔离?

内存和CPU隔离技术可以防止ECS实例上的用户、应用程序和第三方库直接访问已被隔离给QingTian Enclave使用的内存和CPU。您可以通过华为云QingTian命令行工具（qt CLI），使用这部分被隔离的内存和CPU启动QingTian Enclave虚拟机，详细操作请参考[QingTian CLI（qt CLI）](#)。

#### QingTian Enclave 是如何保证内存和 CPU 隔离的?

QingTian Enclave采用经过验证的基于CPU的隔离技术，并结合QingTian架构的独特设计和基于华为自研智能网卡的可信根证书，共同实现隔离。由华为云开发和设计的极简QingTian Hypervisor可以将服务器的物理资源进行分区。相比于其他虚拟化技术，QingTian Hypervisor裁减了所有不必要的功能。QingTian Enclave扩展了QingTian Hypervisor的隔离功能，保护了分配给QingTian Enclave的CPU和内存，保证其与ECS实例的CPU和内存资源相隔离，为您提供一个完全隔离的可执行环境。

## 哪些实例规格支持 QingTian Enclave?

目前c7t、kc2实例已支持QingTian Enclave特性。

## 什么是证明（Attestation）文档？

证明文档用于证明QingTian Enclave实例的可信度量结果。证明文档由QingTian Hypervisor生成，文档内容包括PCR（Platform configuration registers，平台配置寄存器）列表、QingTian Attestation PKI（Public Key Infrastructure，公钥基础设施）证书链、密码算法声明以及Enclave应用自定义数据。

证明文档由华为云QingTian Attestation PKI签署。华为云KMS（Key management Service，密钥管理服务）内置了对QingTian Enclave证明的支持。通过使用QingTian Enclave SDK中包含的华为云KMS API，您可以在QingTian Enclave实例中基于QingTian Enclave证明来执行华为云KMS操作，比如解密、生成随机数和加密等操作。华为云KMS服务提取来自QingTian Enclave的证明文档并根据预设的华为云IAM（Identity and Access Management，统一身份认证服务）授权策略对其进行访问权限控制。

## QingTian Enclave 证明文件的信任根源是什么？该如何验证它？

证明文档由华为云QingTian Attestation PKI（Public Key Infrastructure）签署。华为云QingTian根证书可以从[https://qingtian-enclave.obs.myhuaweicloud.com/huawei\\_qingtian-enclaves\\_root-G1.zip](https://qingtian-enclave.obs.myhuaweicloud.com/huawei_qingtian-enclaves_root-G1.zip)下载获取。文档签名验证方法请参考[文档签名验证](#)。

## QingTian Enclave 如何进行收费？

目前使用QingTian Enclave不会收取额外费用，您只需要支付ECS实例的购买费用。

## 为什么执行隔离服务会失败（systemctl start qt-enclave-env）？

在系统运行过程中，不可避免地会产生碎片化内存，使得隔离服务时无法获取连续内存大页。

执行**systemctl status qt-enclave-env**命令，查看错误日志内是否包含**allocating hugepages error**。

如果包含该错误日志，则说明此时系统内所提供的可用空闲连续大页资源少于您所期望的内存大页数量（\$wanted\_mem\_num）。

您可以采用如下两种方案进行处理。

- 方案一：

- a. 执行以下命令，查看当前系统所能提供的最大可用连续内存大页数量（\$free\_mem\_num）。

```
cat /sys/devices/system/node/node0/hugepages/
hugepages-1048576kB/free_hugepages
```

- b. 执行以下命令，修改/etc/qingtian/enclave/qt-enclave-env.conf配置文件，使得memory\_mib的值低于(\$free\_mem\_num \* 1024)。

```
vim /etc/qingtian/enclave/qt-enclave-env.conf
```

建议您在系统启动后立即执行资源隔离服务，避免反复执行隔离命令造成内存碎片化。



- 方案二：
  - a. 执行以下命令，修改grub文件（/etc/default/grub）。  
**vim /etc/default/grub**  
在grub文件的Linux命令行参数（GRUB\_CMDLINE\_LINUX）中，添加（default\_hugepagesz=1G hugepagesz=1G hugepages=\$wanted\_mem\_num）。
  - b. 执行以下命令，使得配置生效。  
**grub2-mkconfig -o /boot/efi/EFI/hce/grub.cfg**
  - c. 重启虚拟机，重启后可再次查看可用大页数量。  
**reboot**

## 19.8.2 开发部署类

### 一个 ECS 实例可以部署多少个 QingTian Enclave?

QingTian Enclave支持为每个ECS实例创建最多2个Enclave虚拟机。

### 什么是 Vsock? 我该如何使用 Vsock 与 QingTian Enclave 进行通信?

Vsock是一种套接字接口，由上下文 ID (CID) 和端口号定义，上下文ID与TCP/IP连接中的IP地址相同。

Vsock使用标准、定义明确的POSIX套接字API（例如连接、侦听、接受）与QingTian Enclave进行通信。您可以开发基于vsock与QingTian Enclave通信的程序，详细操作请参考[Linux系统上QingTian Enclave应用开发](#)。另外应用程序也可以借助代理，通过vsock发送HTTP请求。

### 为什么使用 kc2 实例启动 QingTian Enclave 后，出现 Vsock 性能下降?

对于kc2实例，如果使用隔离的全部CPU启动QingTian Enclave，会导致Vsock性能下降。

建议您在启动隔离服务时，比预期QingTian Enclave使用的CPU数量，多隔离2个CPU。这样可以使被隔离服务的一部分CPU用于启动QingTian Enclave，一部分CPU用于Vsock转发，避免出现Vsock性能下降。

1. 执行以下命令，修改qt-enclave-env服务的配置文件/etc/qingtian/enclave/qt-enclave-env.conf。  
**vim /etc/qingtian/enclave/qt-enclave-env.conf**
  - 方式一：修改cpu\_count数量为QingTian Enclave的CPU数量加2。
  - 方式二：修改cpu\_list中的CPU数量为QingTian Enclave的CPU数量加2。
2. 执行以下命令，重启qt-enclave-env服务。  
**systemctl restart qt-enclave-env**
3. 执行以下命令，重启QingTian Enclave。  
**qt enclave start --cpus \${isolated\_cpus\_count-2} --mem \${wanted\_mem} --eif \${eif\_file\_location} --cid \${wanted\_cid}**  
其中：
  - isolated\_cpus\_count-2：隔离出来的CPU数量减少2

- wanted\_mem: 期望内存大小
- eif\_file\_location: eif文件位置
- wanted\_cid: 期望cid值

重启QingTian Enclave后观察vsock性能。

## ECS 实例开启 SELinux 后，为什么启动 qt-enclave-env 服务会失败？

问题现象：ECS实例开启SELinux后，启动qt-enclave-env服务失败，查看qt-enclave-env服务日志，失败的日志显示“insmod virtio-qtbox.ko Permission denied”。

问题原因：SELinux通过强制访问控制、细粒度的访问控制、策略强制、类型强制、安全上下文和审计功能等特性，提供了强大的安全机制，可以帮助保护Linux 系统免受恶意攻击和数据泄露的威胁。因此，qt-enclave-env服务中无法直接调用insmod virtio-qtbox.ko命令插入内核模块。

解决方案：请您通过手动执行命令insmod /opt/qingtian/enclave/virtio-qtbox.ko，或者关闭SELinux特性，并重启qt-enclave-env服务规避该问题。

## 如果使用 Ubuntu 类型 Linux 镜像，需要额外做什么工作？

1. 需要您使用[huawei-qingtian](#)源码编译virtio-qtbox和qingtian-tools包
2. 执行以下命令，制作镜像所需的qt-enclave-bootstrap包。

可以下载最新的qt-enclave-bootstrap的包，并解压文件到指定目录，下载地址：[https://repo.huaweicloud.com/hce/2.0/updates/x86\\_64/Packages/](https://repo.huaweicloud.com/hce/2.0/updates/x86_64/Packages/)。

/usr/local/share/qingtian/enclave/init

/usr/local/share/qingtian/enclave/qlsm.ko

/usr/local/share/qingtian/enclave/vmlinux.bin

/usr/local/share/qingtian/enclave/vmlinux.bin.bz2